出國報告（出國類別：考察）

考察歐盟、比利時與德國個人資料保護法規之規劃及施行情形報告

服務機關：行政院科技會報辦公室、法務部
姓名職稱：陳維練 法務部法律事務司司長
柴惠玲 行政院科技會報辦公室組主任
鄭輝彬 法務部資訊處副處長
胡美蓁 法務部法律事務司科長
鄭其昀 法務部法律事務司專員

派赴國家：比利時（歐盟）、德國

出國期間：中華民國 101 年 6 月 9 日至 6 月 17 日

報告日期：中華民國 101 年 9 月 17 日

摘　　要

鑑於我國「個人資料保護法」修法過程，於 91 年年 10 月邀請學者、專家組成修法小組，主要參酌 1995 年歐盟資料保護指令(95/46/EC)內容，同時輔以德國聯邦個人資料保護法制立法例，進行研討修法事宜。惟歐盟執行委員會為因應新科技及新興社會型態，業於 2012 年 1 月 25 日向歐洲理事會及歐洲議會正式提出「一般資料保護規則」草案，包含重新調整特種資料保護政策以及因應新興科技服務等問題，未來立法通過後，歐盟資料保護指令(95/46/EC)亦將廢止，並直接作為歐盟各會員國之統一性個人資料保護法規範。考量我國於 99 年 5 月 26 日修正公布之「個人資料保護法」，主要係參考上開歐盟 1995 年指令，而前開指令既經歐盟大幅翻修，則我國宜再考量歐盟最新個資規範趨勢，檢視我國個人資料保護法，擬定適當修法政策，以與國際接軌。緣此，實有必要追本溯源、瞭解本制度於歐盟之法制實施經驗及最新修法規劃。

本次考察活動針對歐盟及相關國家之個人資料保護法規，分別就歐盟整體立法趨勢、歐盟會員國(比利時聯邦及德國聯邦)之法規施行情形，以及邦層級(德國巴伐利亞邦)之實際執行經驗等 3 個面向，分別考察歐盟執行委員會(司法總署)、比利時個人資料隱私權保護委員會、德國聯邦資料保護及資訊自由委員會及德國巴伐利亞邦個人資料保護委員會等 4 個個人資料保護專責機關。而本次考察目的係在瞭解歐盟、比利時及德國如何因應新興科技服務，規劃或執行個人資料保護法制事項，以及法制運作實際狀況，爰主要針對下列問題提出詢問：（一）保護個人資料之範圍問題；（二）告知義務之制度、實際適用問題；（三）境外傳輸之規範問題；（四）其他最新立法趨勢(例如被遺忘權及刪除權) ；（五）相關機關之組織及其實際運作狀況。經實地訪談，並分析歐盟及相關國家之立法趨勢及施行現況後，爰對於我國將來修正個人資料保護法及相關法律，提出心得建議。

目　　次

附　錄

壹、 考察緣起及考察目的

依據行政院院長於民國 101 年 2 月 16 日第 3286 次院會報告事項，指示本部觀察國際間如何規範個人資料保護事項，並蒐集歐盟有關個人資料保護的相關規定或未來趨勢等資訊，以瞭解個人資料於網路世界中之境外蒐集、處理或利用之適用情形。

鑑於我國「個人資料保護法」修法過程，於 91 年年 10 月邀請學者、專家組成修法小組，主要參酌 1995 年歐盟資料保護指令(95/46/EC)內容，同時輔以德國聯邦個人資料保護法制立法例，進行研討修法事宜。惟歐盟執行委員會為因應新科技及新興社會型態，業於本年(2012 年)1 月 25 日向歐洲理事會及歐洲議會正式提出「一般資料保護規則」草案，包含重新調整特種資料保護政策以及因應新興科技服務[1]等問題，未來立法通過後，1995 年歐盟資料保護指令(95/46/EC)亦將廢止，並直接作為歐盟各會員國之統一性個人資料保護法規範。考量我國於 99 年 5 月 26 日修正公布之「個人資料保護法」，主要係參考上開歐盟 1995 年指令，而前開指令既經歐盟大幅翻修，則我國宜再考量歐盟最新個資規範趨勢，檢視我國個人資料保護法，擬定適當修法政策，以與國際接軌。復因個人資料保護法制之推動，除須妥善完備法制事務外，亦有賴資訊技術上之共同推動。因此，本次考察爰結合法制及資訊專長人員，針對歐盟、比利時、德國聯邦及巴伐利亞邦等個人資料保護法制之規劃與施行情形，進行瞭解及觀察。

[1]歐盟執行委員會於 101 年 1 月 25 日發布新聞稿略以：1995 年指令公布之際，斯時網際網路方在萌芽階段，如今因科技迅速發展及日益增加之全球性個人資料流通，改變個人資料蒐集、取得、利用及傳遞的規模及方式，事實上，現今個人資料蒐集、取得、利用及傳遞以極鉅量、釐秒之速度橫跨洲際；另特別就雲端運算而言，即更多的資料檔案儲存在遠端伺服器，而非個人電腦，個人可以取得遠端電腦資源，而不在某地域內擁有，個人資料可以立即從一國的管轄到另一國，甚至歐盟境外，故對於個人資料保護之主管機關帶來新的極大挑戰。就社群網站、雲端運算、定位服務(location-based service)及智慧卡等科技，我們所作的任何動作，都會留下數位軌跡(digital traces)，為確保個人資料保護之持續，1995 年指令需隨科技之發展與時俱進。

一、 考察行程表

日　期	時 間	考　察　對　象 （地點）	會　晤　人　士
6 月 9 日 （星期六）	上午	(自桃園機場出發)	
6 月 10 日 （星期日）	晚間	(抵達比利時)	
6 月 11 日 （星期一）	上午	比利時個人資料隱私權保護委員會（Commission de la Protection de la Vie Privee）（比利時布魯塞爾）	比利時個人資料隱私權保護委員會主席 Mr. Willem Debeuckolaere
6 月 11 日 （星期一）	下午	駐歐盟兼駐比利時代表處 （比利時布魯塞爾）	駐歐盟兼駐比利時代表處 林代表永樂
6 月 12 日 （星期二）	上午	歐洲執行委員會司法總署 （ European Commission Department of Justice） （比利時布魯塞爾）	歐洲執行委員會司法總署個人資料保護處處長 Ms. Marie-Hélène BOULANGER
6 月 13 日 （星期三）	上午	德國聯邦個人資料及資訊自由委員會（ Der Bundesbeauftrate für den Datenschutz und die Informationsfreiheit） （德國波昂）	參事兼任德國聯邦個人資料及資訊自由委員會部門主管 Ms. Petra Wuttke-Götz
6 月 15 日 （星期五）	上午	德國巴伐利亞邦個人資料保護委員會（ Der Bayerische Landesbeauftragte für den Datenschutz informiert zum Thema） （德國慕尼黑）	德國巴伐利亞邦個人資料保護委員會主席 Dr. Thomas Petri, Vita
6 月 16 日 （星期六）	下午	(返國)	
6 月 17 日 （星期日）	晚間	(抵達桃園機場)	

二、 考察項目

(一)訪問歐盟執行委員會（司法總署）（European Commission Department of Justice）之問題：

1、 歐盟各會員國對於應保護之個人資料，在類型上有無不同？歐盟規劃應立法保護或排除保護個人資料時，其主要考量因素或相關背景為何？例如：歐盟對於自然人之個人或家庭活動中所為個人資料，規劃限縮至「需受有任何報酬利益（without any gainful interest）」為限，以及針對新聞、藝術或文學表達之目的，授權各會員國免除或放寬相關規定，其原因或所欲解決之問題為何？

2、 有關一般個人資料保護規則草案規定之「同意」，取得同意之方式與標準為何？又如係透過網際網路或其他方式取得同意時，如何實踐相關規定？是否有取得證實同意方法之標準格式或相關資料可供參考？

3、 鑑於一般個人資料保護規則草案已就「告知義務（notification）」予以規定，以使各會員國能有一致性規範。惟歐盟評估告知義務之實效性如何？如何使各會員國在適用除外事由時能有一致性結果，例如如何具體適用「告知資訊為不可行（provision of such information proves impossible）」或「需不合勞費（disproportionate effort）」等事由。

4、 關於「被遺忘權（Right to be forgotten）」，資料管理者所應負擔責任之範圍及應採取措施為何？於資料管理者已授權第三人公開該個人資料之情形，資料管理者之責任是否限於應通知該第三人刪除相關連結、影本或備份外，抑或尚須採取其他相關措施？

5、 歐盟一般個人資料保護規則草案擴大適用於境外蒐集資料者（data controller）後，如何確保當事人對於境外蒐集資料者行使相關權利（例如查詢權權利（Right of access for the data subject））？除了共同約束條款（Binding Corporation Rules）之民事上機制外，是否尚有其他行政上或訴訟上機制，例如處罰境外公司規定或代表起訴？因應雲端科技之發展，是否有任何規劃方向？

6、 一般個人資料保護規則針對特種資料之規劃有何新變動？一般個人資料保護規則第 9 條(g)為增進公共利益所進行之必要資料處理（processing is necessary for the performance of a task carried out in the public interest）之規定，應如何定義其中所稱「公共利益（public interest）」或界定其範圍，就其不確定之法律概念，有無具體案例可供參考？

7、 請協助提供實務有關歐盟執行委員會（含第 29 條工作小組）執行業務相關注意事項或手冊，以供我國行政實務之參考。

(二)訪問比利時個人資料隱私權保護委員會（*The Commission for the Protection of Privacy*）之問題：

1、 比利時對於應保護之個人資料，在類型上與歐盟其他國家相較，是否有較具特色規定，其立法保護或排除保護個人資料之主要考量或相關背景為何？為何比利時個人資料保護法規及專責機關之名稱特別揭示保護隱私權等文字？又一般個人資料保護規則相關規定，例如：歐盟對於自然人之個人或家庭活動中所為個人資料，規劃限縮至「需受有任何報酬利益（*without any gainful interest*）」為限，以及針對新聞、藝術或文學表達之目的，授權各會員國免除或放寬相關規定，比利時將來有無規劃修正方向？

2、 為因應網際網路之發展，以及一般個人資料保護規則草案，比利時隱私權保護法對於當事人同意就其個人資料蒐集、處理或利用之方式限於書面，將來有無規劃修正方向？對於網路方式取得同意者，如何加以規範？

3、 比利時隱私及個人資料及隱私權保護法第 31 條告知義務之除外事由規定，例如「告知資訊為不可行（provision of such information proves impossible）」或「需不合勞費（disproportionate effort）」等事由，實務上有無具體適用之標準可供參考？

(三)訪問德國聯邦資料保護與資訊自由委員會（BFDI，The Office of the Federal Commissioner for Data Protection and Freedom of Information）之問題：

1、 多數邦對於公務機關、非公務機關之個人資料保護事項，分別設置不同之監管機關，而不採用聯邦設置於同一監管機關方式，其原因為何？優、缺點及成效如何？對於行政機關違反個人資料規定之處理方式為何？聯邦個人資料保護官（*DPO*）要求行政機關表明意見、勸告其改善或定期於活動報告書中公開之作法，其成效如何？

2、 德國對於應保護之個人資料，在類型上與歐盟其他國家相較，是否有較具特色規定（例如德國電信通訊法(TKG)如何與德國聯邦個人資料保護法（BDSG）配合運作），其立法保護或排除保護個人資料之主要考量或相關背景為何？又將來如何因應一般個人資料保護規則相關規定，例如：歐盟對於自然人之個人或家庭活動中所為個人資料，規劃限縮至「需受有任何報酬利益（*without any gainful interest*）」為限，以及針對新聞、藝術或文學表達之目的，授權各會員國免除或放寬相關規定，德國將來規劃方向為何？

3、 德國聯邦個人資料保護法（*BDSG*）第 4 條(a)關於書面同意之規定，如何適用於網際網路世界？將來如何因應網際網路之發展？又將來一般個人資料保護規則草案之相關規定施行後，德國聯邦個人資料保護法（*BDSG*）如何配合修正？

4、 關於德國聯邦個人資料保護法（*BDSG*）第 13 條第 2 項規定所稱之「公共利益（*public interest*）」，德國目前實務上有無判斷之基準？為因應一般個人資料保護規則第 9 條(g)為增進公共利益所進行之必要資料處理（*processing is necessary for the performance of a task carried out in the public interest*）之規定，德國是否規劃修正相關法規，就其不確定之法律概念，有無實務判斷基準或具體實例可供參考？

5、 請協助提供德國聯邦資料保護與資訊自由辦公室執行業務相關注

意事項或手冊，以供我國行政實務之參考；並推薦值得購買之個人資料保護業務相關專業書籍（*handbook & casebook*）之名稱與出版社。

(四)訪問德國巴伐利亞邦個人資料保護委員會（*The Bavarian State Commissioner for Data Protection*）之問題：

1、德國巴伐利亞邦個人資料保護委員會（*The Bavarian State Commissioner for Data Protection*）的基本概況：工作人員總數（並請將公務員數額與聘僱人員數額分開計算）、工作職掌內部分工方式、年度預算概數。

2、巴伐利亞邦對於公務機關、非公務機關之個人資料保護事項，分別設置不同之監管機關，而不採用聯邦設置同一監管機關方式，其原因為何、優缺點及成效如何？

3、巴伐利亞邦對於公務機關、非公務機關違反個人資料規定之處理方式及其成效如何？如同一案件涉及公務機關、非公務機關時，貴單位與巴伐利亞邦資料保護督察官辦公室（*Bavarian State Office for Data Protection Inspectorate*）之處理程序是否不同？如何共同合作？

4、聯邦及巴伐利亞邦對於個人資料保護法有何差異？例如巴伐利亞邦對於特種資料有無特別規定。

5、巴伐利亞邦個人資料保護法第 15 條書面同意之規定，如何適用於網際網路世界？將來如何因應網際網路之發展？

6、關於巴伐利亞邦個人資料保護法（*BayDSG*）所稱之「公共利益（*public interest*）」，巴伐利亞邦個人資料保護法（*BayDSG*）第 17 條所稱之「公共利益」，目前實務上有無判斷之基準或具體實例可供參考？

7、請協助提供巴伐利亞邦個人資料保護委員會執行業務相關注意事項或手冊，以供我國行政實務之參考；並推薦值得購買之個人資料保護業務相關專業書籍（*handbook & casebook*）之名稱與出版社。

貳、 考察歐盟個人資料保護法制情形

一、 歐盟個人資料保護法規簡介

歐盟現行「個人資料保護指令」(1995 年制定)僅係一框架式立法模式，歐盟各會員國得依據「歐盟個人資料保護指令」規定，將相關規定內國法化，因此各歐盟會員國間之個人資料保護法規範，仍不完全相同。為使歐盟各會員國能適用一致性之個人資料保護法規，歐盟執行委員會已於本年(2012 年)1 月 25 日正式向理事會提出「保護個人關於處理及自由流通其個人資料規則（以下簡稱「一般資料保護規則」)」草案共 91 條（Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)）[2]，並將取代僅 34 條之「歐盟資料保護指令」。依據歐盟執行委員會副主席 Viviane Reding 於 2011 年 11 月 29 日發表之演講所示，個人資料保護指令之立法政策制訂背景，網際網路之發展尚屬蟄伏之勢，如今為因應新興科技服務（社群網站、雲端計算、手機位置或智慧卡片），必須重新調整個人資料保護架構[3]。

二、 歐盟規劃制定一般個人資料保護規則草案之背景及考量

（一）歐盟執行委員會司法總署之簡介

歐盟執行委員會（European Commission）係歐盟最高行政機關，其下設置「司法總署」（Department of Justice）綜理歐盟個人資料保護法制事務外，並設有歐盟個人資料保護督察官（European Data Protection Supervisor，EDPS），負責歐盟內部機關(構)之個人資料保護事務。此外，歐盟並依據個人資料保護指令第 29 條規定，由各會員國主管機關、區域機構或團體及委員會代表組成「第 29 條工作小組」（Article 29 Data Protection Working Party），獨立行使其職權，專

[2] 詳見附錄二。

[3] 有關詳細修法資訊，請參考下列網站：
http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

責歐盟個人資料法保護法規諮商事項，歐盟執行委員會並規劃俟一般個人資料保護規則立法通過，將「第 29 條工作小組」改置為歐盟個人資料保護之專責機關。

（二）考察情形

本考察小組於 101 年 6 月 12 日抵達歐盟執行委員會司法總署，經該總署個人資料保護處處長 Ms. Marie-Hélène BOULANGER、國際組組長 Mr. B. Gencarelli、機構與國際關係處政策官 Mr. Gaspard Demur 等人代表接見，並由該總署個人資料保護處處長 Ms. Marie-Hélène BOULANGER 就本考察小組所提問題，回應如下：

1、 歐盟保護個人資料之類型及範圍，其主要考量因素：

（１）個人資料保護指令與一般個人資料保護規則所規範所保護個人資料之類別並無不同，其保護範圍均為可識別或足資識別之個人資料，而於一般個人資料保護規則草案所作更詳盡、統一性規範下，各會員國之立法空間將縮減，將來必須遵循歐盟個人資料保護規則。

（２）其次，歐盟一般個人資料保護規則雖然明文自然人之個人或家庭活動中所為個人資料，必須為「受有任何報酬利益」，但此在邏輯上仍與個人資料保護指令類似，且因自然人之個人或家庭活動，本來即不應有任何報酬利益，因此予以詳盡明文規範。

（３）關於新聞、藝術或文學領域，個人資料保護指令與一般個人資料保護規則之規範邏輯仍然相同，其二者差別僅在於後者基本上更為清楚，同時衡平各會員國作法，故其並未介入會員國或案件中，要求各會員國應絕對適用。各會員國有不同的社會基準，會有不同類型的解釋適用結果。而歐洲法院針對類似案件(例如 Lindqvist 案[4])所為之判決[5]，已

[4]瑞典一位教區教師，建立一個個人網頁，並可自教區網頁連結進入，惟其未經允許即將受其指導教區居民之姓名、職務、電話號碼等資料於置於上開個人網頁，因而受到處罰。

要求對相關領域給予更寬廣之解釋空間，這亦可能適用於隱私權範疇。此外，一般個人資料保護規則第 80 條規定[6]，亦可避免國家過度介入個人及家庭生活。

2、 有關取得當事人同意之方式、標準，以及網路上之履行方法：

（１）首先，可利用個人資料之事由，不限於當事人之同意，尚包括聲明、契約、法定義務或利益衡平等情形。簡言之，如對資料蒐集者與資料當事人之利益業經公平程序加以平衡時，即無需再經當事人同意。

（２）然而，須取得當事人同意之情形中，即應著重同意之品質，以確保是取得當事人完善的同意。亦即資料蒐集者應以明確、適當的方法，使當事人能自由且具體的得知訊息。當事人可透過一項聲明或明確的行動(包括以在網站的框格勾選方式、任何其他聲明或行為)，而同意之內容應包涵所有為同一目的或用途所進行的處理活動，以確保其個人認知及同意個人資料處理行為。因此，緘默或未回應尚非同意。另如以電子方式請求當事人同意時，此種請求必須是明確、簡潔，且不能對其所提供的服務使用產生不必要之影響。

（３）又一般個人資料保護規則對於同意之方式，並無標準格

---

[5]詳見 Case C-101/01， 2004 All E.R. 561.

6 Article 80(Processing of personal data and freedom of expression):"

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to thirdcountries and international organisations in Chapter V, the independent supervisoryauthorities in Chapter VI and on co-operation and consistency in Chapter VII for theprocessing of personal data carried out solely for journalistic purposes or the purposeof artistic or literary expression in order to reconcile the right to the protection ofpersonal data with the rules governing freedom of expression.

2. Each Member State shall notify to the Commission those provisions of its law whichit has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at thelatest and, without delay, any subsequent amendment law or amendment affecting

them."

式，其具有彈性的，同時賦予各歐盟會員國相當空間的，只要取得正面的回應即可，例如以聲明之方式，抑或是一句話或清楚表現同意之動作亦均能構成。至於網路上如何取得當事人之同意問題，「第 29 條工作小組」現正針對電子隱私權保護、電信行銷及網路 Cookie 之架構議題進行研議中，並將公布新的指引文件[7]。

3、 告知義務之實際效益及除外事由：

（１）一般個人資料保護規則草案並未再增加告知義務，而是著重於加強告知內容之品質，並使告知義務更加明確。履行告知義務的方式可以許多不同方式為之，例如只要提供詳盡之告知內容，即可對多數資料當事人以集體告知之方式為之，亦即不一定須逐一對個別資料當事人進行告知。因此，一般個人資料保護規則草案係在補充現行個人資料保護指令，並尋求更多解決辦法，藉由提供更完整格式內容，以協助產業履行告知義務（經評估，歐盟最常需踐行告知義務之產業為仲介經紀業者）。

（２）其次，針對告知義務中「告知資訊為不可行（provision of such information proves impossible）」或「需不合勞費（disproportionate effort）」等除外條款，適用上有許多可選擇方式，舉例而言，例如醫師或開業醫師無法與個別資料當事人取得聯繫時，可以將告知內容放置於等候室，以使病患於候診時知悉告知內容。

4、 關於「被遺忘權（Right to be forgotten）」之意涵：

一般個人資料保護規則規定之被遺忘權仍然維持個人資料保護指令之架構，並使一般民眾得以實現現行個人資料保護指令規定。而資料管理者留存個人資料應符合必要性及最小性等原則，如無留存

[7] 請參閱歐盟執行委員會第 29 條工作小組 WP 194 號指引文件 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf)

資料之必要時，應將資料予以刪除，並負擔使第三人刪除資料之責任。

5、 境外傳輸之規範：

（１）境外傳輸可以下列 2 種情況加以適用歐盟規範：其一，課與資料管理者義務，此為最主要途徑；其二，透過與歐盟簽訂個人資料執行協定，以茲適用，歐盟目前已經開始與歐盟以外之個人資料保護機關進行合作，例如對於 Google 之規範為例，歐盟已經與加拿大個人資料保護機關共同合作中。

（２）一般個人資料保護規則主要係透過共同約束條款（BCR）[8]方式課與資料管理者義務，目前歐盟與美國資料管理者及處理者之共同約束條款（BCR）已在運作。有部分會員國有集團訴訟之制度，但歐盟現行尚無集團訴訟規定，不過資料當事人仍可請求相關機構代為採取相關措施。

（３）另關於因應雲端科技之規劃方向，可以參考第 29 條工作小組針對運用雲端科技之 BCR 資料處理者所作的指引文件[9]。

6、 對於特種資料之變動方向，以及除外條款規定之「公共利益」範圍：

（１）利用個人資料進行醫學研究，係規範於一般個人資料保護規則第 81 條及第 82 條；利用個人資料進行學術研究，係規範於一般個人資料保護規則第 83 條。上開條款係適用於各種部門，而不限於學術、公部門或私部門，其範圍涵蓋基礎研究至商業研究。對於個人資料進行研究是一個非常敏感的領域，我們仍歡迎會員國對此進行討論。

（２）至於公共利益之範圍可能包括社會安全、稅務、國家安全及司法程序等均屬公共利益之範圍，但仍須依個案而定。

[8]「共同約束條款」（Binding Corp Rules，BCR）是指設立於歐盟會員國境內的個人資料管理者或處理者，在將一個或一組個人資料傳遞給企業集團內一個或多個第三國的管理人或處理人時，所遵循的個人資料保護政策。

[9]請參閱歐盟執行委員會第 29 條工作小組 WP 196 號指引文件 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf)

至於詳細的案例，我們提供相關書籍(即第 29 條工作小組第 13 次個人資料保護年報資料)供參。

7、 提供資料

歐盟並提供第 29 條工作小組第 13 次個人資料保護年報資料（英文版、法文版）供參。

（歐盟執行委員會提供第 29 條工作小組年報資料）

（本考察小組與歐盟執行委員會司法總署人員合影）

參、 考察比利時個人資料保護法制情形

一、比利時個人資料隱私權保護委員會之簡介

比利時個人資料隱私權保護委員會為聯邦層級之個人資料保護專責機關，於1984 年、1990 年、2003 年歷經多次變革及更名後，始改置為現有組織體制。目前比利時個人資料隱私權保護委員會已不受行政監督，僅須向議會負責，故已改制為獨立機關性質。目前比利時個人資料隱私權保護委員會為合議制機關，共有56 名正式人員（包括 1 名資訊專家及支援單位）。此外，該委員會下並設置有國家登記（7 名人員）、社會安全及健康（6 名人員）、銀行（6 名人員）、聯邦機關（6 名人員）、司法（6 名人員）、統計（6 名人員）等 6 個部門性質之委員會，以及 2 個任務編制單位。

二、考察情形

本考察小組於 101 年 6 月 11 日抵達比利時個人資料隱私權保護委員會，該委員會主席 Mr. Willem Debeuckolaere 協同公共關係官 Eva Wiertz 親自接見，並就本考察小組所提問題，回應如下：

1、 比利時個人資料隱私權保護法規特別揭示隱私權保護等文字，對於應保護之個人資料，是否亦有特殊之規範範圍？

（１）隱私權是一個概括、範圍較大之概念，而個人資料之保護是比較實務、範圍較小的概念。為了保護隱私權，必須考量個人資料的特別或一般因素，對於一般個人資料（例如姓名、地址）與敏感性資料（例如醫療、刑事紀錄）加以區別；因此，隱私權是較廣泛的概念，而個人資料可當作是實現隱私權保護的一個工具箱，是以，此二者間時常交互運作。

（２）依個人資料保護指令，各會員國可將其內化為內國法，但將來一般個人資料保護規則草案具有自動生效之性質，比利時必須完全遵守其規定。目前比利時個人資料隱私權保護法主要亦區分為一般個人資料及敏感性個人資料，原則

上任何人符合法律規定，均能蒐集、處理或利用一般個人資料，但對於敏感性個人資料，除非具有法律規定特定資格條件者外，例如醫療研究者、開業醫師、律師、法官、警察、稅務人員，則以禁止接近及使用為原則，且應依其個人資料類別適用個別法律之規定。

（３）對於敏感性資料而言(例如健康資料)，比利時個人資料隱私權保護法第 7 條以下有作一般性之規定，必須具有特定事由，以及特定職務或因工作上需要，始能蒐集、處理或利用健康資料，例如律師為了訴訟程序，而需確認資料當事人是否有精神上問題，此時律師雖非醫事人員，但仍得取得及處理相關健康資料。比利時個人資料隱私權保護委員會為界定符合上述職務之種類，亦有以荷蘭語及法語公布相關指引，以供參考。又私人公司如需運用健康資料時，首先必須取得病患之事前同意（Informed Concent），其次必須依循法定規定之組織，且必須具有研究的必要性。

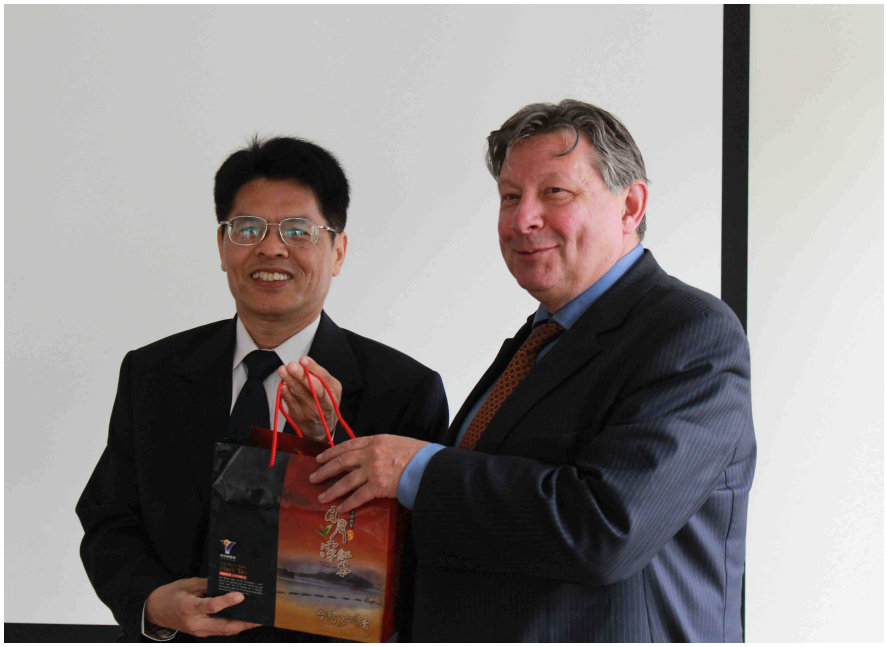
2、 有關取得當事人同意之方式，以及網路上之履行方法

比利時目前依循歐盟個人資料保護指令，但將來歐盟執行委員會所提出之一般個人資料保護規則通過後，可能會有更具體明確的規定。至於當事人同意是否一定需經其簽名，對此已有許多的討論，但目前較明確的是可以透過電子郵件或電子化方式為之，但仍需具有明確性要求。

3、 比利時適用告知義務之除外事由之標準，例如「告知資訊為不可行（provision of such information proves impossible）」或「需不合勞費（disproportionate effort）」

告知義務是所有資料蒐集者在處理個人資料前所應負之義務，在適用除外事由上，必須依個案判斷其需要，故比利時並未訂定一般性標準，舉例而言，郵務公司為了直銷而蒐集個人資料時，因資料當事人可能涵蓋許多國家，且國際上對於行銷並無一致性規定，故資料蒐集者無法逐一取得資料當事人同意時，必須免除對個人進行告

知之義務，僅能要求其以公開方式履行告知義務。



（本考察小組與比利時個人資料隱私權保護委員會主席合影）

（比利時個人資料隱私權保護委員會入口）

肆、 考察德國聯邦個人資料保護法制情形

一、德國聯邦資料保護及資訊自由委員會之簡介

德國聯邦個人資料保護法（Bundesdatenschutzgesetz （BDSG））最近一次的修法日為民國 98 年(西元 2009 年)8 月 14 日，並於同年 9 月 1 日起施行。除了聯邦層級之個人資料保護法外，德國在個別法上也制定了法律，尤其為因應網路的來臨，並分別制定公布通信服務個人資料保護法及電信通訊法（Telekommunikationsgesetz ，TKG）等個人資料保護之個別性法律。

德國聯邦為確保聯邦層級的個人資料保護單位（包括聯邦監察官、聯邦委員會）之獨立性，於民國 65 年(西元 1977 年) 依其個人資料保護法設置德國聯邦資料保護及資訊自由委員會。聯邦監察官由聯邦議會選任，可獨立執行職務並只應遵從法律，且配備擁有職員和預算的辦公室。

二、考察情形

本考察小組於 101 年 6 月 13 日抵達位於德國波昂之聯邦資料保護及資訊自由委員會，經參事兼任該委員會部門主管 Ms. Petra Wuttke-Götz、歐洲及國際關係事務高級參議 Dr. Heiko Haupt、發言人 Mr. Stefan Niederer、第一科參議 Dr. Jost Onstein、第三科 Mr. Dirk Hensel 等人代表接見，並就本考察小組所提問題，回應如下：

1、 德國聯邦對於公務機關、非公務機關之個人資料保護事項，設置於同一監管機關方式，其原因為何？優、缺點及成效如何？對於行政機關違反個人資料規定之處理方式為何？聯邦個人資料保護官（*DPO*）要求行政機關表明意見、勸告其改善或定期於活動報告書中公開之作法，其成效如何？

（１）參事兼任該委員會部門主管 Ms. Petra Wuttke-Götz 經詢問我國個人資料保護事務之分工架構後表示，德國聯邦個人資料保護單位為獨立機關，首長須至國會報告，並赴國外參加國際會議。第一科參議 Dr. Jost Onstein 並表示，德國聯邦是一個屋頂架構，聯邦憲法雖有政府制定，但各邦可

依憲法各自執行法律，因此德國各邦各別設置單獨單位，由各邦相關單位負責實際執行各邦個人資料保護事項。德國聯邦資料保護及資訊自由委員會係聯邦單位，成員來自各部會，與各邦資料保護單位之地位平等。國際會議則由聯邦資料保護及資訊自由委員會代表德國出席，但個人隱私則由各邦管理，各邦資料保護機關可獨立運作。至於資訊自由部分，亦為聯邦資料保護及資訊自由委員會所職掌。聯邦加上各邦共有 17 個主管個人資料保護事務機關，故須常協調並分析利害關係。

（２）為解決協調問題，目前聯邦及各邦一年召開 2 次會議[10]，由聯邦及各邦之 17 個個人資料保護主管機關協調改進及須增加或解釋事項，經該會議決議之事項，各邦均應遵守。因其協調時間較長會對企業造成困擾，此為缺點。至於詳細中央、地方分治事項之劃分，亦會於上開會議中進行討論。

（３）公司係由其總部所在地之資料保護機關負責管理，因此實務上有公司會找檢查密度較低之邦監管，但較不可能為了適用較寬鬆的規範，而特別請求適用特定較寬鬆規範標準的；實務上幾乎沒有公司會因為個人資料處理因素而遷移總部，最多係因為稅務關係而已。又對於特殊新興行業，例如臉書(facebook)，德國主要放在德國國內層次處理。但因其總部在愛爾蘭，尚須依愛爾蘭的規定處理，故仍涉及歐盟與各會員國之另一層次問題，因此各會員國仍在討論中。

（４）德國有 2 個不同制度，有公共資訊與非公共資訊，公共資訊須透明，個人資訊部分則有所限制。聯邦與各邦對於個人資訊之限制有些重疊，但有些則不同，如每個國民在各

[10] 據德國聯邦個人資料及資訊自由委員會會後提出說明，德國俗稱其為「杜塞道夫圈（Dusseldorf Circle）」。

邦都可能有儲存資料時，因此對其限制內容仍有在進行討論。但德國人民不希望政府有太多保有個人資料的職權範圍，因此個人資料保護指令制定時，對於可公開與不公開界限不清，我國對此亦提出疑問。政府資訊部分由聯邦以及 16 個邦負責，個人資料(包括公司機密)則由邦政府負責管理。當有公務部門違反規定時，德國目前僅對公務部門予以告誡，但實務上各機關亦會遵守，因此大致上而言，對於公務部門之告誡仍有其成效；對於非公務部門除告誡外，尚可處以較嚴之最高 30 萬歐元罰金，另外聯邦個人資料保護法雖定有 2 年以下自由刑或易科罰金規定，但目前實務尚未有刑事處罰或判決案例。

2、 德國保護個人資料之類型、範圍及相關個別法律

（１）於民國 99 年(西元 2010 年)間，德國對 Google 街景攝影案例之爭論很激烈，德國政府現已與 Google 達成協商，如果當地人民表示不接受街景攝影時，可向政府表達，政府將向 Google 提出要求。此外，Google 目前亦已於網站中設置相關管道，於民眾表示不要顯示其住家畫面時，即應將其住家畫面模糊。另政府也要求 Google 應將車子號碼及人的面孔要模糊處理，現 Google 已予以自動化處理。

（２）德國上開作法已成很多國家的規範，現在 Google 也知悉其應有限制，有些畫面不可明顯公開，所以 Google map 只公開德國 20 個城市街景。雖然德國亦不樂見只有 20 個大城市公開，但 Google 為此已增加 200 個員工來處理此事，並增加其成本。雖然只有 30%之德國人民其抗議 Google 街景車作法，但總數仍很多。經德國政府對 Google 要求相關作法後，抗議人民已有減少。但自另一方面思考，亦有認為適當公開有助於經濟發展，故 Google 的作法有助於商業利益，因此歐盟各會員國規範上並不完全一致。

（３）德國聯邦個人資料保護法雖有總則性規定，但對於相關機

構，例如如德國電信局，則有訂定個別規定，相關單位須遵守其個別規定並執行。以通訊、電話為例，因其涉及儲存個人資料，故依德國憲法規定，有關個資須予保護，德國爰以個別法予以規定，如個別法有疏漏，則再適用德國一般性法規定作為依據。目前德國有 12 個個別法規定，關於警察辦案、新聞媒體、稅務及社會福利等均有其個別法規定，且上開個別法規定與聯邦法的規定並無不合，均係與德國個人資料保護法互補。

3、 有關取得當事人同意之方式、標準，以及網路上之履行方法

（１）有關當事人書面同意之方式、標準，德國電信法第 94 條[11]有針對電子化同意而為特別規定，在其範圍內，可採用網路上同意作為書面同意。但對於涉及法律爭議案件原則不能以電子郵件取得同意，如須以電子郵件方式取得同意時，應將電子簽章方式告知資料當事人。如果個人希望與聯邦單位以電子郵件來往，可能必須經由一定程序以確認其電子郵件及身分，否則不能受理有其特別方式；又有些單位不受理以電子郵件來往。

（２）另外，對於網際網路社會衍生之跨境個人資料保護問題，例如 facebook 涉及個人資料時是否應依據愛爾蘭法規處理，德國對跨國境之個人資料保護問題已向歐盟提出研議之建議方案，其中包括企業總部不在歐盟時如何處理？如何遵守歐盟個人資料保護框架？如何避免歐盟各會員國之個人資料保護法規重疊？上開問題及德國建議內容亦將於歐洲議會於明年(2013 年)中列入討論。

---

[11] Section 94(**Consent by Electronic Means):"** Consent may also be given electronically where the service provider ensures that

1. the subscriber or user has given his consent deliberately and unequivocally;

2. consent is recorded;

3. the subscriber or user can access his declaration of consent at any time; and

4. the subscriber or user can withdraw his consent at any time with effect for the future."

4、 德國聯邦個人資料保護法第 9 條規定[12]「必要安全維護措施」意涵：首先，個人資料之處理可儘量予以去識別化、假名化方式處理。其次，德國聯邦個人資料保護法第 9 條係針對法定義務予以規範，但如何去作則非法律層次應解決問題；又個人資料檔案之保護與個人資料檔案安全亦屬二事，個人資料檔案保護功能係使個人資料不外洩之規範，德國聯邦雖然設有電腦處理資訊安全機構（BSI）[13]，但其僅為一輔助單位，協助達成檔案安全性作業問題，並不會要求全部資料蒐集者應通過一定安全標準，亦不會介入調查或處理。至於各政府機關、公司企業或行業應如何作到檔案安全，均有設置專人處理，即由專門負責檔案處理人員，負責保護檔案安全，且該專人並無規定一致資格條件，係依各行業實際需求，而訂定不同資格條件及具備專業知識，並不限於法律或資訊人員。而私部門發生一般檔案安全問題時，例如電腦當機或檔案遺失，應由其自行負責處理，政府僅在嚴重時才會予以罰鍰，但處罰其實不足以解決問題，重點仍應儘速陳報相關權責機關以尋求補救措施，而非隱匿實情，否則將來衍生後果會更嚴重。處罰不是目的，重點在於如何補教。

5、 關於德國聯邦個人資料保護法規定之「公共利益（*public interest*）」，德國實務上之判斷基準

（１）德國聯邦資料保護及資訊自由委員會 Dr. Jost Onstein 表示，自從接獲本考察小組所提本項問題後，即一直思考「公共利益」之判斷基準，並表示此問題非僅涉及德國聯邦個人資料保護*法（BDSG）*第 13 條第 2 項規定[14]，而係歐盟整體及個人資料保護指令第 8 條規定共同面臨問題，但有關公

[12] **Section 9 (Technical and organizational measures):"** Public and private bodies which collect, process or use personal data on their ownbehalf or on behalf of others shall take the necessary technical and organizationalmeasures to ensure the implementation of the provisions of this Act, especially therequirements listed in the Annex to this Act. Measures shall be necessary only if the effort required is in reasonable proportion to the desired purpose of protection.

[13] https://www.bsi.bund.de/EN/Home/home_node.html

[14] **Section 13 (Data collection):"** ….(2) Collecting special categories of personal data (Section 3 (9)) shall be lawful only where 1. allowed by law or urgently required for reasons of important public interest,……"

共利益，無論係法律規定或急迫情形，仍應該要有一定規則可循。

（２）然而，個人資料保護指令第 8 條之定義其實並不明確，因此常成為大家爭論之處。目前德國法律與歐盟規定不同，故願意在公共利益之認定上予以折衷，但如遇到歐盟規定與德國法律衝突時，德國之看法則認為除了非公開不可者可認為屬公共利益外，其餘仍應依德國法律行政，例如警察辦理刑事偵查案件、稅務案件，應屬不得公開範圍。其次，公共利益之概念容易遭到誤用，其應非涵括一切範圍，惟德國法律對於公共利益之定義，目前亦無明確規定，且無具體案例；因此，德國認為應遵守本國法律賦予之義務，再視具體情況而決定其標準，例如提供飛機空難旅客名單是否界定為公共利益，仍由各會員國自行決定。又參照德國聯邦資訊自由法規定，公共利益可能主要包含國家安全、公共安全等概念，且上開法規並對國家安全概念有進一步闡述。但縱使德國法律有上開規定，其他歐盟國家可能並無此規定，故歐盟各會員國對於公共利益的解讀有所不同，認知上仍有出入（例如天然災害、稅務）。

6、 提供資料：

德國聯邦資料保護及資訊自由委員會提供「德國聯邦個人資料保護法文本及解釋彙編（說明資訊第 1 冊）」、「德國聯邦資訊自由法文本及解釋彙編（說明資訊第 2 冊）」、「社會資訊保護-權利之確保（說明資訊第 3 冊）」、「德國聯邦資料保護及資訊自由委員會之運作（說明資訊第 4 冊）」、「2009 年至 2010 年個人資料保護之進展報告」等文件供參。

（德國聯邦資料保護及資訊自由委員會資料）

（本考察小組與德國聯邦資料保護及資訊自由委員會代表人員合影）

（本考察小組於德國聯邦資料保護及資訊自由委員會入口合影）

伍、 考察德國巴伐利亞邦個人資料保護法制情形

一、德國巴伐利亞邦個人資料保護委員會之簡介

巴伐利亞邦為德國面積第一大邦、人口第二大邦，總人口約有 1 千 2 百餘萬人，屬德國各邦中高度經濟發展地區。巴伐利亞邦為推動個人資料保護事務，設置有巴伐利亞邦個人資料保護委員會、個人資料保護督察官辦公室等 2 個專責機關，其中巴伐利亞邦個人資料保護委員會負責監管公務機關之個人資料保護業務，而巴伐利亞邦個人資料保護督察官辦公室負責監管非公務機關之個人資料保護業務。

二、考察情形

本考察小組於 101 年 6 月 15 日抵達位於德國慕尼黑之巴伐利亞邦個人資料保護委員會，該委員會主席 Dr. Thomas Petri, Vita 親自接見，並就本考察小組所提問題，回應如下：

1、 德國巴伐利亞邦個人資料保護委員會基本概況：

德國巴伐利亞邦個人資料保護委員會係依巴伐利亞邦憲法設置的憲法機關，首長由邦國會選出，任期 6 年，連選得連任。德國巴伐利亞邦個人資料保護委員會為獨立機關，不受行政管理，最多僅受法院監督。機關編制共有 30 名員工，其中 25 人為正式人員（包含 20 名業務單位人員及 5 名資訊技術人員）、5 人為聘僱人員。本年(2012 年)度機關預算 150 萬歐元，明年(2013 年)度預期將大幅增加至 200 萬歐元，增加之目的主要係為進行巴伐利亞邦的個人資料保護改革，而須增加教育訓練費用，同時也改革薪資，提高員工待遇。德國巴伐利亞邦個人資料保護委員會委員會主席 Dr. Thomas Petri, Vita 對於該邦國會通過上開改革提案，同時表示肯定。

2、 巴伐利亞邦目前分設不同監管機關原因、程序及成效：

（１）巴伐利亞邦目前監管個人資料保護事務係依監管公務機

關、監管非公務機關之業務分設 2 個專責機關，早年巴伐利亞邦個人資料保護機關均隸屬邦之下，且監管非公務機關之專責機關係隸屬於內政部之下。惟因歐洲法院於 2010 年判決，個人資料保護機關設於內政部下有違個人資料保護專責機關之獨立性要求，所以目前巴伐利亞邦之 2 個個人資料保護機關均已獨立設置，不再隸屬邦或內政部之下，具有獨立行使職權之獨立機關性質。

（２）又德國各邦則多自內政部獨立設置 1 個專責機關管理，但巴伐利邦因係德國境內經濟發展程度較高之邦，復考量如欲加以整合，除需修改巴伐利亞邦憲法規定，且 2 個機關在不同地點，合併將耗費過鉅，且影響當地發展，因此成立 2 個獨立行使職權之專責機關進行監管。

（３）巴伐利亞邦分別設置 2 個個人資料保護專責機關之缺點在於，對於部分具有公部門性質單位之適用上容易產生爭議，例如醫院涉及公部分及私部分。分設 2 個監管機關之處理模式是否合理，此屬於議會層次問題。又巴伐利亞邦法律雖已明定上開區分方式，但在具體個案上仍有解釋空間，故有意見不同之風險，只能透過不斷溝通加以解決；因此，遇有爭議時會儘量與另一機關首長交互溝通解決。基本上公務機關本應依法行政，因此監管公務機關之規範較嚴謹；而私部門為私權利主體，較注重私權利的維護，故監管私部門所要求標準相對於監管公務機關之規範較寬鬆，但如非公務機關受公務機關委託，則於委託範圍內仍屬公務機關。

（４）依據巴伐利亞邦個人資料保護法第 3 條規定[15]，受何監管機

[15] Art. 3:“Öffentliche Stellen, die am Wettbewerb teilnehmen
(1) 1 Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten für sie sowie für ihre Zusammenschlüsse und Verbände die Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts. 2 Art. 2 Abs. 7 bleibt unberührt. 3 Für die Durchführung und die Kontrolle des Datenschutzes gelten an Stelle der §§ 4d bis 4g und 38 des Bundesdatenschutzgesetzes die Art. 9 und 25 bis 33.
(2) 1 Soweit öffentlich-rechtliche Versicherungsunternehmen am Wettbewerb teilnehmen, gelten für sie

關管轄，係以個人資料蒐集者之組織性質加以區分，設置於公部門下即由個人資料保護委員會監管，設置於私部門者即由個人資料保護督察官辦公室監管，例如公立醫院財源上受有公部門的補助，且與私立醫院有競爭關係，但組織上仍隸屬於公部門，故屬個人資料保護委員會管轄範圍；又如巴伐利亞邦境內水力公司有些是由公部門經營，有些是由私部門經營，為免其區分困難，仍以其組織加以區分。但此有 2 個例外，公營銀行及保險公司，則由非公務機關管理，理由係因其部分業務內容雖然可能涉及公權力，但其餘經營內容與私營銀行或私營保險公司並無不同，故歸屬為非公務機關。復因公營銀行早期多係配合政府政策從事貸款或補助事業，然而目前其任務功能已不存在，例如具信用合作社性質之 StadtBank 早年具有扶助地區農民性質，惟現今其公益目的幾已不復存在；復因該等銀行早期雖有公務員，可是目前均已屬僱傭關係，故已屬私部門性質；是以，其營業與私人銀行並無差異，爰將其歸類為非公務機關。

（５）德國各邦雖可認定境內單位屬公務機關或非公務機關，以機場公司為例，柏林邦認為機場屬非公務機關，巴伐利亞邦、黑森邦則認屬公務機關。其中尤其從事基本生存照顧業務之事業爭論尤大。但針對上開案例，德國目前已透過各邦每年召開 2 次邦層級會議加以協調，並由各邦輪流擔任主席職務，目前上開案例均已取得共識認屬非公務機關，故將來再產生相同爭議之機會不大。

（６）公務機關違反個人資料保護法時，可予以告誡；私部門違

---

die Vorschriften des Bundesdatenschutzgesetzes, die auf privatrechtliche Versicherungsunternehmen anzuwenden sind. 2 Für öffentlich-rechtliche Kreditinstitute sowie für ihre Zusammenschlüsse und Verbände gelten die Vorschriften des Bundesdatenschutzgesetzes, die auf privatrechtliche Kreditinstitute anzuwenden sind. 3 Art. 2 Abs. 7 bleibt unberührt.
(3) Die Anstalt für Kommunale Datenverarbeitung in Bayern unterliegt den Vorschriften dieses Gesetzes auch, soweit sie am Wettbewerb teilnimmt.“

反個人資料保護法時，可予罰鍰。至於刑事上，雖然對於意圖營利而違反個人資料法者，定有 2 年以下有期徒刑，但此類案件非常少，目前巴伐利亞邦僅有 1 件疑似案件（最終亦未依個人資料保護法規處以刑罰），但其涉及刑罰主要係因其行為本身即已構成刑事犯罪案件，而非係因違反個人資料保護法規部分。

（７）另外，德國各邦個人資料保護法規仍有不同寬鬆程度情形，例如曾發生一個案件，社會福利團體向郵務公司蒐集郵票，但郵務公司將涉及當事人姓名及地址資料之整個信封交付；於此案例中，柏林個人資料保護法規之刑罰規定與巴伐利亞邦相較，柏林規定較嚴，柏林於蒐集時即可處罰，而巴伐利亞邦須至利用時始可處罰。

3、 個人資料保護委員會與資料保護督察官辦公室之合作模式：

對於私部門與公部門管理不同，私部門係為營利，如有違反則處以罰金，但公部門則非營利，因此無罰金之處罰，但會向該機關之上級機關報告或透過法律。因此區分 2 個機關管理，差別僅在監管方式不同，實際上管理並無差異，但公部門因需依法行政，因此管理公部門的效率較好，監管標準亦較高。但在個案上仍會面臨疑議，此時必須由雙方機關首長相互溝通解決，以尋求共識。

4、 德國聯邦及巴伐利亞邦對於個人資料保護法有何差異？例如巴伐利亞邦對於特種資料有無特別規定：

（１）有關德國聯邦與巴伐利亞邦個人資料保護法之差異，主要係因 2007 年至 2008 年間德國發生很多因個人資料外洩所衍生之詐欺案件，故德國聯邦個人資料保護法律於 2010 年間有大幅度修正，其中修正內容主要係因應新科技之發展。相較之下，巴伐利亞邦個人資料保護法 20 年來並未修法，亦未對於電子科技特別規範，故其缺乏新穎性及新科技之考量，此為其缺點。但整體而言，巴伐利亞邦個人資料保護法迄今並無適用上疑義，顯示其規範內容相當穩

定，此為其優點。其次，巴伐利亞邦個人資料保護法有一特色，即於第 26 條[16]規定公務機關應有審核機制，公務機關於首次蒐集資料前應由專人事先審核，經專人認定符合相關規範後，公務機關始可蒐集、處理或利用個人資料並建立資料庫。但蒐集前經當事人事先同意者，則上開事先審核機制則可免除，聯邦的規定並無事先審核程序及法律效果之強制規定，因此難以得知是否已經專人事先審核。

（２）關於健康醫療資訊部分，巴伐利亞邦之公務機關須透過上開事先審核程序後始可蒐集；至於私部門雖然無上開專人審核機制，但德國聯邦個人資料保護法第 28 條第 6 項至第 9 項規定已有嚴格規範。亦包括醫療之個別性法律

5、 巴伐利亞邦個人資料保護法有關取得當事人同意之方式：

---

[16] Art. 26[1] Datenschutzrechtliche Freigabe automatisierter Verfahren
(1) 1Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf der vorherigen schriftlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle. 2Eine datenschutzrechtliche Freigabe nach Satz 1 ist nicht erforderlich für Verfahren, welche durch den Vorstand der Anstalt für Kommunale Datenverarbeitung in Bayern bereits datenschutzrechtlich freigegeben worden sind, soweit diese Verfahren unverändert übernommen werden; das Gleiche gilt bei öffentlichen Stellen des Freistaates Bayern für Verfahren, welche durch das fachlich zuständige Staatsministerium oder die von ihm ermächtigte öffentliche Stelle für den landesweiten Einsatz datenschutzrechtlich freigegeben worden sind. 3Für wesentliche Änderungen von Verfahren gelten die Sätze 1 und 2 entsprechend.
(2) Die datenschutzrechtliche Freigabe hat folgende Angaben zu enthalten:
1.Bezeichnung des Verfahrens,
2.Zweck und Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung,
3.Art der gespeicherten Daten,
4. Kreis der Betroffenen,
5.Art der regelmäßig zu übermittelnden Daten und deren Empfänger,
6.Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung,
7.verarbeitungs- und nutzungsberechtigte Personengruppen,
8.im Fall des Art. 6 Abs. 1 bis 3 die Auftragnehmer,
9.Empfänger vorgesehener Datenübermittlungen in Drittländer.
(3) 1Öffentliche Stellen haben ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens eine Verfahrensbeschreibung mit den in Absatz 2 aufgeführten Angaben zur Verfügung zu stellen; zugleich ist eine allgemeine Beschreibung der Art der für das Verfahren eingesetzten Datenverarbeitungsanlagen und der technischen und organisatorischen Maßnahmen nach Art. 7 und 8 beizugeben. 2Die behördlichen Datenschutzbeauftragten erteilen die datenschutzrechtliche Freigabe, soweit nicht schon eine datenschutzrechtliche Freigabe nach Absatz 1 Sätze 2 und 3 vorliegt. 3Wird ihren datenschutzrechtlichen Einwendungen nicht Rechnung getragen, so legen sie die Entscheidung über die datenschutzrechtliche Freigabe den Personen vor, denen sie nach Art. 25 Abs. 3 Satz 1 unterstellt sind; bei den in Art. 15 Abs. 7 genannten Daten haben sie zuvor eine Stellungnahme des Landesbeauftragten für den Datenschutz einzuholen.

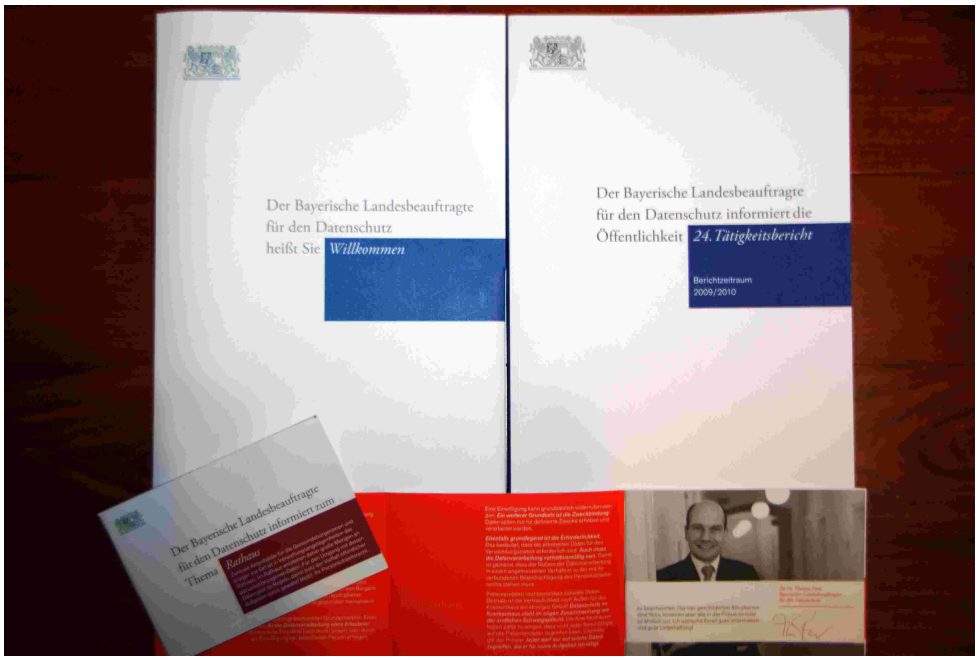
雖然巴伐利亞邦個人資料保護法規定同意須以書面為之，但解釋上仍可由電子郵件方式同意，惟郵件上須有電子簽章的簽名。

6、 巴伐利亞邦個人資料保護法規定之「公共利益（*public interest*）」，實務上判斷基準或具體案例：

巴伐利亞邦對於公共利益並無一致性規定，端視其是否符合公共安全而定。依據基本法規定，只要涉及侵犯人民基本權者，本應有法律規定，而個人資料保護係聯邦憲法規定之基本權，故蒐集個人資料必須有法律規定，因此無需於個人資料保護法中再明確定義或規範公共利益；是以，實以難想像有必須適用個人資料保護法上公共利益條款之案例。至於德國立法時所定公共利益之除外條款，其立法理由僅係為保留一定彈性空間。又新聞自由是否即屬公共利益？如何適用個人資料保護法問題？因新聞自由亦屬聯邦憲法規定之基本權，故此涉及新聞自由與人格權衝突問題，仍應衡酌其利益。此外，亦有新聞法之個別法律，針對此類之個人資料有特別保護的規範。

7、 提供資料：

德國巴伐利亞邦個人資料保護委員會除提供「2009 年至 2010 年巴伐利亞邦公務部門個人資料保護之進展報告」外，並臚列德國個人資料保護註釋書、教科書及案例彙編等目錄供參。



（巴伐利亞邦個人資料保護委員會除提供資料）

（本考察小組與巴伐利亞邦個人資料保護委員會主席合影）

陸、心得及建議

一、個人資料類別：

個人資料保護指令與一般個人資料保護規則所規範所保護個人資料之類別並無不同，可識別或足資識別之個人資料均為保護對象。但歐盟各會員國對於個人資料類別之規範範圍，仍因各國國情不同而有些許差異，例如德國即認為 google map 街景攝影所蒐集之資料應屬個人資料，並僅能公開部分城市之街景資料。其次，歐盟規劃制定一般個人資料保護規則之目的，係在促使歐盟有一致性規範，但為避免國家過度介入個人及家庭生活，並避免過度干預新聞、藝術或文學領域，故於特定領域中，仍給予各歐盟會員國自行規範空間，可依不同的社會基準，再作有不同類型的規範或解釋適用。因此，將來我國修正個人資料保護法規時，亦可依我國社會國情，再行整體檢視及思考我國立法政策上應予保護個人資料之範圍。

二、告知義務內涵：

雖然歐盟各會員國目前對於告知義務之規範並不完全一致，歐盟執行委員會司法總署第 29 條工作小組亦曾對於告知義務所需耗費之成本及實際效益提出質疑，但觀察一般個人資料保護規則草案，歐盟未來立法趨勢仍應維持告知義務，並將加強對於告知義務之內容及品質。至於符合一般個人資料保護規則草案第 14 條規定之告知義務除外條款時（例如「告知資訊為不可行（provision of such information proves impossible）」或「需不合勞費（disproportionate effort）等條款），無論歐盟執行委員會司法總署、比利時個人資料隱私權保護委員會（比利時現行個人資料隱私權保護法已有類似「告知資訊為不可行」或「需不合勞費除外」等除外條款之規定），均表示此時係指資料蒐集者並無法逐一取得資料當事人同意之情形，但仍要求以公開或公布於營業場所等方式進行告知，因此歐盟似認為符合告知義務之除外條款時，雖然無庸逐一對資料當事人進行告知，但仍應以資料當事人可得知之方式予以公告相關內容。惟因一般個人資料保護規則草案尚未

正式通過，因此歐盟將來實務上如何解釋或適用告知義務之除外條款，仍然值得觀察，以作為我國修正個人資料法規之參考。

三、符合當事人同意之要件：

有關當事人同意之方式，我國個人資料保護法雖然參照德國聯邦個人資料保護法規定，必須以書面同意方式為之；但德國為因應網路及電子化科技之發展，已於電信法第 94 條即有針對電子化同意而為特別規定，因此，德國聯邦對於取得當事人書面同意之方式，已透過個別法規定，於個別領域中予以適度放寬，仍可以網路或其他電子方式，藉由電子簽證之電子郵件，或其他可確認身分之電子郵件取得當事人之同意。但如涉及法律爭議案件時，原則仍不得以電子郵件取得同意，例外如須以電子郵件方式取得同意之必要時，則應將電子簽章方式告知資料當事人。

我國目前已規劃於個人資料保護法施行細則中明定，個人資料保護法所定書面意思表示之方式，得依電子簽章法之規定，以電子文件為之，其目的亦在解決相同之問題，其解釋上亦儘量朝向具有彈性之作法。但對於本次考察過程中，歐盟一再強調應將重點著重於取得同意之品質，德國並設有個別法律，據以規範個別領域中以電子化方式取得當事人同意之要件；對此，我國將來研議修正個人資料保護法或相關個別法律時，應可將上開立法模式及解釋方式列入參考依據，以對當事人同意之內涵作更細緻化之規範。

四、公共利益之適用範圍：

有關個人資料保護之一般性法規所稱之「公共利益」，無論歐盟、比利時、德國聯邦或德國巴伐利亞邦均無法明確定義。又有關其適用範圍或案例上，本次考察對象主要區分為下列幾種意見：

（一）較廣之適用範圍：

公共利益之範圍可能包括國家安全、社會安全、稅務、及司法程序範圍，但不限於此。（歐盟執行委員會）

（二）較狹之適用範圍：

> 個人資料涉及人民基本權利，本應以法律定之，因此此種條款之立法目的係在保留彈性，實務上幾乎無適用之案例。但參照德國相關法律，解釋上個人資料保護法規所稱之公共利益可能主要包含國家安全、公共安全等範圍。至於涉及個別法律時（例如稅務、警察之刑事偵查程序、天然災害），是否可否援用公共利益之條款，則持較保留態度。（德國聯邦資料保護及資訊自由委員會、巴伐利亞邦個人資料保護）

雖然歐盟內部對於公共利益的解讀仍有所不同，對其範圍之認知上仍有出入，但基本上歐盟適用公共利益條款之案例情形似乎有限，甚至德國實務上顯少有適用餘地，可能因其相關個別法規已針對個別情形予以明確規範，致無須再回歸適用一般性法律之概括規定，此值得作為我國將來個別法律修正時之參考。因此，將來我國界定公共利益範圍時，建議可思考方向有二：（一）審慎解釋，逐步於個案中累積經驗，確認我國可接受之範圍。（二）針對個別領域，具體明確訂定適用情形，澈底避免爭議。

五、境外個人資料保護機制：

歐盟對於境外個人資料保護之規範機制，尤其針對決新興行業（例如雲端科技）所衍生個人資料保護蒐集、處理或利用行為態樣，如何加以規範並落實對於歐盟人民權益之保護，此對於歐盟或各會員國而言，亦為一困難且仍在研議中之課題；而歐盟現階段主要係透過簽訂國際協定，以及於契約中要求納入共同約束條款（BCR）等方式，對於境外資料管理者或處理者課予遵守歐盟個人資料保護指令或政策之義務，實務上歐盟與美國之資料管理者或處理者，亦已開始運用此一共同約束條款（BCR）制度。我國個人資料保護法制是否可參採歐盟上開制度？如採用後可發揮之效益多大？此或可作為賡續研議之方向。然而在國際上或我國研議有效之個人資料境外保護機制前，無法避免的是，我國個人資料保護法制必須持續參考國際上主要國家立法趨勢，適時修正我國個人資料保護法，以使我國個人

資料保護規範能與國際接軌，避免我國法制與國際上立法趨勢如發生扞格時，可能進而影響我國境內合理運用個人資料之範圍。

六、組織面：

本次考察過程中，歐盟及相關國家之個人資料保護機關甚為強調個人資料保護主管機關之獨立性。對此，歐洲法院甚至曾針對德國個人資料保護主管機關之獨立性提出質疑作出判決，因而促使德國重新定位個人資料保護主管機關。

鑑於我國目前係由各中央目的事業主管機關分別負責個人資料保護事項，尚未採用專責機關模式，因此本次考察亦針對巴伐利亞邦成立 2 個個人資料保護獨立專責機關之實務運作經驗進行觀察，該邦囿於巴伐利亞邦憲法因素，向來係就公務部門、非公務部門分別設置 2 個獨立專責機關，故其多個監管機關之運作模式應較為成熟且具經驗，惟其實務上仍難以避免界定困難情形，必須經常透過首長相互聯繫以取得共識。是以，將來我國擴大施行個人資料保護法後，各目的事業主管機關如何在執行上取得共識，以及在監管上相互配合，實為我國將來應予重視之課題。

附　錄

附錄一、考察項目中外文譯本

法務部 101 年考察歐盟（General Data Protection Regulation）之規劃與實施情形擬提問題

Prepared Questions in the Planning and Implementation of EU General Data Protection Regulation for 2012 Ministry of Justice Delegation to EU

壹、前言

I. Foreword

中華民國（臺灣）於民國 84 年 8 月 11 日公布施行電腦處理個人資料保護法。又為加強對於個人資料之保護，參考 1995 年歐盟資料保護指令（*95/46/EC*），於民國 99 年 5 月 26 日修正公布個人資料保護法。中華民國（臺灣）新修正之個人資料保護法共分為「總則」、「公務機關對個人料之蒐集、處理及利用」、「非公務機關對個人料之蒐集、處理及利用」、「損害賠償及團體訴訟」、「罰則」、「附則」等 6 章，條文共計 56 條。

（http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021）

In August 11, 1995, the Republic of China (Taiwan) promulgated and enforced Computer Matching and Privacy Protection Amendments Act. In order to further strengthen protection to personal information, the Republic of China (Taiwan), taking reference of 95/46/EC, revised the above-mentioned act and promulgated Personal Information Protection Act. The newly revised act of Republic of China (Taiwan) is divided into 6 chapters, namely“General Provisions,” “ Collection, Disposal, and Use of Personal Information by Government Organs,” “Collection, Disposal, and Use of Personal Information by Non-Government Organs,” “Compensation for Loss and Group Lawsuit,” “ Penalties,”and

“Supplementary Provisions,”with a total of 56 articles.

（http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021）

為瞭解歐盟、德國目前個人資料保護之實務運作狀況，以及將來配合一般個人資料保護規則修正草案（*General Data Protection Regulation*）之相關措施，乃有本次考察活動，詳細欲詢問之問題如下：

In order to understand the current actual workings of European Union (EU) and Germany in the field of personal information protection and with the intention of being in line with the upcoming 2012 General Data Protection Regulation of EU, the Ministry of Justice has organized this visit to EU and Germany. The following are questions to be raised by the delegation:

貳、訪問歐盟執行委員會（法律部門）(*European Commission Department of Justice*）之問題：

II. Questions to European Commission Department of Justice:

1、 歐盟各會員國對於應保護之個人資料，在類型上有無不同？歐盟規劃應立法保護或排除保護個人資料時，其主要考量因素或相關背景為何？例如：歐盟對於自然人之個人或家庭活動中所為個人資料，規劃限縮至「需受有任何報酬利益（*without any gainful interest*）」為限，以及針對新聞、藝術或文學表達之目的，授權各會員國免除或放寬相關規定，其原因或所欲解決之問題為何？

1. What are the differences in measures of various EU member countries regarding personal information to be protected? What are the major factors or relevant background information being considered when EU plans to legislate to protect or refrain from protecting personal information? For example, EU’s plan to restrict personal information of individual or family activities of natural

person to the realm of “without any gainful interest;” EU’s relevant regulations to keep its member countries free from or relieved from part of, the regulations in order to achieve the purpose of expression of journalism, arts, and literature. What are the reasons and problems to be solved which are brought to attention by the said examples?

2、有關一般個人資料保護規則草案規定之「同意」，取得同意之方式與標準為何？其中第 8 條處理兒童資料所應取得其父母或監護人同意與其他條款取得同意之規定，其方法、標準，是否不同；又如係透過網際網路或其他方式取得同意時，如何實踐相關規定？是否有取得證實同意方法之標準格式或相關資料可供參考？

2. Regarding “agreement” stipulated in the draft of the 2012 EU regulations on information protection for ordinary people, what are the approaches and criteria to reach under an agreement? Regarding Article 8, which stipulates that consents by parents or guardians are required when handling information of children, or other articles with similar requirement of such consents, what are the differences in approaches or criteria when comparing content of the said articles? In addition, when seeking such consents through the Internet or other means, please tell us how to implement the said regulations? Are there standard patterns for obtaining verified consents or other relevant information available for our reference?

3、鑑於一般個人資料保護規則草案已就「告知義務（*notification*）」予以規定，以使各會員國能有一致性規範。惟歐盟評估告知義務之實效性如何？如何使各會員國在適用除外事由時能有一致性結果，例如如何具體適用「告知資訊為不可行（*provision of such information proves impossible*）」或「需不合勞費（*disproportionate effort*）」

等事由。

3. We understand that the draft of the EU regulations on information protection for ordinary people has already specified the rules of "informing obligation" aimed at achieving a unified rule among its member countries. However, what is the actual effect in the implementation of informing obligation in EU"s evaluation? How to ensure that various member countries can have a common result in the application of extraordinary reasons? (for example, how to actually concretely apply affairs such as "*provision of such information proves impossible*" or "*disproportionate effort* ")

4、關於「被遺忘權（*Right to be forgotten*）」，資料管理者所應負擔責任之範圍及應採取措施為何？於資料管理者已授權第三人公開該個人資料之情形，資料管理者之責任是否限於應通知該第三人刪除相關連結、影本或備份外，抑或尚須採取其他相關措施？

4. Regarding "*Right to be forgotten,*" what is the realm of responsibility of, and measures to be taken by, a data manager? On the condition that the data manager has authorized a third person to make public personal information, what is the data manager's realm of responsibility: Is it limited to informing the third person to delete relevant links, photocopies or copies? Are there other relevant measures to be taken?

5、歐盟一般個人資料保護規則草案擴大適用於境外蒐集資料者（*data controller*）後，如何確保當事人對於境外蒐集資料者行使相關權利（例如查詢權權利（*Right of access for the data subject*））？除了共同約束條款（*Binding Corporation Rules*）之民事上機制外，是否尚有其他行政上或訴訟上機制，例如處罰境外公司規定或代表起訴？因應雲端科技之發展，是否有任何規劃方向？

5. After the draft of the EU regulations on information protection for ordinary people is expanded to apply foreign data controller, how to ensure that the person(s) concerned exercises relevant rights on foreign data controllers (for example, right of access for the data subject)? Except for binding corporation rules（BCR） in the civil affairs mechanism, are there other administrative and law-suit mechanisms (for example, regulations to punish foreign companies or prosecute company representatives)? To cope with the development of cloud computing technology, is there any plan or direction on the drawing board?

6、一般個人資料保護規則針對特種資料之規劃有何新變動？一般個人資料保護規則第 9 條(g)為增進公共利益所進行之必要資料處理（*processing is necessary for the performance of a task carried out in the public interest*）之規定，應如何定義其中所稱「公共利益（*public interest*）」或界定其範圍，就其不確定之法律概念，有無具體案例可供參考？

6. What are the changes in the planning of the 2012 EU regulations on information protection for ordinary people? Article 9 (g) of the said regulations contains rules for processing necessary for the performance of a task carried out in the public interest. How to define “public interest” and its realm? Regarding its unstable legal concept, are there concrete cases for our reference?

7、請協助提供實務有關歐盟執行委員會（含第 29 條工作小組）執行業務相關注意事項或手冊，以供我國行政實務之參考；並推薦值得購買之個人資料保護業務相關專業書籍（*handbook & casebook*）之名稱與出版社。

7. Please kindly provide relevant notes or handbooks on actual

business execution of European Commission (including task force stipulated in Article 29) for the reference of Taiwan in actual administration affairs. Please also provide names and publishing houses of recommended books (handbook and casebook) related to the business for personal information protection.

規劃與實施情形擬提問題

Planung und Ausführung für die sowie die voraussichtlichen Fragen bei der Vorortuntersuchung des Bundesdatenschutzgesetzes （BDSG）des taiwanesischen Justizministeriums im Jahr 2012

壹、前言

I. Vorwort

中華民國（臺灣）於民國 84 年 8 月 11 日公布施行電腦處理個人資料保護法。又為加強對於個人資料之保護，參考 1995 年歐盟資料保護指令（*95/46/EC*），於民國 99 年 5 月 26 日修正公布個人資料保護法。中華民國（臺灣）新修正之個人資料保護法共分為「總則」、「公務機關對個人料之蒐集、處理及利用」、「非公務機關對個人料之蒐集、處理及利用」、「損害賠償及團體訴訟」、「罰則」、「附則」等 6 章，條文共計 56 條。

（http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021）

Taiwans Regierung hat das Datenschutzgesetz hinsichtlich der Verarbeitung der persönlichen Daten mit Computer am 11. August 1995 veröffentlicht und gleichzeitig in Kraft gesetzt. Um den Schutz der persönlich bezogenen Daten zu verbessern, wird die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 (der Richtlinie) als Referenz herangezogen und das Datenschutzgesetz am 26. Mai 2010 abgeändert und veröffentlicht. Die neue Fassung des Taiwanesischen Datenschutzgesetzes umfasst „Allgemeine Grundsätze “, „Erhebung, Verarbeitung und Nutzung der persönlichen Daten durch die Behörden und die öffentlichen Organe bzw. Institutionen “, „Erhebung, Verarbeitung und Nutzung der persönlichen Daten durch Nicht-öffentliche Organe und Institutionen “, „Schadenersatz und Gruppenprozess “, „Strafe “ und „Anhang “; insgesamt 6 Kapitel und 56 Paragrafen.

（http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021）

為瞭解歐盟、德國目前個人資料保護之實務運作狀況，以及德國將來配合一般個人資料保護規則修正草案（*General Data Protection Regulation*）之相關措施，乃有本次考察活動，詳細欲詢問之問題如下：

Um die praktische Ausführung des Datenschutzgesetzes und die relevanten Maßnahmen zur Änderungen der Allgemeinen Europäischen Datenschutzverordnung in der EU und in Deutschland näher zu verstehen, werden dieser Besuch und die Vorortuntersuchung geplant und voraussichtlich die folgenden Fragen gestellt.

貳、訪問德國聯邦資料保護與資訊自由辦公室（BFDI，The Office of the Federal Commissioner for Data Protection and Freedom of Information）之問題：

II. Frage, die voraussichtlich dem Amt des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gestellt werden:

一、 多數邦對於公務機關、非公務機關之個人資料保護事項，分別設置不同之監管機關，而不採用聯邦設置於同一監管機關方式，其原因為何？優、缺點及成效如何？對於行政機關違反個人資料規定之處理方式為何？聯邦個人資料保護官（*DPO*）要求行政機關表明意見、勸告其改善或定期於活動報告書中公開之作法，其成效如何？

1. Der persönliche Datenschutz bezüglich der öffentlichen und Nicht-öffentliche Behörden bzw. Organen wie Institutionen wird in Mehrheit der Länder von unterschiedlichen Aufsichtsbehörden beaufsichtigt. Was ist der Grund, dass diese Angelegenheit nicht wie beim Bund von einer Behörde beaufsichtigt wird? Was ist der Vor- und Nachteil dieser Arbeitsteilung und wie effektiv ist mit dieser Arbeitsaufteilung? Wie wird behandelt, wenn die öffentlichen Behörden bzw. Organen wie Institutionen gegen die Vorschriften des Datenschutzgesetzes verstoßen haben? Wie effektiv ist das Verfahren,

dass der Bundesdatenschutzbeauftragte die Stellungnahme der öffentlichen Behörden bzw. Organen wie Institutionen verlangt und er die Verbesserung riet oder er regelmäßige Aktivitätsberichte veröffentlicht?

二、 德國對於應保護之個人資料，在類型上與歐盟其他國家相較，是否有較具特色規定（例如德國電信通訊法(TKG)如何與德國聯邦個人資料保護法（BDSG）配合運作），其立法保護或排除保護個人資料之主要考量或相關背景為何？又將來如何因應一般個人資料保護規則相關規定，例如：歐盟對於自然人之個人或家庭活動中所為個人資料，規劃限縮至「需受有任何報酬利益（*without any gainful interest*）」為限，以及針對新聞、藝術或文學表達之目的，授權各會員國免除或放寬相關規定，德國將來規劃方向為何？

2. Gibt es beim deutschen Datenschutzgesetz in Bezug auf die Typen Besonderheiten im Vergleich zu anderen europäischen Ländern (wie z. B. wie können sich das deutsche Telekommunikationsgesetz (TKG) und das Deutschen Bundesdatenschutzgesetz (BDSG) miteinander zusammen anpassen und ausgeführt werden. Was ist der Hintergrund und Hauptüberlegung der Gesetzgebung dafür, dass die persönlichen Daten geschützt oder nicht geschützt werden. Wie werden in Zukunft ab 2012 die relevanten Bestimmungen der Regeln des allgemeinen personenbezogenen Datenschutzes angepasst, z.B. EU hat geplant, die persönlichen Daten der natürlichen Person oder die persönlichen Daten in der familiären Aktivitäten auf „ ohne jegliches gewinnbringendes Interesse“ zu beschränken, und die Mitgliedsstaaten zu bevollmächtigen, die Bestimmungen des Schutzes der persönlichen Daten, die zum Zweck der/des journalistischen, künstlerischen und literarischen Darstellung

bzw. Ausdruckes zu befreien oder zu lockern. Wie passt Deutschland sich dies in der Zukunft an?

三、 德國聯邦個人資料保護法（*BDSG*）第 4 條(a)關於書面同意之規定，如何適用於網際網路世界？將來如何因應網際網路之發展？又將來一般個人資料保護規則草案之相關規定施行後，德國聯邦個人資料保護法（*BDSG*）如何配合修正？

3. Wie soll die Bestimmung über schriftliche Zustimmung in §4a des Bundesdatenschutzgesetzes im Internet gelten gemacht werden? Wie kann es in der Zukunft an die Entwicklung des Internets angepasst werden? Wie kann die relevanten Bestimmungen der Änderungen der Allgemeinen europäischen Datenschutzverordnung 2012 ins Bundesdatenschutzgesetz umgesetzt werden?

四、 關於德國聯邦個人資料保護法（*BDSG*）第 13 條第 2 項規定所稱之「公共利益（*public interest*）」，德國目前實務上有無判斷之基準？為因應一般個人資料保護規則第 9 條(g)為增進公共利益所進行之必要資料處理（*processing is necessary for the performance of a task carried out in the public interest*）之規定，德國是否規劃修正相關法規，就其不確定之法律概念，有無實務判斷基準或具體實例可供參考？

4. Gibt es derzeit praktische Grundlage oder konkrete Fälle, die man zur Beurteilung des „Öffentlichen Interesses“ in Sinne des §13 Abs. 2 des Bundesdatenschutzgesetzes als Referenz heranziehen kann ? Hat Deutschland vor, die Bestimmung des § 9g der Allgemeinen europäischen Datenschutzverordnung 2012 über die erforderliche Verarbeitung zur Erfüllung der Aufgabe des öffentlichen Interesses zu ändern? Gibt es in der Praxis Grundlage für die Beurteilung der Unsicherheit der juristischen Begriffe oder konkrete Beispiele, die

man als Referenz dafür heranziehen kann?

五、 德國目前施行個人資料保護法所面臨主要問題以及因應修法方向為何？又為因應一般個人資料保護規則草案之提出，德國目前有無任何規劃修法方向或相關配套措施？例如確立「被遺忘權（*Right to be forgotten*）」後，德國將配合採取何種相關措施，以確保當事人行使該權利？

5. Was sind derzeit die Hauptprobleme bei der Ausführung des Bundesdatenschutzgesetzes und wie sieht die Richtlinie bzw. Richtung der Revisionen bzw. Gesetzesänderung aus? Gibt es Planung der Gesetzesänderungen bzw. Maßnahme zur Anpassung der Bestimmungen der Änderungen der Allgemeinen Europäischen Datenschutzverordnung 2012? Z.B. Was für Maßnahmen sollen ergriffen werden, nachdem das Recht, vergessen zu werden, festgelegt wird, um die Ausübung dieses Rechtes des Betroffenen sicherzustellen?

六、 請協助提供德國聯邦資料保護與資訊自由辦公室執行業務相關注意事項或手冊，以供我國行政實務之參考；並推薦值得購買之個人資料保護業務相關專業書籍（*handbook & casebook*）之名稱與出版社。

6. Bitte um Lieferung der Merkblätter oder Broschüre über die Geschäftausführung des Bundesdatenschutzes und des Büros der Informationsfreiheit, die wir für die administrative Praxis in unserem Land zur Referenz heranziehen können. Des weitere wird auch gebeten, uns hervorragende professionelle Handbücher und Fallsammlung über Datenschutz zu empfehlen.

附錄二、一般個人資料保護規則草案

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard
to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects the fundamental rights and freedoms of natural persons, and
in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:
(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;
(b) by the Union institutions, bodies, offices and agencies;
(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;
(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;
(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in
the Union by a controller not established in the Union, where the processing activities are related to:

(a) the offering of goods or services to such data subjects in the Union; or

(b) the monitoring of their behaviour.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'personal data' means any information relating to a data subject;

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(6) 'processor' means a natural or legal person, public authority, agency or any other

body which processes personal data on behalf of the controller;
(7) 'recipient' means a natural or legal person, public authority, agency or any other body
to which the personal data are disclosed;
(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;
(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an
individual which are inherited or acquired during early prenatal development;
(11) 'biometric data' means any data relating to the physical, physiological or behavioural
characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;
(12) ‘data concerning health’ means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;
(13) ‘main establishment’ means as regards the controller, the place of its establishment in
the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;
(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;
(15) ‘enterprise’ means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;
(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(17) ‘binding corporate rules’ means personal data protection policies which are adhered
to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;
(18) 'child' means any person below the age of 18 years;
(19) 'supervisory authority' means a public authority which is established by a Member
State in accordance with Article 46.

CHAPTER II

PRINCIPLES

Article 5

Principles relating to personal data processing

Personal data must be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;
(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;
(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.

Article 6

Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or

(b) the law of the Member State to which the controller is subject.

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

4. Where the purpose of further processing is not compatible with the one for which the

personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

Article 7

Conditions for consent

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
4. Consent shall not provide a legal basis for the processing, where there is a significant
imbalance between the position of the data subject and the controller.

Article 8

Processing of personal data of a child

1. For the purposes of this Regulation, in relation to the offering of information society
services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.
2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.
4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 9

Processing of special categories of personal data

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.
2. Paragraph 1 shall not apply where:
(a) the data subject has given consent to the processing of those personal data,

subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profitseeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or

(e) the processing relates to personal data which are manifestly made public by the data subject; or

(f) processing is necessary for the establishment, exercise or defence of legal claims; or

(g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or

(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or

(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or

(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data

referred to in paragraph 1 and the exemptions laid down in paragraph 2.

Article 10

Processing not allowing identification

If the data processed by a controller do not permit the controller to identify a natural person,
the controller shall not be obliged to acquire additional information in order to identify the
data subject for the sole purpose of complying with any provision of this Regulation.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

SECTION 1
TRANSPARENCY ANDMODALITIES

Article 11

Transparent information and communication

1. The controller shall have transparent and easily accessible policies with regard to the
processing of personal data and for the exercise of data subjects' rights.
2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

Article 12

Procedures and mechanisms for exercising the rights of the data subject

1. The controller shall establish procedures for providing the information referred to in
Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.
2. The controller shall inform the data subject without delay and, at the latest within one
month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an

unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

4. The information and the actions taken on requests referred to in paragraph 1 shall be

free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.

6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 13

Rights in relation to recipients

The controller shall communicate any rectification or erasure carried out in accordance with

Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves

impossible or involves a disproportionate effort.

SECTION 2
INFORMATION AND ACCESS TO DATA

Article 14

Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;

(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(c) the period for which the personal data will be stored;
(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
(f) the recipients or categories of recipients of the personal data;
(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;
(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.
2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.
3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.
4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:
(a) at the time when the personal data are obtained from the data subject; or
(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.
5. Paragraphs 1 to 4 shall not apply, where:
(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or
(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or
(c) the data are not collected from the data subject and recording or disclosure is

expressly laid down by law; or
(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.
6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.
8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 15

Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:
(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;
(d) the period for which the personal data will be stored;
(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;
(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
(g) communication of the personal data undergoing processing and of any available information as to their source;
(h) the significance and envisaged consequences of such processing, at least in the

case of measures referred to in Article 20.
2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.
4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3
RECTIFICATION AND ERASURE

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller the rectification of personal
data relating to them which are inaccurate. The data subject shall have the right to obtain
completion of incomplete personal data, including by way of supplementing a corrective
statement.

Article 17

Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
(c) the data subject objects to the processing of personal data pursuant to Article

19;
(d) the processing of the data does not comply with this Regulation for other reasons.
2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.
3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:
(a) for exercising the right of freedom of expression in accordance with Article 80;
(b) for reasons of public interest in the area of public health in accordance with Article 81;
(c) for historical, statistical and scientific research purposes in accordance with Article 83;
(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
(e) in the cases referred to in paragraph 4.
4. Instead of erasure, the controller shall restrict processing of personal data where:
(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;
(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;
(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;
(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).
5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.
6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.
7. The controller shall implement mechanisms to ensure that the time limits

established
for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.
8. Where the erasure is carried out, the controller shall not otherwise process such personal data.
9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:
(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;
(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;
(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

Article 18

Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic
means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.
2. Where the data subject has provided the personal data and the processing is based on
consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.
3. The Commission may specify the electronic format referred to in paragraph 1 and the
technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 4
RIGHT TO OBJECT AND PROFILING

Article 19

Right to object

1. The data subject shall have the right to object, on grounds relating to their particular

situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.

Article 20

Measures based on profiling

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Automated processing of personal data intended to evaluate certain personal aspects
relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. The Commission shall be empowered to adopt delegated acts in accordance with

Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

SECTION 5
RESTRICTIONS

Article 21

Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of
the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

(a) public security;

(b) the prevention, investigation, detection and prosecution of criminal offences;

(c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;

(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);

(f) the protection of the data subject or the rights and freedoms of others.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific
provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

CHAPTER IV

CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 22

Responsibility of the controller

1. The controller shall adopt policies and implement appropriate measures to ensure and
be able to demonstrate that the processing of personal data is performed in

compliance with this Regulation.
2. The measures provided for in paragraph 1 shall in particular include:
(a) keeping the documentation pursuant to Article 28;
(b) implementing the data security requirements laid down in Article 30;
(c) performing a data protection impact assessment pursuant to Article 33;
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);
(e) designating a data protection officer pursuant to Article 35(1).
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.
Article 23
Data protection by design and by default
1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.
4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with

the examination procedure referred to in Article 87(2).

Article 24

Joint controllers

Where a controller determines the purposes, conditions and means of the processing of
personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as
regards the procedures and mechanisms for exercising the rights of the data subject, by means
of an arrangement between them.

Article 25

Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.
2. This obligation shall not apply to:
(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or
(b) an enterprise employing fewer than 250 persons; or
(c) a public authority or body; or
(d) a controller offering only occasionally goods or services to data subjects residing in the Union.
3. The representative shall be established in one of those Member States where the data
subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.
4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Article 26

Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:
(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;
(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
(c) take all required measures pursuant to Article 30;
(d) enlist another processor only with the prior permission of the controller;
(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III;
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;
(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;
(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.
4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

Article 27

Processing under the authority of the controller and processor

The processor and any person acting under the authority of the controller or of the processor
who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.

Article 28

Documentation

1. Each controller and processor and, if any, the controller's representative, shall

maintain documentation of all processing operations under its responsibility.
2. The documentation shall contain at least the following information:
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
(b) the name and contact details of the data protection officer, if any;
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(d) a description of categories of data subjects and of the categories of personal data relating to them;
(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
(g) a general indication of the time limits for erasure of the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:
(a) a natural person processing personal data without a commercial interest; or
(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 29

Co-operation with the supervisory authority

1. The controller and the processor and, if any, the representative of the controller, shall

co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

SECTION 2
DATA SECURITY

Article 30

Security of processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

(a) prevent any unauthorised access to personal data;

(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

(c) ensure the verification of the lawfulness of processing operations.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 31

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.
2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.
3. The notification referred to in paragraph 1 must at least:
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;
(c) recommend measures to mitigate the possible adverse effects of the personal data breach;
(d) describe the consequences of the personal data breach;
(e) describe the measures proposed or taken by the controller to address the personal data breach.
4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.
6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject

without undue delay.
2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).
3. The communication of a personal data breach to the data subject shall not be required
if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.
4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.
6. The Commission may lay down the format of the communication to the data subject
referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data
subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in
paragraph 1:

(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;
(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;
(d) personal data in large scale filing systems on children, genetic data or biometric data;
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those

implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 34

Prior authorisation and prior consultation

1. The controller or the processor as the case may be shall obtain an authorisation from
the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data

protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.

9. The Commission may set out standard forms and procedures for prior authorisations
and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 4
DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case
where:

(a) the processing is carried out by a public authority or body; or

(b) the processing is carried out by an enterprise employing 250 persons or more; or

(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors

may designate a data protection officer.
5. The controller or processor shall designate the data protection officer on the basis of
professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.
6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.
7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.
8. The data protection officer may be employed by the controller or processor, or fulfil
his or her tasks on the basis of a service contract.
9. The controller or the processor shall communicate the name and contact details of the
data protection officer to the supervisory authority and to the public.
10. Data subjects shall have the right to contact the data protection officer on all issues
related to the processing of the data subject’s data and to request exercising the rights under this Regulation.
11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

Article 36

Position of the data protection officer

1. The controller or the processor shall ensure that the data protection officer is properly
and in a timely manner involved in all issues which relate to the protection of personal data.
2. The controller or processor shall ensure that the data protection officer performs the

duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer in performing
the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Article 37

Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer at least with the following tasks:

(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;

(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;

(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;

(d) to ensure that the documentation referred to in Article 28 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer’s own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer

referred to in paragraph 1.

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct

1. The Member States, the supervisory authorities and the Commission shall encourage
the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:
(a) fair and transparent data processing;
(b) the collection of data;
(c) the information of the public and of data subjects;
(d) requests of data subjects in exercise of their rights;
(e) information and protection of children;
(f) transfer of data to third countries or international organisations;
(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;
(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.
2. Associations and other bodies representing categories of controllers or processors in
one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.
3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.
4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Article 39

Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

3. The Commission may lay down technical standards for certification mechanisms and

data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

CHAPTER V

TRANSFER OF PERSONAL DATA TO THIRD

COUNTRIES

OR INTERNATIONAL ORGANISATIONS

Article 40

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing

after transfer to a third country or to an international organisation may only take place if,

subject to the other provisions of this Regulation, the conditions laid down in this Chapter are

complied with by the controller and processor, including for onward transfers of personal data
from the third country or an international organisation to another third country or to another
international organisation.

Article 41

Transfers with an adequacy decision

1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation in question has entered into.

3. The Commission may decide that a third country, or a territory or a processing sector
within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.

5. The Commission may decide that a third country, or a territory or a processing sector
within that third country, or an international organisation does not ensure an adequate

level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).

6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

7. The Commission shall publish in the *Official Journal of the European Union* a list of

those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.

8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.

Article 42

Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

(a) binding corporate rules in accordance with Article 43; or

(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when

declared generally valid by the Commission pursuant to point (b) of Article 62(1); or

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

Article 43

Transfers by way of binding corporate rules

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:

(a) are legally binding and apply to and are enforced by every member within the controller’s or processor's group of undertakings, and include their employees;

(b) expressly confer enforceable rights on data subjects;

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify:

(a) the structure and contact details of the group of undertakings and its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;
(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;
(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;
(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;
(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;
(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;
(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 44

Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for important grounds of public interest; or

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the

personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Where the processing is based on point (h) of paragraph 1, the controller or processor

shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.

4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.

6. The controller or processor shall document the assessment as well as the appropriate

safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

Article 45

International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

CHAPTER VI

INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 46

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible
for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.

2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.

3. Each Member State shall notify to the Commission those provisions of its law which
it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 47

Independence

1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.

2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible

with
their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.
5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.
6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.
7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.

Article 48

General conditions for the members of the supervisory authority

1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.
2. The members shall be chosen from persons whose independence is beyond doubt and
whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.
3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.
4. A member may be dismissed or deprived of the right to a pension or other benefits in
its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.
5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.

Article 49

Rules on the establishment of the supervisory authority

Each Member State shall provide by law within the limits of this Regulation:
(a) the establishment and status of the supervisory authority;

(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;
(c) the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the office;
(d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
(e) whether the members of the supervisory authority shall be eligible for reappointment;
(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;
(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.

Article 50

Professional secrecy

The members and the staff of the supervisory authority shall be subject, both during and after
their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their
official duties.

SECTION 2
DUTIES AND POWERS

Article 51

Competence

1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.
2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this

Regulation.
3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 52

Duties

1. The supervisory authority shall:
(a) monitor and ensure the application of this Regulation;
(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;
(d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;
(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;
(g) authorise and be consulted on the processing operations referred to in Article 34;
(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);
(i) approve binding corporate rules pursuant to Article 43;
(j) participate in the activities of the European Data Protection Board.
2. Each supervisory authority shall promote the awareness of the public on risks, rules,
safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.
3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall
provide a complaint submission form, which can be completed electronically, without excluding other means of communication.
5. The performance of the duties of the supervisory authority shall be free of charge for
the data subject.
6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.

Article 53

Powers

1. Each supervisory authority shall have the power:
(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;
(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;
(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;
(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;
(e) to warn or admonish the controller or the processor;
(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;
(g) to impose a temporary or definitive ban on processing;
(h) to suspend data flows to a recipient in a third country or to an international organisation;
(i) to issue opinions on any issue related to the protection of personal data;
(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.
2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:
(a) access to all personal data and to all information necessary for the performance

of its duties;
(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.
The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.
3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).
4. Each supervisory authority shall have the power to sanction administrative offences,
in particular those referred to in Article 79(4), (5) and (6).

Article 54

Activity report

Each supervisory authority must draw up an annual report on its activities. The report shall be
presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.

CHAPTER VII

CO-OPERATION AND CONSISTENCY

SECTION 1
CO-OPERATION

Article 55

Mutual assistance

1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data subjects in several Member States are likely to be affected by processing operations.
2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing

operations contrary to this Regulation.
3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.
4. A supervisory authority to which a request for assistance is addressed may not refuse
to comply with it unless:
(a) it is not competent for the request; or
(b) compliance with the request would be incompatible with the provisions of this Regulation.
5. The requested supervisory authority shall inform the requesting supervisory authority
of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.
6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.
7. No fee shall be charged for any action taken following a request for mutual assistance.
8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.
9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.
10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 56

Joint operations of supervisory authorities

1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint

operations, in which designated members or staff from other Member States' supervisory authorities are involved.

2. In cases where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay.

3. Each supervisory authority may, as a host supervisory authority, in compliance with

its own national law, and with the seconding supervisory authority’s authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority’s members or staff involved in joint operations or, in so far as the host supervisory authority’s law permits, allow the seconding supervisory authority’s members or staff to exercise their executive powers in accordance with the seconding supervisory authority’s law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.

4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.

5. Where a supervisory authority does not comply within one month with the obligation

laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).

6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.

SECTION 2
CONSISTENCY

Article 57

Consistency mechanism

For the purposes set out in Article 46(1), the supervisory authorities shall co-operate

with
each other and the Commission through the consistency mechanism as set out in this section.

Article 58

Opinion by the European Data Protection Board

1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:

(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or

(b) may substantially affect the free movement of personal data within the Union; or

(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or

(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or

(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or

(f) aims to approve binding corporate rules within the meaning of Article 43.

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.

5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.

6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.

7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.
8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

Article 59

Opinion by the Commission

1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.
2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.
3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.
4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.

Article 60

Suspension of a draft measure

1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the

supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:
(a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or
(b) adopt a measure pursuant to point (a) of Article 62(1).
2. The Commission shall specify the duration of the suspension which shall not exceed
12 months.
3. During the period referred to in paragraph 2, the supervisory authority may not adopt
the draft measure.

Article 61

Urgency procedure

1. In exceptional circumstances, where a supervisory authority considers that there is an
urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.
3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.
4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3
of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

Article 62

Implementing acts

1. The Commission may adopt implementing acts for:
(a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;
(b) deciding, within the period referred to in Article 59(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 58(2), as having general validity;
(c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;
(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8).
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.
3. The absence or adoption of a measure under this Section does not prejudice any other
measure by the Commission under the Treaties.

Article 63

Enforcement

1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.
2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.

SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 64

European Data Protection Board

1. A European Data Protection Board is hereby set up.

2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.

3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.

4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.

Article 65

Independence

1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67.

2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.

Article 66

Tasks of the European Data Protection Board

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;

(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;

(e) promote the co-operation and the effective bilateral and multilateral exchange

of information and practices between the supervisory authorities;
(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;
(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.
2. Where the Commission requests advice from the European Data Protection Board, it
may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.
3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.
4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

Article 67

Reports

1. The European Data Protection Board shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries.
The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).
2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.

Article 68

Procedure

1. The European Data Protection Board shall take decisions by a simple majority of its
members.
2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.

Article 69

Chair

1. The European Data Protection Board shall elect a chair and two deputy chairpersons
from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.
2. The term of office of the chair and of the deputy chairpersons shall be five years and
be renewable.

Article 70

Tasks of the chair

1. The chair shall have the following tasks:
(a) to convene the meetings of the European Data Protection Board and prepare its agenda;
(b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.
2. The European Data Protection Board shall lay down the attribution of tasks between
the chair and the deputy chairpersons in its rules of procedure.

Article 71

Secretariat

1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat.
2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair.
3. The secretariat shall be responsible in particular for:
(a) the day-to-day business of the European Data Protection Board;
(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;
(c) the use of electronic means for the internal and external communication;
(d) the translation of relevant information;
(e) the preparation and follow-up of the meetings of the European Data Protection Board;
(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.

Article 72

Confidentiality

1. The discussions of the European Data Protection Board shall be confidential.

2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.
3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.

CHAPTER VIII

REMEDIES, LIABILITY AND SANCTIONS

Article 73

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.
2. Any body, organisation or association which aims to protect data subjects' rights and
interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.
3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

Article 74

Right to a judicial remedy against a supervisory authority

1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.
2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of

Article 52(1).
3. Proceedings against a supervisory authority shall be brought before the courts of the
Member State where the supervisory authority is established.
4. A data subject which is concerned by a decision of a supervisory authority in another
Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.
5. The Member States shall enforce final decisions by the courts referred to in this Article.

Article 75

Right to a judicial remedy against a controller or processor

1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.
3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.
4. The Member States shall enforce final decisions by the courts referred to in this Article.

Article 76

Common rules for court proceedings

1. Any body, organisation or association referred to in Article 73(2) shall have the right
to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.
2. Each supervisory authority shall have the right to engage in legal proceedings and

bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.
3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.
4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.
5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

Article 77

Right to compensation and liability

1. Any person who has suffered damage as a result of an unlawful processing operation
or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.
2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

Article 78

Penalties

1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.
2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.
3. Each Member State shall notify to the Commission those provisions of its law which
it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 79

Administrative sanctions

1. Each supervisory authority shall be empowered to impose administrative sanctions in
accordance with this Article.
2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation
with the supervisory authority in order to remedy the breach.
3. In case of a first and non-intentional non-compliance with this Regulation, a warning
in writing may be given and no sanction imposed, where:
(a) a natural person is processing personal data without a commercial interest; or
(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.
4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:
(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);
(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).
5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:
(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;
(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;
(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not

take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;
(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;
(e) does not or not sufficiently determine the respective responsibilities with cocontrollers
pursuant to Article 24;
(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);
(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.
6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:
(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;
(b) processes special categories of data in violation of Articles 9 and 81;
(c) does not comply with an objection or the requirement pursuant to Article 19;
(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;
(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;
(f) does not designate a representative pursuant to Article 25;
(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;
(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;
(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;

(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;
(k) misuses a data protection seal or mark in the meaning of Article 39;
(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;
(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);
(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);
(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.

CHAPTER IX

PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80

Processing of personal data and freedom of expression

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.
2. Each Member State shall notify to the Commission those provisions of its law which

it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

Article 81

Processing of personal data concerning health

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2),

processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:

(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or

(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or

(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Article 82

Processing in the employment context

1. Within the limits of this Regulation, Member States may adopt by law specific rules

regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of

employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Each Member State shall notify to the Commission those provisions of its law which
it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Article 83

Processing for historical, statistical and scientific research purposes

1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:

(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:

(a) the data subject has given consent, subject to the conditions laid down in Article 7;

(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or

(c) the data subject has made the data public.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.

Article 84

Obligations of secrecy

1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.
2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 85

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply,
at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.
2. Churches and religious associations which apply comprehensive rules in accordance
with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.

CHAPTER X

DELEGATED ACTS AND IMPLEMENTING ACTS

Article 86

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article
12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred

on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article
12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to
the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Article 87

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

FINAL PROVISIONS

Article 88

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 89

Relationship to and amendment of Directive 2002/58/EC

1. This Regulation shall not impose additional obligations on natural or legal persons in
relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

2 Article 1(2) of Directive 2002/58/EC shall be deleted.

Article 90

Evaluation

The Commission shall submit reports on the evaluation and review of this Regulation to the
European Parliament and the Council at regular intervals. The first report shall be submitted
no later than four years after the entry into force of this Regulation. Subsequent reports shall
be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal
instruments, in particular taking account of developments in information technology and in
the light of the state of progress in the information society. The reports shall be made public.

Article 91

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from [*two years from the date referred to in paragraph 1*].

This Regulation shall be binding in its entirety and directly applicable in all Member

States.

Done at Brussels,

For the European Parliament For the Council

The President The President

附錄三、比利時個人資料隱私權保護法

13 FEBRUARY 2001 – Royal Decree implementing the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data

Unofficial translation – September 2008

This translation has not been finalized. Modifications to the present document consequently remain possible.

ALBERT II, King of Belgians,

All those who are and shall be, we salute.

Whereas the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, modified by the Law of 11 December 1998 transposing Directive 95/46/EC of 24 October 1995 of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and particularly articles 4, § 1, 2° and 5°; 6, § 2, first paragraph, a), and g); 6, § 4; 7, § 2, a) and k); 7, § 3; 8, § 4, e); 8, § 4; 9, § 1, e); 9, § 2, first paragraph, e); 9, § 2, third paragraph; 10, § 1, second and fourth paragraph; 12, § 2; 13, second and fourth paragraph; 17, §§ 8 and 9, and 18, third paragraph;

Whereas article 52 of the Law of 11 December 1998;

Whereas opinions no 08/99 of 8 March 1999 and 25/99 of 23 June 1999 of the Commission for the Protection of the Privacy;

Whereas the opinion of the Inspector of Finance, issued on 9 April 1999;

Whereas the agreement of the Minister of Budget, expressed on 28 May 1999;

Whereas the decision of the Council of Ministers;

Whereas the Council of State's opinions of 21 June 1999 and 8 November 2000;

As proposed by Our Minister of Justice and following our Ministers' opinion after careful deliberation among them,

We have decided and we shall decide:

CHAPTER I. – Definitions

Article 1. For the purposes of this decree:

1° "the Law" shall be construed as the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data;

2° "the Commission" shall be construed as the Commission for the Protection of the Privacy;

3° "encoded personal data" shall be construed as personal data that can only be related to an identified or identifiable person by means of a code;

4° "non-encoded personal data" shall be construed as data other than encoded personal data;

5° "anonymous data" shall be construed as data that cannot be related to an identified or identifiable person and that are consequently not personal data;

1

6° "intermediary organization" shall be construed as any natural person, legal person, un-associated organization or public authority, other than the controller of the processing of non-encoded data, encoding the aforementioned data.

CHAPTER II. – Further processing of personal data for historical, statistical or scientific purposes

Section I. – General Principles

Art 2. The further processing of personal data for historical, statistical or scientific purposes shall be considered in accordance with article 4, § 2, 1°, second sentence of the Law if it is carried out under the conditions set forth in this chapter.

The storage of personal data for historical, statistical or scientific purposes, as referred to in article 4, § 1, 5° second sentence of the Law, is authorized under the conditions set forth in this chapter.

Art 3. The further processing of historical, statistical or scientific purposes shall take place using anonymous data.

Art 4. If it is impossible to realize the historical, statistical or scientific purposes using anonymous data for the further processing, the controller of the further processing for historical, statistical or scientific purposes may process encoded data pursuant to the provisions of section 2 of this chapter.

In that case he shall mention in the notification of the processing, which he shall make pursuant to article 17 of the Law, the reasons why it is impossible to realize the historical, statistical or scientific purposes using anonymous data for the further processing.

Art 5. If it is impossible to realize the historical, statistical or scientific purposes using encoded data for the further processing, the controller of the further processing for historical, statistical or scientific purposes may process non-encoded data pursuant to the provisions of section 2 of this chapter.

In that case he shall mention in the notification of the processing, which he shall make pursuant to article 17 of the Law, the reasons why it is impossible to realize the historical, statistical or scientific purposes using encoded data for the further processing.

Art 6. The controller of the further processing of personal data for historical, statistical or scientific purposes must not perform any operations aiming at the transformation of anonymous data into personal data or of encoded personal data into non-encoded personal data.

Section II. – Processing encoded personal data

2

Art 7. Personal data shall be encoded prior to any further processing for historical, statistical or scientific purposes.

Art 8. If the controller of the processing of personal data collected for clearly specified, explicitly described and legitimate purposes, further processes those personal data for historical, statistical or scientific purposes or entrusts a processor with the processing, the personal data shall be encoded prior to the further processing, either by the controller, the processor or an intermediary organization.

In that last case the intermediary organization shall be considered as processor in the meaning of article 1, § 5 of the Law.

Art. 9 If the controller of the processing of personal data collected for clearly specified, explicitly described and legitimate purposes discloses the personal data to a third party with a view to further processing for historical, statistical or scientific purposes, the personal data shall be encoded by the controller or an intermediary organization prior to the disclosure.

In that last case the intermediary organization shall be considered as processor in the meaning of article 1, § 5 of the Law.

Art 10. If several controllers for the processing of personal data collected for clearly specified, explicitly described and legitimate purposes disclose personal data to the same third party (-ies) with a view to further processing for historical, statistical or scientific purposes, the personal data shall be encoded by an intermediary organization prior to the disclosure.

In that last case the intermediary organization shall be considered as processor in the meaning of article 1, § 4 of the Law.

Art 11. The intermediary organization shall be independent from the controller of the further processing of the personal data for historical, statistical or scientific purposes.

Art 12. The controller of the processing of personal data collected for clearly specified, explicitly described and legitimate purposes and the intermediary organization encoding the personal data with a view to further processing for historical, statistical or scientific purposes, shall take appropriate technical and organizational measures in order to prevent encoded data from being transformed into non-encoded data.

Art 13. The controller of the processing of personal data collected for clearly specified, explicitly described and legitimate purposes and the intermediary organization may only disclose encoded data with a view to further processing for historical, statistical or scientific purposes when the controller of

3

the further processing produces a receipt of complete notification, issued by the Commission pursuant to article 17, § 2 of the Law.

Art 14. The controller of the processing of personal data collected for clearly specified, explicitly described and legitimate purposes or the intermediary organization must provide the data subject prior to the encoding of the data referred to in articles 6 to 8 of the Law with the following information:

the identity of the controller;

the categories of data being processed;

the origin of the data;

a precise description of the historical, statistical or scientific purposes of the processing;

the recipients or categories of recipients of the data;

the existence of a right to access and to rectify one's personal data;

the existence of the data subject's right to object.

Art 15. The controller of the processing of personal data collected for clearly specified, explicitly described and legitimate purposes and the intermediary organization do not have to comply with the duty imposed by article 14 of the present decree if this duty proves impossible or would involve a disproportionate effort, and if they have followed the procedure established by article 16 of this decree.

Art 16. The controller of the processing of personal data collected for clearly specified, explicitly described and legitimate purposes or the intermediary organization do not have to comply with the duty imposed by article 14 if the intermediary organization is an administrative authority having the explicit task, by or under the law, of gathering and encoding personal data, and if it is subject to specific measures laid down by or under the law in order to protect privacy in this process.

Art 16. The controller of the processing of personal data collected for clearly specified, explicitly described and legitimate purposes or the intermediary organization wishing to encode the data referred to in articles 6 to 8 of the Law without informing the data subject in advance, shall complete the notification he is to make under article 17 of the Law with the following information:

1° a precise description of the historical, statistical or scientific purposes of the processing;

2° the reasons justifying the processing of the personal data referred to in articles 6 to 8 of the Law;

3° the reasons why the data mentioned in article 14 cannot be communicated to the data subject or the disproportion of the effort to do so;

4

4° the categories of persons whose personal data mentioned in articles 6 to 8 of the Law are being processed;
5° the individuals or categories of individuals having access to the personal data;
6° the origin of the data.
Within forty-five days upon receipt of the notification, the Commission shall transmit a recommendation to the controller or the intermediary organization, if necessary accompanied by additional conditions to be respected when further processing the encoded personal data referred to in articles 6 to 8 of the Law.
The term established in the second paragraph may be prolonged by forty-five days once. The Commission shall inform the controller of the prolongation of the first term prior to the expiration of that term.
If the Commission has not given a recommendation upon expiration of the terms referred to in this article, the request shall be considered as accepted.
The Commission shall publish its recommendation in the register referred to in article 18 of the Law.
Art 17. The controller must report any modification to the data he has transmitted to the Commission pursuant to article 16 of the present decree.

Section III. – Processing non-encoded personal data

Art 18. Prior to the further processing of non-encoded personal data for historical, statistical or scientific purposes, the controller of the further processing shall provide the data subject with the following information:
1° the identity of the controller;
2° the categories of data being processed;
3° the origin of the data;
4° a precise description of the historical, statistical or scientific purposes of the processing;
5

5° the recipients or categories of recipients of the data;
6° the existence of a right to access and to rectify one's personal data;
7° the existence of the duty to ask the data subject's consent prior to the processing of non-encoded personal data for historical, statistical or scientific purposes.

Art 19. The data subject must give his explicit consent to the processing of non-encoded personal data relating to him for historical, statistical or scientific purposes prior to the processing.

Art 20. The controller of the further processing of non-encoded personal data for historical, statistical or scientific purposes does not have to respect the duties imposed by articles 18 and 19 of the present decree:
1° if the further processing for historical, statistical or scientific purposes is restricted to non-encoded personal data that have been made public as a result of steps deliberately taken by the data subject or that are closely related to the public character of the data subject or of the facts in which the data subject is or was involved;
or
2° if complying with these duties proves impossible or would require a disproportionate effort, and the controller has followed the procedure established in article 21 of the present decree.

Art 21. Any controller of the further processing of non-encoded personal data for historical, statistical or scientific purposes wishing to process the data without informing the data subject in advance and asking the latter for his consent, shall complete the notification required for this purpose under article 17 of the Law with the following information:
1° a precise description of the historical, statistical or scientific purposes of the processing;
2° the reasons why it is necessary to process non-encoded data;
3° the reasons why the data subject cannot be asked for an informed consent, or the disproportion of the effort required to obtain such consent;
4° the categories of individuals whose non-encoded personal data are being processed;
5° the individuals or categories of individuals having access to the non-encoded data;
6

6° the origin of the data.

Within a forty-five day term upon receipt of the notification, the Commission shall transmit a recommendation to the controller of the further processing, if necessary accompanied by any additional conditions to be respected when further processing the non-encoded data for historical, statistical or scientific purposes.

The term established in the second paragraph may be prolonged by forty-five days once. The Commission shall inform the controller of the further processing of the prolongation of the first term prior to the expiration of that term.

If the Commission has not given a recommendation upon expiration of the terms referred to in this article, the request shall be considered as accepted.

The Commission shall publish its recommendation in the register referred to in article 18 of the Law.

Art 22. Any modification to the data the controller has transmitted to the Commission pursuant to article 21 of the present decree must be reported to the latter.

Section IV. – Publication of the results of the processing

Art 23. The results of the processing for historical, statistical or scientific purposes must not be published in a form allowing for the identification of the data subject unless:

1° the latter has given his explicit consent and the privacy of third parties is not violated, or

2° the publication of non-encoded data is restricted to data that have been made public as a result of steps deliberately taken by the data subject or that are closely related to the public character of the data subject or of the facts in which the data subject was or has been involved.

Section V. – Exception

Art 24. Chapter II of the present decree does not apply to the services and authorities referred to in article 3, § 4 of the Law when further processing personal data for historical, statistical or scientific purposes.

CHAPTER III. – Conditions for processing the personal data referred to in articles 6 to 8 of the L aw

7

Art 25. When processing the personal data referred to in articles 6 to 8 of the Law, the controller must, moreover, take the following measures:
1° the categories of individuals having access to the personal data must be designated by the controller or, as the case may be, by the processor, with a precise description of their function with respect to the data processing operation in question;
2° the list of designated individuals must be kept at the disposal of the Commission by the controller or, if such is the case, the processor;
3° the controller must ensure that the individuals designated respect the confidential nature of the data in question under a contractual or statutory obligation or under an equivalent contractual provision;
4° when informing the data subject under article 9 of the Law or in the notification referred to in article 17, § 1 of the Law, the controller must mention the law or regulation authorizing the processing of the personal data referred to in articles 6 to 8 of the Law.
Art 26. If processing the personal data referred to in articles 6 and 7 of the Law is only authorized with the data subject's written consent, the controller must inform the latter of the reasons for the processing and provide him with the list of the categories of individuals having access to the personal data, in addition to the data that must be supplied by virtue of article 9.
Art 27. If processing the personal data referred to in articles 6 and 7 of the Law is only authorized with the data subject's written consent, such processing shall be prohibited if the controller is the data subject's current or potential employer or if the data subject is in a dependent position with respect to the controller, preventing the former from giving his free consent.
This prohibition shall be lifted when the processing is intended for the data subject to benefit from.
CHAPTER IV. – Conditions for exemption from the duty of information referred to in article 9, § 2 of the Law
Art 28. The controller of the further processing of personal data for historical, statistical or scientific purposes processing encoded data only shall be exempt from the duty to inform the data subject referred to in article 9, § 2 of the Law, provided that the conditions set forth in Chapter II, Section II of the present decree have been met.
Art 29. Any administrative authority that has the explicit task of gathering and encoding personal data by or under the law, and that is subject to specific measures laid down by or under the law for
8

the purpose of protecting privacy in this process, shall be exempt from the duty of information referred to in article 9, § 2 of the Law if it acts as intermediary organization.

Art 30. Except for the case described in articles 28 and 29 of the present decree, any controller invoking an exemption from the duty of information referred to in article 9, § 2 of the Law, because informing the data subject proves impossible or would involve a disproportionate effort, shall provide the aforementioned information at the time of his first contact with the data subject.

If the controller referred to in the first paragraph discloses the personal data to a third party, the information referred to in article 9, § 2 of the Law shall be provided by that third party at the time of his first contact with the data subject.

Art 31. Any controller unable to inform the data subject because this proves impossible or would involve a disproportionate effort, shall mention this in the notification he makes to the Commission under article 17 of the Law.

The Commission shall publish the list of controllers in the public register described in article 18 of the Law and mention the reasons justifying the exemption.

CHAPTER V. – Exercise of the rights referred to in articles 10 and 12 of the Law

Art 32. Any individual proving his identity has the right to access the information mentioned in article 10 under the conditions laid down by law, such by means of a signed and dated request submitted on the spot, sent by post or sent using a means of telecommunication:

either to the controller or his representative in Belgium, or an individual authorized or appointed by him;

either to the processor who shall transmit it to one of the aforementioned individuals if necessary.

If the request is delivered on the spot, the individual receiving it shall immediately provide the requester with a dated and signed receipt.

Art 33. Any request to prohibit the use of, to rectify or to delete personal data and any objection based on article 12 of the Law shall be submitted following the same procedure and to the individuals mentioned in article 32 of the present decree.

9

Art 34. If personal data are collected from the data subject in writing, the controller shall use the document he collects the data with to ask the former whether he wishes to exercise the right to object provided for by article 12, § 1, third paragraph of the Law.

If the personal data are collected from the data subject otherwise than in writing, the controller shall ask the former whether he wishes to exercise the right to object provided for by article 12, § 1, third paragraph of the Law. The data subject may do so on a document the controller provides him with at the latest two months after the personal data were collected or using any technical means making it possible to prove that he was offered the possibility to exercise the aforementioned right.

Art 35. If the personal data are not collected from the data subject, any controller who is subject to article 9, § 2, c) of the Law, shall ask the former in writing whether he wishes to exercise the right to object provided for by article 12, § 1, third paragraph of the Law.

CHAPTER VI. – Exercise of the right referred to in article 13 of the Law

Art 36. This chapter shall establish the procedure for the submission of requests under article 13 of the Law.

Art 37. The data subject must submit the request to the Commission by means of a dated and signed letter mentioning his surname, first name, date of birth, nationality and include a copy of his identity card, passport or any equivalent document.

The request shall also mention the following information, provided that it is known to the requester:

the name of the authority or service involved;

all relevant elements regarding the data under discussion, such as their nature, the circumstances of or the reason for access to the data, as well as possible rectifications.

Art 38. If the Commission considers it useful to do so, it may ask the data subject for additional information.

Art 39. If the data referred to in articles 37 and 38 of the present decree are not provided, the request may be declared inadmissible.

Art 40. The request shall be inadmissible if it is submitted within a one-year term starting from the date the Commission's previous answer regarding the same data and the same services was sent.

This term may be deviated from if the data subject lists reasons justifying such deviation in his request.

Art 41. If the request is considered inadmissible, the data subject shall be informed of that fact by letter.

This letter shall mention that the data subject may be heard upon request, such in the presence of his counsellor if necessary.

Art 42. Inspection at the service involved shall be carried out by the Commission's President or by one or more of its members designated by him.

The verifications of the processing operations of personal data referred to in article 3, § 5, 1° of the Law shall be carried out by magistrates designated among the Commission members.

The President and the members performing the check may request the assistance of or be represented by one or more members of the Commission's secretariat.

Art 43. During the inspection at the service concerned, the Commission shall carry out or order any verification it sees fit.

During the check at the service concerned, referred to in article 3, § 5 of the Law, the Commission may have data rectified or removed, or have data introduced that differ from those processed by the service concerned. It may prohibit the disclosure of the data.

During the check at the service concerned, referred to in article 3, § 5 of the Law, the Commission shall recommend such measures as it considers necessary. It shall motivate its recommendations.

Art 44. After those verifications the service concerned shall inform the Commission of the effect that has been given to them.

Art 45. The Commission shall reply to the data subject's request by letter within a three-month term starting from the moment the information referred to in article 44 of the decree was transmitted.

Art 46. If the data subject's request relates to a processing operation carried out by a police service with a view to an identity check, the Commission shall communicate to the data subject that the necessary verifications have been carried out.

If necessary, the Commission shall provide the data subject with all other information it sees fit upon receipt of the opinion of the service concerned.

11

CHPATER VII. – Notification of the automatic processing of personal data

Section I. – Fees to be paid to the Commission upon notification

Art 47. If the notification referred to in article 17 of the Law is made using the paper form made available by the Commission for that purpose, the amount of the fee to be paid to the Commission by the controller shall be established at 125 euros or 5042 francs for the notification of all data provided to the Commission by the same controller at the same time.

Art 48. If notification is made using the magnetic information carrier made available by the Commission for that purpose, the amount of the fee to be paid to the Commission shall be established at 25 euros or 1008 francs for the notification of all data provided to the Commission by the same controller at the same time.

Art 49. The amount of the fee to be paid to the Commission by the controller upon notification at the same time of one or more modifications of the information in his original declaration, shall be established at 20 euros or 807 francs.

Art 50. The controller shall pay the fees referred to in this section using the documents made available by the Commission for that purpose.

Section II. – Categories of processing operations exempt from the duty of notification

Art 51. Except for §§ 4 and 8, the provisions of article 17 of the Law do not apply to the processing of personal data relating exclusively to data that are necessary for the payroll administration of individuals employed by or working for the controller, provided that the data are only used for that payroll administration, that they are only disclosed to the recipients who are entitled to them and that they are not stored any longer than necessary for the purposes of the processing.

Art 52. Except for §§4 and 8, the provisions of article 17 of the Law do not apply to the processing of personal data relating exclusively to data that are necessary for the personnel administration of individuals employed by or working for the controller.

The processing must not involve personal data regarding the data subject's health, nor sensitive or judicial data in the meaning of articles 6 and 8 of the Law, nor data aiming at an assessment of the individual.

The personal data being processed must not be kept any longer than necessary for personnel administration and may only be disclosed to third parties in the framework of the application of a provision from a law or ordinance, or whenever necessary to achieve the objectives.

12

Art 53. Except for §§ 4 and 8, the provisions of article 17 of the Law do not apply to the processing of personal data relating only to keeping the controller's accounts, provided that the data are only used for accounting purposes, that the processing only relates to individuals whose data are necessary for those purposes and that the personal data are not kept any longer than necessary for accounting purposes.
The data being processed may only be disclosed to third parties in the framework of the application of a provision from a law or ordinance, or whenever necessary for accounting purposes.
Art 54. Except for §§ 4 and 8, the provisions of article 17 of the law do not apply to the processing of personal data relating only to associate and shareholder administration, provided that the processing only relates to data needed for such administration, that the data only relate to individuals whose data are needed for such administration, that the data are not disclosed to third parties, except in the framework of the application of provision from a law or ordinance, and that the personal data are not kept any longer than necessary for the purposes of the processing.
Art 55. Except for §§ 4 and 8, the provisions of article 17 of the Law do not apply to the processing of personal data relating only to the controller's customer or supplier management.
The processing may only relate to the controller's potential, existing and former customers or suppliers.
The processing must not relate to personal data regarding the data subject's health, nor to sensitive or judicial data in the meaning of articles 6 and 8 of the Law.
For customer administration no individuals must be registered during a data processing operation on the basis of data provided by third parties.
The data must not be kept any longer than necessary for normal company management by the controller and may only be disclosed to third parties in the framework of the application of a provision from a law or ordinance, or for the purposes of normal company management.
Art 56. Except for §§ 4 and 8, the provisions of article 17 of the Law shall not apply to the processing of personal data carried out by a foundation, an association any other non-profit organization in the course of its normal activities.
The processing may only relate to member administration, to individuals the controller regularly enters into contact with or to supporters of the foundation, association or organization.
13

During the processing operations no individuals must be registered on the basis of data provided by third parties. The personal data being processed must not be kept any longer than necessary for member, contact or supporter administration and may only be disclosed to third parties in the framework of the application of a provision from a law or ordinance.

Art 57. Except for §§ 4 and 8, the provisions of article 17 of the Law shall not apply to the processing of identification data that is necessary for communication and that is carried out for the sole purpose of contacting the data subject, provided that the data are not disclosed to third parties and that they are not kept any longer than necessary for the purpose of the processing.

The first paragraph of this article only relates to the processing of personal data that are not referred to in another provision of the present decree.

Art 58. Except for §§ 4 and 8, the provisions of article 17 of the Law shall not apply to the processing of personal data that only relate to visitor registration in the context of access control, provided that the data are restricted to the visitor's name and professional address, the identification of his employer, the identification of the visitor's vehicle, the name, department and function of the individual being visited and the time of the visit.

The personal data may only be used for access control and must not be kept any longer than necessary for that purpose.

Art. 59 Except for §§ 4 and 8, the provisions of article 17 of the Law shall not apply to the processing of personal data carried out by education institutions with a view to the management of the relationship with their pupils or students.

The processing may only relate to personal data of potential, current and former pupils or students of the education institution concerned.

During the processing no individuals must be registered on the basis of data provided by third parties. The personal data being processed may only be disclosed to third parties in the framework of the application of a provision from a law or ordinance and must not be kept any longer than necessary for managing the relationship with the pupil or student.

Art 60. Except for §§ 4 and 8, the provisions of article 17 of the Law shall not apply to the processing of personal data carried out by municipalities pursuant to the Law of 19 July 1991 on population registers and identity cards and modifying the Law of 8 August 1983 establishing a National Register of natural persons, pursuant to electoral legislation and to the legal provisions concerning the registers of the registry office.

Art 61. Except for §§ 4 and 8, the provisions of article 17 of the Law shall not apply to the processing of personal data carried out by administrative authorities if the processing is subject to specific regulations issued by or under the law that lay down how the data being processed are accessed, used and obtained.

Art 62. Except for §§ 4 and 8, the provisions of article 17 of the Law shall not apply to the processing of personal data carried out by the social security institutions referred to in articles 1 and 2, first paragraph, 2° of the Law of 15 January 1990 establishing and organizing the Crossroads Bank of Social Security, which aim at the application of social security, provided that these institutions meet the provisions of the aforementioned law and its implementing decrees when processing the data.

The list referred to in article 46, first paragraph, 6°bis of the Law of 15 January 1990 establishing and organizing the Crossroads Bank of Social Security shall be kept at the disposal of the Commission for the Protection of the Privacy by the Crossroads Bank, pursuant to the conditions set out by mutual agreement between both parties.

On the basis of this list, the Commission for the Protection of the Privacy shall update the public register of automatic processing referred to in article 18 of the Law.

CHAPTER VIII. – Public register of the automatic processing of personal data

Art 63. The public register of the automatic processing of personal data referred to in article 18 of the Law, hereinafter public register, may be accessed as follows:

direct access at a distance using a means of telecommunication;

direct access on the spot, in the offices designated for that purpose by the Commission;

indirect access by means of a request for an extract, submitted to the Commission.

Art 64. For direct access at a distance the Commission shall make a copy of the public register available on a server that is accessible through the Internet.

Besides the mode of access described in the first paragraph, the Commission may suggest other access possibilities.

Art 65. For direct access on the spot, the Commission shall make the necessary offices available during normal office hours, as well as computer appliances equipped with appropriate software, such for any individual presenting himself to the Commission in order to access the public register.

15

Art 66. Any individual may present himself to the Commission or submit a written request to it in order to obtain an extract from the public register.
The oral or written request for an extract must include at least one of the following elements:
1° the identification number or the name of the processing operation(s) the extract relates to;
2° the complete or abbreviated name of the controller that is to be mentioned in the extract requested;
3° in case of a written request sent by letter, the address to send the extract to.
Art 67. If the requested extract form the public register relates to more than ten processing operations and several controllers or to over one hundred processing operations of the same controller, the Commission may deliver a simplified extract mentioning the identification number, the name and the purpose of every processing operation, as well as the identification number, the name and the municipality with the postal code for every controller.
In the case described in the first paragraph, the Commission shall inform the requester of the extract of his right to direct access of the public register as well as of the ways in which this right may be exercised.
Art 68. Access to the public register shall be free of charge.
Art 69. No person can be obliged to disclose his reasons for accessing the public register to the Commission, regardless of whether the access is direct or indirect.

CHAPTER IX. – Final provisions

Art 70. All provisions of the Law of 11 December 1998 shall enter into force on the first day of the sixth month following the Law's month of publication in the Belgian Official Journal.
As of that day, all controllers of existing and future processing operations must comply with the provisions of the Law of 11 December 1998.
Art 71. The notifications referred to in article 17, § 7 of the Law that were made before the date this decree entered into effect, shall be considered in accordance with the provisions of the Law and of the present decree.
16

If the data included in the notification referred to in the first paragraph are modified, any controller making a notification in the meaning of article 17, § 7 of the Law shall act in accordance with the stipulations of the Law and of the present decree.

Art 72. The following Royal Decrees shall be cancelled:

1) Royal Decree no 1 establishing the date of entry into force of the provisions of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data;

2) Royal Decree no 2 of 28 February 1993 establishing the terms within which the holder of a file must comply with the proviions of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, with regard to existing processing operations at the time of entry into force;

3) Royal Decree of 12 August 1999 implementing article 11, 4° of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data;

4) Royal Decree no 3 of 7 September 1993 designating the individuals to whom the request for disclosure of personal data based on article 10 of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data is to be submitted;

5) Royal Decree no 4 of 7 September 1993 establishing the amount and the conditions for the payment of a preliminary charge for the holder of the file when exercising the right to access personal data pursuant to article 10 of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data;

6) Royal Decree no 5 of 7 September 1993 designating the individuals to whom the requests for access deletion or prohibition of the use of person data based on article 12 of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data is to be submitted;

7) Royal Decree no 8 of 7 February 1995 establishing the purposes, criteria, conditions and of authorized processing operations of the data referred to in article 8 of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, modified by Royal Decree no 17 of 21 November 1996;

8) Royal decree no 9 of 7 February 1995 on granting exemptions of the application of article 9 of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data and establishing a procedure of collective information provision to the individuals certain processing operations relate to, modified by Royal Decree no 15 of 12 March 1996;

9) Royal Decree no 12 of 7 March 1995 establishing the fees to be paid to the Commission for the Protection of the Privacy upon notification of the processing operations performed on personal data, modified by Royal Decree no 12bis of 12 March 1996;

17 18

10) Royal Decree no 13 of 12 March 1996 on the conditional exemption from the duty of notification for certain types of automatic processing operations of personal data implying no apparent risk concerning privacy violation, modified by the Royal Decree of 18 April 1996;

11) Royal Decree no 14 of 22 May 1996 establishing the purposes, criteria and conditions for authorized procession of the data referred to in article 6 of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data.

Art 73. The present decree shall enter into force on the first day of the sixth month following the decree's month of publication in the Belgian Official Journal.

Art 74. Our Minister of Justice is in charge of implementing this decree.

Issued in Brussels, 13 February 2001.

ALBERT

Under Royal Authority:

The Minister of Justice,

M. VERWILGHEN

附錄四、德國聯邦個人資料保護法

Federal Data Protection Act (BDSG)
In the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66),
last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I,
p. 2814),
in force from 1 September 2009
The changes effective 1 April 2010 and 11 June 2010 are printed in italics. See footnote for date effective.

Table of Contents

law

Chapter 1

Federal Data Protection Act (BDSG) As at 1 September 2009 with amendments 2010

3

Legal basis for data processing

Chapter 2

Rights of the data subject

Chapter 3

Supervisory authority

Part IV

Special provisions

Part I

General and common provisions

Section 1 Purpose and scope

(1) The purpose of this Act is to protect individuals against infringement of their right
to privacy as the result of the handling of their personal data.
(2) This Act shall apply to the collection, processing and use of personal data by
1. public bodies of the Federation,
2. public bodies of the *Länder*, where data protection is not covered by *Land* legislation and where the *Länder*
a) execute federal law, or
b) act as judiciary bodies and administrative matters are not involved,
3. private bodies
that collect data for use in data processing systems, or use such systems to process
or use data, or collect data in or from non-automated filing systems, or use such
systems to process or use data, unless the data are collected, processed or

used
solely for personal or domestic activities.
(3) Where other federal laws apply to personal data and their publication, they shall
take precedence over the provisions of this Act. The obligation to abide by legal
obligations of secrecy or professional or special official secrecy not based on law
shall remain unaffected.
(4) The provisions of this Act shall take precedence over those of the Administrative
Procedures Act where personal data are processed in ascertaining the facts.
(5) This Act shall not apply in so far as a controller located in another European Union Member State or another state party to the Agreement on the European Economic Area collects, processes or uses personal data inside the country, except
where such collection, processing or use is carried out by a branch inside the country. This Act shall apply in so far as a controller not located in a European Union
Member State or other state party to the Agreement on the European Economic Area
collects, processes or uses personal data inside the country. In so far as the controller is to be named under this Act, information on representatives located inside
the country shall also be furnished. Sentences 2 and 3 shall not apply where data
storage media are used solely for the purpose of transit through the country. Section
38 (1) first sentence shall remain unaffected.

Section 2 Public and private bodies

(1) “Public bodies of the Federation” shall mean the authorities, judiciary bodies and
other public-law institutions of the Federation, of the direct federal corporations,
institutions and foundations under public law as well as their associations irrespective
of their legal forms. The successor companies created by law from the Special Fund

“Deutsche Bundespost” shall be considered public bodies as long as they have an
exclusive right under the Postal Act.
(2) “Public bodies of the *Länder*” shall mean the authorities, judiciary bodies and
other public-law institutions of a *Land*, of a municipality, an association of

municipalities or other legal persons under public law subject to *Land* supervision as
well as their associations irrespective of their legal forms.
(3) Private-law associations of public bodies of the Federation and the *Länder* performing public administration tasks shall be considered public bodies of the Federation irrespective of private shareholdings if
1. they operate in more than one *Land*, or
2. the Federation possesses the absolute majority of shares or votes.
Otherwise, they shall be regarded as public bodies of the *Länder*.
(4) “Private bodies” shall mean natural or legal persons, companies and other private-law associations not covered by subsections 1 through 3. If a private body
performs sovereign public administration tasks, it shall be a public body within the
meaning of this Act.

Section 3 Further definitions

(1) “Personal data” shall mean any information concerning the personal or material circumstances of an identified or identifiable natural person (“data subject”).
(2) “Automated processing” shall mean the collection, processing or use of personal data by means of data processing systems. A “non-automated filing system”
shall mean any non-automated collection of personal data which is similarly structured and which can be accessed and evaluated according to specific characteristics.
(3) “Collection” shall mean the acquisition of data on the data subject.
(4) “Processing” shall mean the recording, alteration, transfer, blocking and erasure of personal data. Specifically, irrespective of the procedures applied,
1. “recording” shall mean the entry, recording or preservation of personal data on a storage medium so that they can be further processed or used,

2. “alteration” shall mean the modification of the substance of recorded personal
data,
3. “transfer” shall mean the disclosure of personal data recorded or obtained by
data processing to a third party either
a) through transfer of the data to a third party, or
b) by the third party inspecting or retrieving data available for inspection or retrieval,
4. “blocking” shall mean the identification of recorded personal data so as to restrict their further processing or use,
5. “erasure” shall mean the deletion of recorded personal data.
(5) “Use” shall mean any utilization of personal data other than processing.
(6) “Rendering anonymous” shall mean the alteration of personal data so that information concerning personal or material circumstances cannot be attributed to an
identified or identifiable natural person or that such attribution would require a disproportionate amount of time, expense and effort.

(6a) “Aliasing” shall mean replacing the data subject’s name and other identifying
features with another identifier in order to make it impossible or extremely difficult to
identify the data subject.
(7) “Controller” shall mean any person or body which collects, processes or uses
personal data on his, her or its own behalf, or which commissions others to do the
same.
(8) ‘Recipient’ shall mean any person or body to whom or which data are disclosed.
‘Third party’ shall mean any person or body other than the controller. Third parties
shall not mean the data subject or persons or bodies collecting, processing or using
personal data in Germany, in another European Union Member State or another

state party to the Agreement on the European Economic Area.
(9) ‘Special categories of personal data’ shall mean information on racial or ethnic
origin, political opinions, religious or philosophical beliefs, trade-union membership,
health or sex life.
(10) ‘Mobile personal storage and processing media’ shall mean data storage media
1. which are issued to the data subject,
2. on which personal data can be processed automatically, in addition to the storage function, by the issuing body or another body, and
3. which the data subject must use to influence such processing.
(11) ‘Employees’ shall mean
1. employees,
2. persons employed for the purpose of occupational training,
3. persons participating in measures to integrate them into the labour market or
to clarify their ability or suitability for work (rehabilitation measures),
4. persons employed at certified workshops for persons with a disability,
5. persons employed under the Youth Volunteer Service Act,
6. persons comparable to employees due to their economic dependence, including home-based workers and those of similar status,
7. applicants for employment and those whose employment has ended,
8. civil servants, federal judges, military personnel and persons in the alternative civilian service.

Section 3a Data reduction and data economy

Personal data shall be collected, processed and used, and data processing systems
shall be chosen and organized in accordance with the aim of collecting, processing
and using as little personal data as possible. In particular, personal data shall be
rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection.

Section 4 Lawfulness of data collection, processing and use

(1) The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent.
(2) Personal data shall be collected from the data subject. They may be collected
without the data subject's participation only if
1. allowed or required by law, or
2. a) the data must be collected from other persons or bodies due to the nature of the administrative task to be performed or the commercial purpose, or
b) collecting the data from the data subject would require disproportionate effort
and there are no indications that overriding legitimate interests of the data subject
would be adversely affected.
(3) If personal data are collected from the data subject, the controller shall inform
him/her as to
1. the identity of the controller,
2. the purposes of collection, processing or use, and
3. the categories of recipients only where, given the circumstances of the individual case, the data subject need not expect that his/her data will be transferred to such recipients,
unless the data subject is already aware of this information. If personal data are
collected from the data subject pursuant to a law requiring the provision of such
information, or if providing this information is required for the granting of legal benefits, the data subject shall be informed that providing this information is required
or voluntary, as the case may be. The law and the consequences of refusing to provide information shall be explained to the data subject as necessary in the individual case.

Section 4a Consent

(1) Consent shall be effective only when based on the data subject's free decision.
Data subjects shall be informed of the purpose of collection, processing or use and,

as necessary in the individual case or on request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances
warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance.
(2) In the field of scientific research, a special circumstance as referred to in subsection 1 third sentence shall be deemed to exist if the defined purpose of research would be seriously affected if consent were obtained in writing. In this case,
the information referred to in subsection 1 second sentence and the reasons the
defined purpose of research would be seriously affected shall be recorded in writing.
(3) Where special categories of personal data (Section 3 (9)) are collected, processed or used, the consent must also refer specifically to these data.

Section 4b Transfer of personal data abroad and to supranational or intergovernmental bodies

(1) The transfer of personal data to bodies
1. in other European Union Member States,
2. in other states parties to the Agreement on the European Economic Area, or
3. of the institutions of the European Communities
shall be subject to Section 15 (1), Section 16 (1) and Sections 28 through 30a in
accordance with the laws and agreements applicable to such transfers, if data are
transferred in connection with activities which fall fully or partly within the scope of the
law of the European Communities.
(2) Subsection 1 shall apply accordingly to transfers of personal data to bodies under
subsection 1, if data are transferred in connection with activities which do not fall
within the scope of the law of the European Communities, and to transfers of personal data to other bodies abroad or to supranational or intergovernmental bodies. Personal data shall not be transferred if the data subject has a legitimate

interest in ruling out the possibility of transfer, especially if the bodies listed in the first
sentence fail to ensure an adequate level of data protection. The second sentence
shall not apply if transfer is necessary for a public body of the Federation to carry out
its duties for compelling reasons of defence or to fulfil supranational or intergovernmental obligations in the field of crisis management or conflict prevention
or for humanitarian measures.
(3) The adequacy of the level of protection afforded shall be assessed in the light
of all the circumstances surrounding a data transfer operation or set of data transfer
operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing, the country of origin and country of
final destination, the rules of law, both general and sectoral, applicable to the recipient and the professional rules and security measures applicable to the recipient.
(4) In the cases referred to in Section 16 (1) no. 2, the body transferring the data
shall inform the data subject of the data transfer. This shall not apply if it can be
assumed that the data subject will otherwise acquire this information, or if informing
the data subject would endanger public safety or otherwise be detrimental to the
Federation or a *Land*.
(5) The body transferring the data shall be responsible for ensuring the lawfulness
of the transfer.
(6) The body to which the data are transferred shall be informed of the purpose for which the data are being transferred.

Section 4c Derogations

(1) In connection with activities which fall fully or partly within the scope of the law of
the European Communities, the transfer of personal data to bodies other than

those
listed in Section 4b (1) shall be lawful, even if they do not ensure an adequate level
of data protection, if
1. the data subject has given his/her consent,

10
2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request,
3. the transfer is necessary for the conclusion or performance of a contract which has been or is to be concluded in the interest of the data subject between the controller and a third party,
4. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims,
5. the transfer is necessary in order to protect the vital interests of the data subject, or
6. the transfer is made from a register which is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law are fulfilled in the particular case.
The body to which the data are transferred shall be informed that the transferred data
may be processed or used only for the purpose for which they are being transferred.
(2) Without prejudice to subsection 1 first sentence, the competent supervisory authority may authorize a transfer or a set of transfers of personal data to bodies
other than those listed in Section 4b (1), where the controller adduces adequate
safeguards with respect to the protection of privacy and exercise of the corresponding rights; such safeguards may in particular result from contractual clauses or binding corporate regulations. The Federal Commissioner for Data Protection and Freedom of Information shall be responsible in the case of postal and
telecommunications companies. Where public bodies are to transfer personal data,
they shall undertake the examination referred to in the first sentence.

(3) The *Länder* shall notify the Federation of decisions made in accordance with
subsection 2 first sentence.

Section 4d Obligation to notify

(1) Before carrying out any automated processing operations, private controllers shall
notify the competent supervisory authority, while federal controllers and controllers of
postal and telecommunications companies shall notify the Federal Commissioner for
Data Protection and Freedom of Information in accordance with Section 4e.

(2) The obligation to notify shall not apply if the controller has appointed a data protection official.

(3) Further, the obligation to notify shall not apply if the controller collects, processes
or uses personal data for its own persons and no more than nine employees are
employed in collecting, processing or using personal data, and either the data subject
has given his/her consent or the collection, processing or use is needed to create,
carry out or terminate a legal obligation or a quasi-legal obligation with the data subject.

(3) Further, the obligation to notify shall not apply if the controller collects, processes
or uses personal data for its own persons and, as a rule, no more than nine employees are permanently employed in collecting, processing or using personal
data, and either the data subject has given his/her consent or the collection,

processing or use is needed to create, carry out or terminate a legal obligation or a
quasi-legal obligation with the data subject.[1]

(4) Subsections 2 and 3 shall not apply in case of automated processing in which the
controller commercially records personal data
1. for the purpose of transfer,

2. for the purpose of transfer in anonymous form, or
3. the purposes of market or opinion research.
(5) Where automated processing operations present special risks to the rights and
freedoms of data subjects, these operations shall be examined before the start of
processing (prior checking). Such prior checks shall be carried out in particular
1. if special categories of personal data (Section 3 (9)) are to be processed, or
2. the processing of personal data is intended to assess the data subject's personality and his/her abilities, performance or behaviour,
unless a statutory obligation applies, the data subject's consent has been given, or
the collection, processing or use is needed to create, carry out or terminate a legal
obligation or quasi-legal obligation with the data subject.
(6) The data protection official shall be responsible for conducting prior checks. The
data protection official shall carry out prior checks following receipt of the overview in
accordance with Section 4g (2) first sentence. In case of doubt, the data protection
official shall consult the supervisory authority or, in case of postal and telecommunications companies, the Federal Commissioner for Data Protection and
Freedom of Information.

Section 4e Contents of notification

Where automated processing operations are subject to the obligation to notify, they
shall include the following information:
1. name or company of the controller,
2. owners, management boards, managing directors or other managers appointed in accordance with the law or company regulations, and the persons in charge of data processing,
3. the controller's address,
4. the purposes of the data collection, processing or use,
5. a description of the category or categories of data subject and of the data or categories of data relating to them,
6. the recipients or categories of recipient to whom the data might be

disclosed,
7. standard data retention periods,
8. plans to transfer data to third countries,
9. a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Section 9 to ensure security of processing.

[1] In force from 1 April 2010.

Section 4d (1) and (4) shall apply accordingly to the amendment of information provided under the first sentence and to the start and conclusion of the activity subject to the obligation to notify.

Section 4f Data protection official

(1) Public and private bodies which process personal data by automated means shall appoint in writing a data protection official. Private bodies shall be obligated to appoint a data protection official within one month of commencing their activities. The same shall apply where personal data are collected, processed or used by other means and, as a rule, at least 20 persons are employed for this purpose. The first and second sentences shall not apply to private bodies in which, as a rule, no more than nine persons are permanently employed in the automated processing of personal data. One data protection official may be appointed for several areas where the structure of a public body so requires. Where private bodies carry out automated processing subject to prior checking, or commercially carry out automated processing of personal data for the purpose of transfer, transfer in anonymous form or for purposes of market or opinion research, they shall appoint a data protection official irrespective of the number of persons employed in automated processing.

(2) Only persons with the specialized knowledge and reliability necessary to carry out their duties may be appointed to serve as data protection officials. The

necessary
level of specialized knowledge is determined in particular by the extent of data processing carried out by the controller and the protection required by the personal
data collected or used by the controller. A person from outside the controller may be
appointed data protection official; monitoring shall also extend to personal data which
are subject to professional or special official secrecy, in particular tax secrecy under
Section 30 of the German Fiscal Code. With the consent of their supervisory authority, public bodies may appoint an employee from another public body as their
data protection official.
(3) Data protection officials shall be directly subordinate to the head of the public or
private body. They shall be free to use their specialized knowledge in the area of
data protection. They may not be penalized for performing their duties. The appointment of a data protection official may be revoked by applying Section 626 of
the Civil Code accordingly; in the case of private bodies, the appointment may be
revoked also at the request of the supervisory authority. If a data protection official is
to be appointed under subsection 1, then this employment may not be terminated,
unless the controller has just cause to terminate without notice. After the data protection official has been recalled, he or she may not be terminated for a year
following the end of appointment, unless the controller has just cause to terminate
without notice. The controller shall enable the data protection official to take part in
advanced training measures and shall assume the expense of such measures in
order for the data protection official to maintain the specialized knowledge to perform

his or her duties.
(4) Data protection officials shall be obligated to secrecy concerning the identity of
data subjects and concerning circumstances enabling data subjects to be identified,
unless they are released from this obligation by the data subject.

(4a) Where in the course of their activities data protection officials become aware of
data for which the head of a public or private body or a person employed by such a
body has the right to refuse to give evidence, this right shall also apply to data protection officials and their assistants. The person to whom the right to refuse to
give evidence applies for professional reasons shall decide whether to exercise this
right unless it is impossible to effect such a decision in the foreseeable future. Where
the right of data protection officials to refuse to give evidence applies, their files and
other documents shall not be subject to seizure.
(5) The public and private bodies shall support data protection officials in performing
their duties and shall provide assistants, premises, furnishings, equipment and other
resources as needed to perform these duties. Data subjects may contact the data
protection official at any time.

Section 4g Duties of the data protection official

(1) The data protection official shall work to ensure compliance with this Act and with
other data protection provisions. For this purpose, in case of doubt the data protection official may consult the competent authority responsible for monitoring the
controller’s data protection. The data protection official may make use of advising as
referred to in Section 38 (1) second sentence. In particular, the data protection

official
shall
1. monitor the proper use of data processing programs used to process personal data; for this purpose, the data protection official shall be informed in good time of projects for the automated processing of personal data,
2. take appropriate measures to familiarize persons employed in the processing
of personal data with the provisions of this Act and other data protection provisions, and with the various special requirements of data protection.
(2) The controller shall provide the data protection official with an overview of the
information listed in Section 4e, first sentence, and a list of persons entitled to access. The data protection official shall make the information referred to in Section
4e first sentence nos. 1 through 8 available in an appropriate form to any person on
request.
(2a) Where no obligation to appoint a data protection official applies at a private
body, the head of the private body shall ensure that the duties referred to in subsections 1 and 2 are performed by other means.
(3) Subsection 2 second sentence shall not apply to the authorities referred to in
Section 6 (2) fourth sentence. Subsection 1 second sentence shall apply on the
condition that the authority's data protection official contacts the head of the authority; any disagreements between the authority's data protection official and the
head of the authority shall be settled by the supreme federal authority.

Section 5 Confidentiality

Persons employed in data processing shall not collect, process or use personal data
without authorization (confidentiality). Such persons, when employed by private
bodies, shall be obligated when taking up their duties to maintain confidentiality. The
obligation of confidentiality shall continue after their employment ends.

14

Section 6 Inalienable rights of the data subject

Section 6 Rights of the data subject[2]

(1) The data subject's right of access (Sections 19, 34) and to rectification, erasure or
blocking (Sections 20, 35) may not be excluded or restricted by a legal transaction.

(2) If the data subject's data are recorded automatically in such a way that more than
one body is authorized to record the data, and the data subject is unable to determine which body recorded the data, the data subject may contact each of these
bodies. Each body shall be obligated to forward the data subject's request to the
body which recorded the data. The data subject shall be informed that the request
has been forwarded and to which body it was forwarded. If they record personal data
in performing their legally mandated duties within the scope of the German Fiscal
Code for purposes of monitoring and examination, the bodies listed in Section 19 (3),
the public prosecution authorities, the police and the public finance authorities may
inform the Federal Commissioner for Data Protection and Freedom of Information
instead of the data subject. In this case, the further procedure shall be based on
Section 19 (6).

*(3) Personal data concerning the data subject's exercise of a right based on this or
other data protection provisions may be used only to fulfil obligations of the controller
arising from the exercise of this right.*[3]

Section 6a Automated individual decisions

(1) Decisions which produce legal effects concerning the data subject or significantly
affect him/her may not be based solely on automated processing of personal

data
intended to evaluate certain personal aspects relating to him/her.
In particular, a decision not made by a natural person based on the evaluation of
content shall constitute a decision based solely on automated processing.[4]
(2) This shall not apply if
1. the decision is taken in the course of entering into or performing a contractual
relationship or other legal relationship, and the request lodged by the data subject has been satisfied, or
2. there are suitable measures to safeguard the data subject's legitimate interests and the controller informs the data subject that a decision within the meaning of subsection 1 has been taken. In particular, arrangements allowing data subjects to assert their point of view shall constitute suitable measures. The controller shall be obligated to review its decision.
2. there are suitable measures to safeguard the data subject's legitimate interests, the controller informs the data subject that a decision within the

[2] In force from 1 April 2010.

[3] In force from 1 April 2010.

[4] In force from 1 April 2010.

meaning of subsection 1 has been taken, and upon request explains the main reasons for this decision.[5]
(3) The data subject's right of access under Sections 19 and 34 shall also extend to
the logic involved in the automated processing of his or her personal data.

Section 6b Monitoring of publicly accessible areas with optic-electronic devices

(1) Monitoring publicly accessible areas using optic-electronic devices (video surveillance) shall be lawful only as far as necessary
1. for public bodies to perform their duties,
2. to exercise the right to determine who shall be allowed or denied access, or
3. to pursue legitimate interests for specifically defined purposes,
and there are no indications of overriding legitimate interests of the data subject.
(2) Suitable measures shall be taken to make clear that the area is being monitored

and to identify the controller.
(3) Data collected under subsection 1 may be processed or used if necessary to
achieve the intended purposes and if there are no indications of overriding legitimate
interests of the data subject. These data may be processed or used for another purpose only if necessary to prevent threats to state and public security or to prosecute crimes.
(4) Where a specific person can be identified using data collected through video
surveillance, the person shall be notified of processing or use in accordance with
Sections 19a and 33.
(5) The data shall be erased as soon as they are no longer needed to achieve the
purpose or if further storage would conflict with legitimate interests of the data subject.

Section 6c Mobile storage and processing media for personal data

(1) A body which issues mobile storage and processing media for personal data or
which applies to such media a procedure for the automated processing of personal
data which runs wholly or partly on such media, or which alters or makes available
such a procedure shall
1. inform the data subject of its identity and address,
2. explain to the data subject, in generally understandable terms, how the medium works, including the type of personal data to be processed,
3. inform the data subject how to exercise his or her rights under Sections 19, 20, 34 and 35, and
4. inform the data subject what measures are to be taken in case the medium is
lost or destroyed, if the data subject is not already aware of this.
(2) The body subject to the obligations in subsection 1 shall ensure that devices or
facilities necessary for data subjects to exercise their right of access are available in
sufficient quantity for use free of charge.

[5] In force from 1 April 2010.

(3) Communication operations which initiate data processing on the medium must be
clearly apparent to the data subject.

Section 7 Compensation

If a controller harms a data subject through collection, processing or use of his or her
personal data which is unlawful or improper under this Act or other data protection
provisions, the controller or its supporting organization shall be obligated to compensate the data subject for damage suffered. The obligation to provide compensation shall be waived if the controller exercised due care in the case.

Section 8 Compensation in case of automated data processing by public bodies

(1) If a public body harms a data subject through collection, processing or use of his
or her personal data which is unlawful or improper under this Act or other data protection provisions, the body's supporting organization shall be obligated to compensate the data subject for damage suffered irrespective of any fault.

(2) In case of a serious violation of privacy, the data subject shall receive appropriate
financial compensation for non-financial damage suffered.

(3) Claims under subsections 1 and 2 shall be limited to a total of € 130,000. If compensation exceeding the maximum of € 130,000 is to be paid to more than one
person due to the same incident, the compensation paid to each person shall be
reduced in proportion to the maximum amount.

(4) If, in the case of automated processing, more than one body is authorized to
record data and the injured person is unable to determine which body recorded his/her data, then each body shall be liable.

(5) Section 254 of the Civil Code shall apply to contributory negligence on the part of
the data subject.

(6) The limitation provisions stipulated for tortious acts in the Civil Code shall

apply
accordingly with regard to statutory limitation.

Section 9 Technical and organizational measures

Public and private bodies which collect, process or use personal data on their own
behalf or on behalf of others shall take the necessary technical and organizational
measures to ensure the implementation of the provisions of this Act, especially the
requirements listed in the Annex to this Act. Measures shall be necessary only if the
effort required is in reasonable proportion to the desired purpose of protection.

Section 9a Data protection audit

In order to improve data protection and data security, suppliers of data processing
systems and programs, and bodies conducting data processing may have independent and approved experts examine and evaluate their data protection strategy and their technical facilities and may publish the results of this examination.
The detailed requirements pertaining to examination and evaluation, the procedure
and the selection and approval of experts shall be covered in a separate law.

Section 10 Automated retrieval procedures

(1) It shall be lawful to establish an automated procedure to retrieve personal data as
long as this procedure is appropriate in view of the legitimate interests of data

subjects and the tasks or commercial purposes of the bodies involved. Provisions on
the lawfulness of individual retrieval shall remain unaffected.
(2) The bodies involved shall ensure that the lawfulness of the retrieval procedure
can be monitored. For this purpose, they shall specify in writing:
1. the reason for and purpose of the retrieval procedure,
2. third parties to which data are transferred,
3. the type of data to be transferred,
4. technical and organizational measures required under Section 9.

In the public sector, the supervisory authorities may specify this information as necessary.
(3) In cases where the bodies referred to in Section 12 (1) are involved, the Federal Commissioner for Data Protection and Freedom of Information shall be informed when retrieval procedures are established and of the information specified under subsection 2. Establishing retrieval procedures in which the bodies referred to in Section 6 (2) and Section 19 (3) are involved shall be lawful only if the federal or *Land* ministry responsible for the recording body and the retrieving body has given its consent.
(4) The lawfulness of individual retrieval shall be the responsibility of the third party to which data are transferred. The recording body shall examine the lawfulness of retrieval only if there is cause for such examination. The recording body shall ensure that the transfer of personal data can be ascertained and checked at least by means of suitable random sampling procedures. If an entire collection of personal data is retrieved or transferred (batch processing), it shall be sufficient to ensure that the lawfulness of retrieval or transfer of the entire collection can be ascertained and checked.
(5) Subsections 1 through 4 shall not apply to the retrieval of generally accessible data. Generally accessible data are those which anyone can use, with or without prior registration, permission or the payment of a fee.

Section 11 Collection, processing or use of personal data on behalf of others

(1) If other bodies collect, process or use personal data on behalf of the controller,

the controller shall be responsible for compliance with the provisions of this Act and
other data protection provisions. The rights referred to in Sections 6, 7 and 8 shall be
asserted with regard to the controller.
(2) The processor shall be chosen carefully, with special attention to the suitability of
the technical and organizational measures applied by the processor. The work to be
carried out by the processor shall be specified in writing, including in particular the
following:
1. the subject and duration of the work to be carried out,
2. the extent, type and purpose of the intended collection, processing or use of data, the type of data and category of data subjects,
3. the technical and organizational measures to be taken under Section 9,
4. the rectification, erasure and blocking of data,
5. the processor's obligations under subsection 4, in particular monitoring,

6. any right to issue subcontracts,
7. the controller's rights to monitor and the processor's corresponding obligations to accept and cooperate,
8. violations by the processor or its employees of provisions to protect personal
data or of the terms specified by the controller which are subject to the obligation to notify,
9. the extent of the controller's authority to issue instructions to the processor,
10. the return of data storage media and the erasure of data recorded by the processor after the work has been carried out.
In case of public bodies, the work to be carried out may also be specified by the
authority responsible for expert supervision. The controller shall verify compliance
with the technical and organizational measures taken by the processor before data
processing begins and regularly thereafter. The result shall be documented.
(3) The processor may collect, process or use the data only as instructed by

the
controller. If the processor believes that an instruction by the controller violates this
Act or other data protection provisions, the processor shall inform the controller of
this immediately.
(4) For the processor, other than Sections 5, 9, 43 (1) no. 2, Sections 10 and 11 (2)
nos. 1 through 3 and (3), and Section 44, only the provisions on data protection
monitoring or supervision shall apply, namely for
1. a) public bodies,
b) private bodies, when the majority of shares or votes is publicly owned and the controller is a public body,
Sections 18, 24 through 26 or the corresponding provisions of the data protection laws of the *Länder*,
2. other private bodies, where they collect, process or use personal data on behalf of others for commercial purposes as service providers, Sections 4f, 4g and 38.
(5) Subsections 1 through 4 shall apply accordingly if other bodies carry out the
inspection or maintenance of automated procedures or data processing systems and
the possibility of access to personal data during such inspection and maintenance
cannot be ruled out.

Part II

Data processing by public bodies

Chapter 1

Legal basis for data processing

Section 12 Scope

(1) The provisions of this Part shall apply to public bodies of the Federation where
they are not engaged in competition as commercial enterprises under public law.

(2) Where data protection is not governed by *Land* law, Sections 12 through 16 and
Sections 19 and 20 shall also apply to the public bodies of the *Länder*, where they
1. execute federal law and are not engaged in competition as commercial enterprises under public law, or
2. act as judiciary bodies and administrative matters are not involved.
(3) Section 23 (4) shall apply accordingly to data protection officials at *Land* level.
(4) If personal data are collected, processed or used for the purpose of past, current
or future employment contracts, Section 28 (2) no. 2 and Sections 32 through 35
shall apply in the place of Sections 13 through 16 and Sections 19 and 20.

Section 13 Data collection

(1) Collecting personal data shall be lawful when the knowledge of such data is necessary for the controller to perform its tasks.
(1 a) If personal data are collected from a private body rather than from the data subject, this body shall be informed of the legal provision requiring the supply of information or that such supply is voluntary.
(2) Collecting special categories of personal data (Section 3 (9)) shall be lawful only where
1. allowed by law or urgently required for reasons of important public interest,
2. the data subject has given his consent in accordance with Section 4a (3),
3. necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent,
4. data are involved which the data subject has manifestly made public,
5. necessary to prevent a significant threat to the public security,
6. urgently required to prevent significant disadvantages to the common good or to preserve significant concerns of the common good,
7. required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where these data are processed by health professionals or other persons subject to the obligation of professional secrecy,
8. necessary for the purposes of scientific research, where the scientific interestin carrying out the research project significantly outweighs the data subject’s interest in ruling out the possibility of collection and the purpose of

the research cannot be achieved in any other way or would require a disproportionate effort, or
9. required for compelling reasons of defence or to fulfil supranational or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures.

Section 14 Recording, alteration and use of data

(1) The recording, alteration or use of personal data shall be lawful when required to
carry out the tasks for which the controller is responsible and for the purpose for

which the data were collected. If no prior collection took place, the data may be altered or used only for the purpose for which they were recorded.
(2) Recording, alteration or use for other purposes shall be lawful only if
1. allowed or required by law,
2. the data subject has given his consent,
3. this is clearly in the interest of the data subject and there is no reason to assume that the data subject would refuse to give his consent if he knew of such other purpose,
4. information supplied by the data subject must be checked because there is reason to believe this information is incorrect,
5. the data are generally accessible or the controller would be allowed to publish them, unless the data subject has a clear and overriding legitimate interest in ruling out the possibility of a change of purpose,
6. required to prevent significant disadvantages to the common good or a threat
to public security or to preserve significant concerns of the common good,
7. required to prosecute criminal or administrative offences, to enforce sentences or measures within the meaning of Section 11 (1) no. 8 of the Criminal Code or of reformatory or disciplinary measures within the meaning of the Youth Courts Act or to enforce decisions on fines,
8. required to prevent a serious infringement of the rights of another person, or
9. necessary for the purposes of scientific research, where the scientific interest
in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection and the purpose of the research cannot be achieved in any other way or would require a

disproportionate effort.
(3) Processing or use for the purpose of exercising supervisory and monitoring authority, of auditing or conducting organizational studies for the controller shall not
constitute processing or use for other purposes. This shall also apply to processing
or use for training or examination purposes by the controller, unless the data subject
has overriding legitimate interests.
(4) Personal data recorded exclusively for purposes of monitoring data protection,
safeguarding data or ensuring proper operation of a data processing system may
only be used for these purposes.
(5) Recording, altering or using special categories of personal data (Section 3 (9)) for
other purposes shall be lawful only if
1. the conditions are met which would allow collection under Section 13 (2) nos.
1 through 6 or 9, or
2. necessary for the purposes of scientific research, where the public interest in
carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort.

In weighing the public interest under the first sentence, no. 2, special attention shall
be paid to the scientific interest in the research project.
(6) Recording, altering or using special categories of personal data (Section 3 (9)) for
the purposes referred to in Section 13 (2) no. 7 shall be subject to the obligation of
secrecy which applies to the persons referred to in Section 13 (2) no. 7.

Section 15 Transfer of data to public bodies

(1) Transfer of personal data to public bodies shall be lawful if

1. required to carry out the tasks for which the body transferring the data or the third party to which the data are transferred is responsible, and
2. the conditions are met which would allow use under Section 14.
(2) The body transferring the data shall be responsible for ensuring the lawfulness of the transfer. If the data are transferred at the request of the third party to which the data are transferred, the third party shall be responsible. In this case, the body transferring the data shall examine only whether the request for transfer lies within the remit of the third party to which the data are transferred, unless there is special reason to examine the lawfulness of transfer. Section 10 (4) shall remain unaffected.
(3) The third party to which the data are transferred may process or use these data for the purpose for which they were transferred. Processing or use for other purposes shall be lawful only under the conditions of Section 14 (2).
(4) Subsections 1 through 3 shall apply accordingly to the transfer of personal data to religious associations under public law, if it is ensured that these religious associations take sufficient data protection measures.
(5) If personal data which may be transferred under subsection 1 are linked to other personal data of the data subject or a third party in such a way that they cannot be separated without a disproportionate effort, then it shall be lawful to transfer also these data, unless the data subject or a third party clearly has an overriding legitimate interest in keeping them secret; use of these data shall not be lawful.
(6) Subsection 5 shall apply accordingly if personal data are transferred within the same public body.

Section 16 Transfer of data to private bodies

(1) Transfer of personal data to private bodies shall be lawful if
1. required to carry out the tasks for which the transferring party is responsible and the conditions are met which would allow use under Section 14, or

2. the third party to which the data are transferred provides credible evidence of
its legitimate interest in knowledge of the data to be transferred and the data subject has no legitimate interest in ruling out the possibility of transfer. By way of derogation from the first sentence no. 2, the transfer of special categories of personal data (Section 3 (9)) shall be lawful only if the conditions are met which would allow use under Section 14 (5) and (6) or as far as necessary for the establishment, exercise or defence of legal claims.
(2) The body transferring the data shall be responsible for ensuring the lawfulness of
the transfer.

(3) In the cases referred to in subsection 1 no. 2, the body transferring the data shall
inform the data subject of the transfer of his/her data. This shall not apply if it can be
assumed that the data subject will otherwise acquire this information, or if informing
the data subject would endanger public safety or otherwise be detrimental to the
Federation or a *Land*.
(4) The third party to which the data are transferred may process or use these data
only for the purpose for which they were transferred. The transferring body shall point
this out to the third party. Processing or use for other purposes shall be lawful if transfer would be lawful under subsection 1 and the transferring body has consented.

Section 17 (deleted)

Section 18 Implementation of data protection in the federal administration

(1) The supreme federal authorities, the president of the Federal Railway Property
Agency, and the direct federal corporations, institutions and foundations under public
law subject only to legal supervision by the Federal Government or a supreme federal authority shall ensure that this Act and other data protection provisions

are
implemented within their area of responsibility. The same shall apply to the boards of
directors of the successor companies created by law from the Special Fund “Deutsche Bundespost” as long as they have an exclusive right under the Postal Act.
(2) The public bodies shall keep a register of the data processing systems used. For
their automated processing, they shall record in writing the information under Section
4e and the legal basis for processing. This requirement may be waived in the case of
automated processing for administrative purposes which does not restrict the data
subject’s right of access under Section 19 (3) or (4). The written records may be
combined for automated processing conducted more than once in the same or similar manner.

Chapter 2

Rights of the data subject

Section 19 Access to data

(1) Upon request, data subjects shall be given information on
1. recorded data relating to them, including information relating to the source of the data,
2. the recipients or categories of recipients to which the data are transferred, and
3. the purpose of recording the data.
The request should specify the type of personal data on which information is to be
given. If the personal data are recorded neither in automated form nor in nonautomated
filing systems, this information shall be provided only if the data subject provides information enabling the data to be located and if the effort required is not
disproportionate to the data subject’s interest in the information. The controller shall
exercise due discretion in determining the procedure for providing such

information
and in particular the form in which it is provided.

23
(2) Subsection 1 shall not apply to personal data recorded only because they may
not be erased due to legal, statutory or contractual provisions on retention, or only for
purposes of monitoring data protection or safeguarding data, and providing information would require a disproportionate effort.
(3) If the provision of information relates to the transfer of personal data to authorities
for the protection of the constitution, to the Federal Intelligence Service, the Military
Counterintelligence Service and, as far as the security of the Federation is concerned, other agencies of the Federal Ministry of Defence, such provision shall be
lawful only with the consent of these bodies.
(4) Information shall not be provided if
1. the information would endanger the orderly performance of tasks for which the controller is responsible,
2. the information would threaten the public security or order or otherwise be detrimental to the Federation or a *Land*, or
3. the data or the fact of their recording, in particular due to the overriding legitimate interests of a third party, must be kept secret by law or due to the nature of the data,
and therefore the data subject's interest in obtaining information shall not take precedence.
(5) No reasons must be given for refusing to provide information if stating the actual
and legal grounds for refusal would threaten the purpose of refusing to provide information. In this case, data subjects shall be informed of the possibility to contact
the Federal Commissioner for Data Protection and Freedom of Information.
(6) If no information is provided to the data subject, at the data subject's request this
information shall be supplied to the Federal Commissioner for Data Protection and

Freedom of Information unless the relevant supreme federal authority finds in the
individual case that doing so would endanger the security of the Federation or a
Land. The information provided by the Federal Commissioner to the data subject
may not provide any indication of the knowledge available to the controller without its
consent.
(7) Information shall be provided free of charge.

Section 19a Notification

(1) If data are collected without the data subject's knowledge, he or she shall be
notified of such recording, the identity of the controller and the purposes of collection,
processing or use. The data subject shall also be notified of recipients or categories
of recipients except where he or she must expect transfer to such recipients. If a
transfer is planned, notification shall be provided no later than the first transfer.
(2) Notification shall not be required if
1. the data subject already has this information,
2. notifying the data subject would involve a disproportionate effort, or
3. recording or transfer of personal data is expressly laid down by law.
The controller shall stipulate in writing the conditions under which notification shall
not be provided in accordance with no. 2 or 3.

(3) Section 19 (2) through (4) shall apply accordingly.

Section 20 Rectification, erasure and blocking of data; right to object

(1) Personal data shall be rectified if they are inaccurate. If personal data neither
processed in automated form nor recorded in non-automated filing systems are found
to be inaccurate, or if the data subject disputes their accuracy, this shall be documented in an appropriate manner.
(2) Personal data processed in automated form or recorded in non-automated

filing
systems shall be erased if
1. unlawfully recorded, or
2. the controller no longer needs them to carry out the tasks for which it is responsible.
(3) Instead of being erased, data shall be blocked if
1. erasure would violate retention periods set by law, statute or contract,
2. there is reason to believe that erasure would adversely affect legitimate interests of the data subject, or
3. erasure would be impossible or would involve a disproportionate effort due to
the special category of recording.
(4) Further, personal data processed in automated form or recorded in nonautomated
filing systems shall be blocked if the data subject disputes their accuracy and their accuracy or inaccuracy cannot be verified.
(5) Personal data may not be collected, processed or used for processing in automated form or in non-automated filing systems if the data subject lodges an
objection with the controller and examination indicates that legitimate interests of the
data subject due to his particular personal situation override the interest of the controller in such collection, processing or use. The first sentence shall not apply if
collection, processing or use is required by law.
(6) Personal data which are neither processed in automated form nor recorded in
non-automated filing systems shall be blocked if the authority finds in the particular
case that, in the absence of blocking, legitimate interests of the data subject would
be adversely affected and the data are no longer needed for the authority to carry out
its tasks.
(7) Blocked data may be transferred or used without the data subject’s consent only if
1. it is vital for scientific purposes, to supply necessary evidence, or for other reasons in the overriding interest of the controller or a third party, and

2. the transfer or use of the data for this purpose would be allowed if the data were not blocked.
(8) The bodies to which these data were transferred for recording shall be informed
of the rectification of inaccurate data, the blocking of disputed data and erasure or
blocking due to unlawful recording, if this does not involve a disproportionate effort
and does not conflict with legitimate interests of the data subject.
(9) Section 2 (1) through (6), (8) and (9) of the Federal Archives Act shall be applied
accordingly.

Section 21 Appeals to the Federal Commissioner for Data Protection and Freedom of Information

Anyone who believes his or her rights have been infringed through the collection,
processing or use of his or her personal data by public bodies of the Federation may
appeal to the Federal Commissioner for Data Protection and Freedom of Information.
This shall apply to the collection, processing or use of personal data by federal courts
only where they are active in administrative matters.

Chapter 3

Federal Commissioner for Data Protection and Freedom of Information

Section 22 Election of the Federal Commissioner for Data Protection and Freedom of Information

(1) At the proposal of the Federal Government, the German Bundestag shall elect the
Federal Commissioner for Data Protection and Freedom of Information with more
than half of the statutory number of its members. The Federal Commissioner must be
at least 35 years old at the time of election. The person elected shall be appointed by

the Federal President.
(2) The Federal Commissioner shall swear the following oath before the Federal
Minister of the Interior:
“I swear to do everything in my power to further the good and the benefit of the German people, to protect them from harm and to defend the Basic Law and the laws of the Federation, to perform my duties conscientiously and to exercise
justice in all my dealings, so help me God.”
The reference to God may be omitted from the oath.
(3) The Federal Commissioner’s term of office shall be five years. It may be renewed
once.
(4) The Federal Commissioner shall, in accordance with this Act, have official federal
status under public law. He or she shall be independent in the performance of his or
her duties and subject only to the law. He or she shall be subject to the legal supervision of the Federal Government.
(5) The Federal Commissioner shall be established at the Federal Ministry of the
Interior. He or she shall be subject to the administrative supervision of the Federal
Ministry of the Interior. The Federal Commissioner shall be provided with the staff
and material resources necessary to carry out his or her tasks; these resources shall
be shown in a separate chapter of the budget of the Federal Minister of the Interior.
The posts shall be filled in agreement with the Federal Commissioner. Staff members
who do not agree to the intended measure may be transferred, seconded or reassigned only in agreement with the Federal Commissioner.
(6) If the Federal Commissioner is temporarily prevented from performing his or her
duties, the Federal Minister of the Interior may appoint a deputy to perform these
duties. The Federal Commissioner shall be consulted on the appointment.

26

Section 23 Legal status of the Federal Commissioner for Data Protection and
Freedom of Information

(1) The mandate of the Federal Commissioner for Data Protection and Freedom of
Information shall commence on delivery of the certificate of appointment. It shall end
1. on expiry of the term of office,
2. on dismissal.
The Federal President shall dismiss the Federal Commissioner at the latter's request
or at the suggestion of the Federal Government where there are grounds which
would justify dismissal from service in the case of a judge with life tenure. In the
event that the appointment is ended, the Federal Commissioner shall be given a
document signed by the Federal President. Dismissal shall be effective on delivery of
this document. At the request of the Federal Minister of the Interior, the Federal
Commissioner shall be obligated to continue his or her work until a successor has
been appointed.
(2) The Federal Commissioner shall not hold any other paid office or pursue any
commercial activity or occupation in addition to his or her official duties and shall not
belong to the management or supervisory board of a profit-oriented enterprise, nor to
a government or legislative body of the Federation or a *Land*. The Federal
Commissioner may not deliver extra-judicial opinions in exchange for payment.
(3) The Federal Commissioner shall inform the Federal Ministry of the Interior of any
gifts received in connection with his or her office. The Federal Ministry of the
Interior

shall decide how such gifts shall be used.
(4) The Federal Commissioner shall have the right to refuse to give testimony concerning persons who have confided in him/her in his/her capacity as Federal Commissioner and concerning the information confided. This shall also apply to the staff of the Federal Commissioner, on the condition that the Federal Commissioner decides on the exercise of this right. Within the scope of the Federal Commissioner's right of refusal to give testimony, he or she may not be required to submit or surrender files or other documents.
(5) Even after his or her appointment has ended, the Federal Commissioner shall be obligated to secrecy concerning matters of which he/she is aware by reason of his/her duties. This shall not apply to official communications or to matters which are common knowledge or which by their nature do not require confidentiality. Even after leaving office, the Federal Commissioner may not testify in or outside court or make statements concerning such matters without the permission of the Federal Ministry of the Interior. This shall not affect the legal obligation to report crimes and to uphold the free and democratic order wherever it is threatened. Sections 93, 97, 105 (1), Section 111 (5) in conjunction with Section 105 (1) and Section 116 (1) of the German Fiscal Code shall not apply to the Federal Commissioner and his or her staff. The fifth sentence shall not apply where the financial authorities require such knowledge in order to conduct legal proceedings due to a tax offence and related tax proceedings, in the prosecution of which there is compelling public interest, or where the person required to provide information or persons acting on his/her behalf have

intentionally provided false information. If the Federal Commissioner determines that
data protection provisions have been violated, he or she shall be authorized to report
the violation and inform the data subject accordingly.

27
(6) Permission to testify as a witness may be refused only if the testimony would be
detrimental to the welfare of the Federation or a *Land*, or would seriously endanger
or significantly interfere with the execution of public duties. Permission to provide a
report may be refused if providing a report would be detrimental to official interests.
Section 28 of the Act on the Federal Constitutional Court shall remain unaffected.
(7) From the start of the calendar month in which the Federal Commissioner's appointment commences until the end of the calendar month in which his/her appointment ends, or, in the case of subsection 1 sixth sentence, until the end of the
month in which he/she ceases his/her work, the Federal Commissioner shall be paid
at the level of a federal civil servant in pay grade B 9. The Federal Travel Expenses
Act and the Federal Relocation Expenses Act shall apply accordingly. In all other
respects, Section 12 (6), Sections 13 through 20 and 21a (5) of the Act on Federal
Ministers shall apply, except that the four-year term of office stipulated in Section 15
(1) of the Act on Federal Ministers shall be replaced by a five-year term and pay
grade B 11 stipulated in Section 21a (5) of the Act on Federal Ministers shall be
replaced by pay grade B 9. By way of derogation from the third sentence in conjunction with Sections 15 through 17 and 21a (5) of the Act on Federal Ministers,

the Federal Commissioner’s pension shall be calculated, counting his or her term as
Federal Commissioner as a pensionable period of service, on the basis of the Federal Act Governing Civil Servants' Pensions and Allowances, if this is more favourable and if, before his or election as Federal Commissioner, he or she was a
civil servant or judge in at least the last position to be held before reaching pay grade
B 9.
(8) Subsection 5, fifth through seventh sentences shall apply accordingly to the public
bodies responsible for monitoring compliance with data protection provisions in the
Länder.

Section 24 Monitoring by the Federal Commissioner for Data Protection and
Freedom of Information

(1) The Federal Commissioner for Data Protection and Freedom of Information shall
monitor compliance by the public bodies of the Federation with the provisions of this
Act and other data protection provisions.
(2) Monitoring by the Federal Commissioner shall also extend to
1. personal data obtained by public bodies of the Federation concerning the contents of and specific circumstances relating to postal communications and telecommunications, and
2. personal data subject to professional or special official secrecy, especially tax
secrecy under Section 30 of the German Fiscal Code.
The fundamental right to privacy of correspondence, posts and telecommunications
in Article 10 of the Basic Law shall be thus restricted. Personal data subject to monitoring by the commission established under Section 15 of the Act to Restrict the
Privacy of Correspondence, Posts and Telecommunications shall not be subject to
monitoring by the Federal Commissioner unless the commission requests the Federal Commissioner to monitor compliance with data protection provisions

in
connection with specific procedures or in specific areas and to report solely to the
commission. Personal data in files on background security checks shall not be subject to monitoring by the Federal Commissioner if the data subject lodges an

28
objection with the Federal Commissioner concerning the monitoring of data relating
to the data subject in the particular case.
(3) The federal courts shall be subject to monitoring by the Federal Commissioner
only where they are active in administrative matters.
(4) The public bodies of the Federation shall be obligated to assist the Federal Commissioner and his or her assistants in performing their duties. In particular, they
shall be given
1. information in reply to their questions, as well as the opportunity to inspect all
documents and especially recorded data and data processing programs in connection with monitoring under subsection 1,
2. access to all official premises at all times.
The authorities referred to in Section 6 (2) and Section 19 (3) shall provide assistance only to the Federal Commissioner him- or herself and assistants specially
designated by him or her in writing. The second sentence shall not apply to these
authorities where the supreme federal authority finds in the particular case that the
information or inspection would endanger the security of the Federation or a *Land*.
(5) The Federal Commissioner shall inform the public body of the monitoring results.
The Federal Commissioner may include recommendations for improving data protection, especially for remedying problems found in the processing or use of personal data. Section 25 shall remain unaffected.
(6) Subsection 2 shall apply accordingly to the public bodies responsible for

monitoring compliance with data protection provisions in the *Länder*.

Section 25 Complaints lodged by the Federal Commissioner for Data Protection and Freedom of Information

(1) If the Federal Commissioner for Data Protection and Freedom of Information finds
violations of the provisions of this Act or other data protection provisions or other
problems with the processing or use of personal data, he or she shall lodge a complaint
1. in the case of the federal administration: with the competent supreme federal
authority,
2. in the case of the Federal Railway Property Agency: with its president,
3. in the case of successor companies created by law from the Special Fund “Deutsche Bundespost” as long as they have an exclusive right under the Postal Act: with their boards of directors,
4. in the case of direct federal corporations, institutions and foundations under public law as well as their associations: their boards of directors or other bodies authorized to represent them,
and shall require them to respond within a period to be determined by the Federal
Commissioner. In the cases of the first sentence no. 4, the Federal Commissioner
shall inform the responsible supervisory authority at the same time.

(2) The Federal Commissioner may dispense with a complaint or a response from
the body concerned, especially if the problems involved are insignificant or have
been remedied in the meantime.

(3) The response should also describe the measures taken as a result of the Federal
Commissioner’s complaint. The bodies referred to in subsection 1, first sentence no.
4 shall provide the competent supervisory authority a copy of their response to the
Federal Commissioner at the same time.

Section 26 Additional duties of the Federal Commissioner for Data Protection
and Freedom of Information

(1) The Federal Commissioner for Data Protection and Freedom of Information shall submit an activity report to the German Bundestag every two years. The report shall inform the German Bundestag and the public about important developments in the field of data protection.

(2) At the request of the German Bundestag or the Federal Government, the Federal Commissioner shall draft expert opinions and provide reports. At the request of the German Bundestag, the Petitions Committee, the Bundestag's Committee on Internal Affairs or the Federal Government, the Federal Commissioner shall also investigate data protection matters and incidents at public bodies of the Federation. The Federal Commissioner may consult the German Bundestag at any time.

(3) The Federal Commissioner may make recommendations to the Federal Government and the federal bodies referred to in Section 12 (1) for improving data protection and may advise them in matters of data protection. The Federal Commissioner shall inform the bodies referred to in Section 25 (1) nos. 1 through 4 if the recommendation or advice does not concern them directly.

(4) The Federal Commissioner shall work to cooperate with the public bodies responsible for monitoring compliance with data protection provisions in the *Länder* and with the supervisory authorities under Section 38. Section 38 (1) third and fourth sentences shall apply accordingly.

(4) The Federal Commissioner shall work to cooperate with the public bodies responsible for monitoring compliance with data protection provisions in the Länder and with the supervisory authorities under Section 38. Section 38 (1) fourth

and fifth
sentences shall apply accordingly.[6]

Part III

Data processing by private bodies and commercial enterprises under public law

Chapter 1
Legal basis for data processing

Section 27 Scope

(1) The provisions of this Part shall apply as far as personal data are processed or used by means of data processing systems or collected for that purpose, or data are processed or used in or from non-automated filing systems or collected for that purpose by

1. private bodies,
2. a) public bodies of the Federation, where they are engaged in competition as commercial enterprises under public law,
b) public bodies of the *Länder*, where they are engaged in competition as commercial enterprises under public law, execute federal law and data protection is not governed by *Land* law.

This shall not apply where data are collected, processed or used solely for personal or domestic activities. In cases of no. 2 a, Sections 18, 21 and 24 through 26 shall apply in place of Section 38.

(2) The provisions of this Part shall not apply to the processing and use of personal data outside of non-automated filing systems, as long as the personal data have not clearly been obtained from automated processing.

Section 28 Collection and recording of data for own commercial purposes

(1) The collection, recording, alteration or transfer of personal data or their use

[6] In force from 1 April 2010.

as a
means to pursue own commercial purposes shall be lawful
1. if necessary to create, perform or terminate a legal obligation or quasi-legal obligation with the data subject,
2. as far as necessary to safeguard legitimate interests of the controller and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing or use, or
3. if the data are generally accessible or the controller would be allowed to publish them, unless the data subject has a clear and overriding legitimate interest in ruling out the possibility of processing or use.
When personal data are collected, the purposes for which the data are to be processed or used shall be specifically defined.
(2) The transfer or use for another purpose shall be lawful
1. under the conditions given in subsection 1 first sentence no. 2 or no. 3,
2. where necessary
a) to safeguard legitimate interests of a third party, or
b) to prevent threats to state or public security or to prosecute crimes
and there is no reason to believe that the data subject has a legitimate interest in ruling out the possibility of transfer or use, or
3. if necessary in the interest of a research institution for the purpose of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection, and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort.
(3) The processing or use of personal data for purposes of advertising or trading in
addresses shall be lawful if the data subject has given his or her consent and, if such
consent was not given in written form, the controller proceeds in accordance with
subsection 3a. In addition, processing or use of personal data shall be lawful where
the data consist of lists or other summaries of data from members of a category of

persons defined only in terms of the data subject's membership of this category, his

or her occupation, name, title, academic degree(s), address and year of birth, and
where processing or use is necessary
1. for purposes of advertising from the controller which collected the data, except for information on membership of the category, from the data subject under subsection 1 first sentence no. 1 or from publicly accessible sources such as telephone or business directories,
2. for purposes of advertising in view of the data subject's occupation and at his
or her work address, or
3. for purposes of soliciting donations eligible for tax concessions under Section
10b (1) and Section 34g of the Income Tax Act.
For purposes under the second sentence no. 1, the controller may record data in
addition to the data referred to there. Summarized personal data under the second
sentence may also be transferred for advertising purposes if the transfer is recorded
in accordance with Section 34 (1a) first sentence; in this case, the advertisement
must clearly identify the body which first collected the data. Regardless of whether
the conditions of the second sentence are met, personal data may be used for advertising third-party offers if the data subject can clearly identify from the advertisement the controller responsible for using the data. Processing or use as
referred to in the second through fourth sentences shall be lawful only where it does
not conflict with legitimate interests of the data subject. Data transferred under the
first, second and fourth sentences may be processed or used only for the purpose for
which they were transferred.
(3a) If consent under Section 4a (1) third sentence is given in a form other than writing, the controller shall provide the data subject with written confirmation of the
substance of the consent unless consent was given in electronic form and the

controller ensures that the declaration of consent is recorded and the data subject
can access and revoke it at any time with future effect. If consent is to be given together with other written declarations, it shall be made distinguishable in its printing
and format.
(3b) The controller may not make the conclusion of a contract dependent on the data
subject's consent under subsection 3 first sentence, if access to equivalent contractual benefits is impossible or unreasonable without providing consent. Consent provided under such circumstances shall be invalid.
(4) If the data subject lodges an objection with the controller regarding the processing
or use of his or her data for advertising purposes or market or opinion research,
processing or use for these purposes shall be unlawful. In approaching the data
subject for the purpose of advertising or market or opinion research, and in the cases
of subsection 1 first sentence no. 1 also when creating a legal or quasi-legal obligation, the data subject shall be informed of the identity of the controller and of
the right to object under the first sentence; where the party approaching the data
subject uses the data subject's personal data recorded by a body unknown to him or
her, the approaching party shall also ensure that the data subject may obtain information about the source of the data. If the data subject lodges an objection with
the third party to which the data were transferred in connection with purposes under
subsection 3 as to the processing or use for purposes of advertising or market or
opinion research, the third party shall block the data for these purposes. In the cases

of subsection 1 first sentence no. 1, the requirements as to the form of the

objection
may not be stricter than for the creation of a legal or quasi-legal obligation.
(5) The third party to which the data are transferred may process or use these data
only for the purpose for which they were transferred. Private bodies may process or
use the data for other purposes only subject to the conditions of subsections 2 and 3,
and public bodies may process or use the data for other purposes only subject to the
conditions of Section 14 (2). The transferring body shall point this out to the third
party.
(6) The collection, processing and use of special categories of personal data (Section
3 (9)) for own commercial purposes shall be lawful without the data subject's consent
in accordance with Section 4a (3) if
1. necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent,
2. data are involved which the data subject has manifestly made public,
3. necessary to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of collection, processing or use, or
4. necessary for the purposes of scientific research, where the scientific interest
in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection, processing and use and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort.
(7) The collection of special categories of personal data (Section 3 (9)) shall further
be lawful when required for the purposes of preventive medicine, medical diagnosis,
the provision of care or treatment or the management of health-care services, and
where these data are processed by health professionals subject to the

obligation of
professional secrecy or by other persons also subject to an equivalent obligation of
secrecy. The processing and use of data for the purposes referred to in the first
sentence shall be subject to the obligation of secrecy which applies to the persons
referred to in the first sentence. The collection, processing or use of data concerning
the health of persons for a purpose listed in the first sentence by members of a profession other than those listed in Section 203 (1) and (3) of the Criminal Code
which involves identifying, healing or relieving illnesses, or producing or selling aids
shall be lawful only subject to the same conditions authorizing a physician to do so.
(8) Special categories of personal data (Section 3 (9)) may be transferred or used for
other purposes only subject to the conditions of subsection 6 nos. 1 through 4 or of
subsection 7 first sentence. Transfer or use shall be lawful also if necessary to prevent threats to state and public security or to prosecute serious crimes.
(9) Non-profit-seeking organizations with a political, philosophical, religious or tradeunion
aim may collect, process or use special categories of personal data (Section 3 (9)) as needed for their activities. This shall apply only to the personal data of their
members or to persons who have regular contact with them in connection with their
purposes. Transferring these personal data to persons or bodies outside the organization shall be lawful only subject to the conditions of Section 4a (3). Subsection 2 no. 2 b shall apply accordingly.

33

Section 28a Data transfer to rating agencies

(1) Transferring personal data concerning a claim to rating agencies shall be lawful
only if the performance owed has not been rendered on time, the transfer is

necessary to safeguard the legitimate interests of the controller or a third party and
1. the claim has been established by a final decision or a decision declared enforceable for the time being, or if an executory title has been issued under Section 794 of the Code of Civil Procedures,
2. the claim has been established under Section 178 of the Insolvency Act and has not been disputed by the debtor at the verification meeting,
3. the data subject has expressly acknowledged the claim,
4. a) the data subject received at least two written reminders after the due date,
b) at least four weeks elapsed between the first reminder and the data transfer,
c) the controller gave the data subject sufficient notice before transferring the information, or at least informed the data subject of the impending transfer in the first reminder, and
d) the data subject did not dispute the claim, or
5. the contractual relationship on which the claim is based can be terminated without prior notice for payment in arrears and the controller has informed the data subject of the impending transfer.
The first sentence shall apply accordingly if the controller itself uses the data under
Section 29.
(2) For the future transfer under Section 29 (2), credit institutions may transfer to
rating agencies personal data about the creation, orderly execution and termination
of a contractual relationship concerning a bank transaction as referred to in Section 1
(1) second sentence, no. 2, 8, or 9 of the Banking Act unless the data subject's legitimate interest in ruling out the possibility of transfer manifestly overrides the
interest of the rating agency in knowledge of the data. The data subject shall be
informed of this before the contract is concluded. The first sentence shall not apply to
contracts concerning current accounts without overdraft protection. For the future
transfer under Section 29 (2), the transfer of data concerning the behaviour of

data
subjects which serve to create market transparency in the context of pre-contractual
relationships of trust shall be unlawful, even with the data subject's consent.
(3) Within one month of becoming aware of any subsequent alteration of facts based
on a transfer conducted in accordance with subsection 1 or 2, the controller shall
inform the rating agency of such alteration, as long as the rating agency still has the
data originally transferred. The rating agency shall inform the body which transferred
the data when it has erased the data originally transferred.[7]

[7] *In force from 1 April 2010.*

Section 28b Scoring

For the purpose of deciding on the creation, execution or termination of a contractual
relationship with the data subject, a probability value for certain future action by the
data subject may be calculated or used if
1. the data used to calculate the probability value are demonstrably essential for
calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure,
2. if the probability value is calculated by a rating agency, the conditions for transferring the data used under Section 29, and in all other cases the conditions of lawful use of data under Section 28 are met,
3. the probability value is not calculated solely on the basis of address data,
4. if address data are used, the data subject shall be notified in advance of the planned use of these data; this notification shall be documented.[8]

Section 29 Commercial data collection and recording for the purpose of transfer

(1) Commercial collection, recording or alteration of personal data for the purpose of
transfer, in particular for the purpose of advertising, the activities of rating agencies or

trade in addresses, shall be lawful if
1. there is no reason to believe that the data subject has a legitimate interest in ruling out the possibility of collection, recording or alteration, or
2. the data can be acquired from generally accessible sources or the controller would be allowed to publish them, unless the data subject has a clear and overriding legitimate interest in ruling out the possibility of collection, recording or alteration.
Section 28 (1) first sentence and subsections 3 through 3b shall apply.
(1) The commercial collection, recording, alteration or use of personal data for the
purpose of transfer, in particular for the purpose of advertising, the activities of rating
agencies or trade in addresses, shall be lawful if
1. there is no reason to believe that the data subject has a legitimate interest in ruling out the possibility of collection, recording or alteration,
2. the data can be acquired from generally accessible sources or the controller would be allowed to publish them, unless the data subject has a clear and overriding legitimate interest in ruling out the possibility of collection, recording or alteration, or
3. the conditions of Section 28a (1) or (2) are met; data as defined in Section 28a (2) fourth sentence may not be collected or recorded.
Section 28 (1) second sentence and subsections 3 through 3b shall apply.[9]
(2) Transfer for the purposes specified in subsection 1 shall be lawful if

[8] In force from 1 April 2010.

[9] In force from 1 April 2010.

1. the third party to which the data are transferred has presented credible evidence of legitimate interest in knowledge of the data, and
2. there is no reason to believe that the data subject has a legitimate interest in ruling out the possibility of transfer.
Section 28 (3) through (3b) shall apply accordingly. In the case of transfer in accordance with no. 1, the evidence of legitimate interest and the means of presenting this evidence in a credible way shall be documented by the transferring
body. In the case of transfer using automated retrieval, the third party to which the
data are transferred shall be responsible for documentation.

(2) Transfer for the purposes specified in subsection 1 shall be lawful if
1. the third party to which the data are transferred has presented credible evidence of legitimate interest in knowledge of the data, and
2. there is no reason to believe that the data subject has a legitimate interest in ruling out the possibility of transfer.
Section 28 (3) through (3b) shall apply accordingly. In the case of transfer in accordance with the first sentence no. 1, the evidence of legitimate interest and the
means of presenting this evidence in a credible way shall be documented by the
transferring body. In the case of transfer using automated retrieval, the third party to
which the data are transferred shall be responsible for documentation. The transferring body shall take random samples in accordance with Section 10 (4) third
sentence and in doing so also determine whether a legitimate interest exists in the
particular case.[10]
(3) Personal data shall not be included in electronic or printed address, telephone,
business or similar directories if it is clear from the electronic or printed directory that
such inclusion is contrary to the data subject's will. The recipient of the data shall
ensure that identifiers from electronic or printed directories or registers are retained
upon their inclusion in directories or registers.
(4) Section 28 (4) and (5) shall apply to the processing or use of the transferred data.
(5) Section 28 (6) through (9) shall apply accordingly.
(6) Any body which for the purpose of transfer commercially collects, records or
alters personal data which may be used to evaluate the creditworthiness of consumers shall treat requests for information from lenders in other European Union
Member States or other states party to the Agreement on the European Economic
Area the same way it treats information requests from domestic lenders.[11]

(7) Anyone who refuses to conclude a consumer loan contract or a contract concerning financial assistance for payment with a consumer as the result of information provided by a body as referred to in subsection 6 shall immediately notify
the consumer of this refusal and the information received. Such notification shall not
be made if it would endanger public security or order. Section 6a shall remain unaffected.[12]

[10] In force from 1 April 2010.

[11] In force from 11 June 2010.

[12] In force from 11 June 2010.

Section 30 Commercial data collection and recording for the purpose of transfer in anonymous form

(1) If personal data are commercially collected and recorded for the purpose of transfer in anonymous form, those features enabling personal or material circumstances to be attributed to an identified or identifiable natural person shall be
recorded separately. These features may be combined with the information only
where necessary for the purpose for which the data are recorded or for scientific
purposes.

(2) The alteration of personal data shall be lawful if

1. there is no reason to believe that the data subject has a legitimate interest in ruling out the possibility of alteration, or
2. the data can be acquired from generally accessible sources or the controller would be allowed to publish them, unless the data subject has a clear and overriding legitimate interest in ruling out the possibility of alteration.

(3) The personal data shall be erased if they were unlawfully recorded.

(4) Section 29 shall not apply.

(5) Section 28 (6) through (9) shall apply accordingly.

Section 30a Commercial data collection and recording for purposes of market
or opinion research

(1) The commercial collection, processing or use of personal data for purposes of

market or opinion research shall be lawful if
1. there is no reason to believe that the data subject has a legitimate interest in ruling out the possibility of collection, processing or use, or
2. the data can be acquired from generally accessible sources or the controller would be allowed to publish them, and the data subject's legitimate interest in ruling out the possibility of collection, processing or use does not clearly override the interest of the controller.
Special categories of personal data (Section 3 (9)) may be collected, processed or
used only for a specific research project.
(2) Personal data collected or recorded for purposes of market or opinion research
may be processed or used only for these purposes. Data which were not acquired
from generally accessible sources and which the controller may not publish may be
processed or used only for the research project for which they were collected. They
may be processed or used for a different purpose only if they have been rendered
anonymous in such a way that the identification of the data subject is no longer possible.
(3) Personal data shall be rendered anonymous as soon as allowed by the purpose
of the research project for which they were collected. Until then, the features enabling
information concerning personal or material circumstances attributable to an identified or identifiable person shall be kept separately. These features may be
combined with the information only where necessary for the purpose of the research
project.
(4) Section 29 shall not apply.

(5) Section 28 (4) and (6) through (9) shall apply accordingly.

Section 31 Special restrictions on use

Personal data recorded exclusively for purposes of monitoring data protection,

safeguarding data or ensuring proper operation of a data processing system may
only be used for these purposes.

Section 32 Data collection, processing and use for employment-related purposes

(1) An employee’s personal data may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring,
for carrying out or terminating the employment contract. Employees’ personal data
may be collected, processed or used to investigate crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the collection, processing or use of such data is necessary to investigate
the crime, and the employee does not have an overriding legitimate interest in ruling
out the possibility of collection, processing or use, and in particular the type and
extent are not disproportionate to the reason.

(2) Subsection 1 shall also apply when personal data are collected, processed or
used without the help of automated processing systems, or are processed or used in
or from a non-automated filing system or collected in such a filing system for processing or use.

(3) The rights of participation of employee staff councils shall remain unaffected.

Chapter 2

Rights of the data subject

Section 33 Notification of the data subject

(1) If personal data are recorded for own purposes for the first time without the data
subject’s knowledge, the data subject shall be notified of such recording, the type of
data, the purpose of collection, processing or use and the identity of the controller. If
personal data are commercially recorded for the purpose of transfer without

the data
subject’s knowledge, the data subject shall be notified of their initial transfer and of
the type of data transferred. In the cases covered by the first and second sentences
above, the data subject shall also be notified of the categories of recipients, where,
given the circumstances of the individual case, the data subject need not expect that
his/her data will be transferred to such recipients.
(2) Notification shall not be required if
1. the data subject has become aware of the recording or transfer by other means,
2. the data were recorded only because they may not be erased due to legal, statutory or contractual provisions on retention, or only for purposes of monitoring data protection or safeguarding data, and providing information would require a disproportionate effort,
3. the data must be kept secret by law or due to the nature of the data, namely due to the overriding legal interests of a third party,

4. recording or transfer is expressly laid down by law,
5. recording or transfer is necessary for the purposes of scientific research and notification would require a disproportionate effort,
6. the responsible public body has informed the controller that disclosure of the data would threaten the public security or order or otherwise be detrimental to the Federation or a *Land*, or
7. the data were recorded for own purposes and
a) were acquired from generally accessible sources and notification would require a disproportionate effort due to the large number of cases concerned, or
b) notification would seriously endanger the commercial purposes of the controller, unless the interest in notification overrides this danger,
8. The data were commercially recorded for the purpose of transfer, and
a) were acquired from generally accessible sources, where they related to the persons who published the data, or
b) the data are compiled in lists or otherwise summarized (Section 29 (2) second sentence)

and notification would require a disproportionate effort due to the large number of cases concerned,
9. data acquired from generally accessible sources recorded commercially for the purpose of market or opinion research and notification would require a disproportionate effort due to the large number of cases concerned.
The controller shall stipulate in writing the conditions under which notification shall
not be provided in accordance with the first sentence, nos. 2 through 7.

Section 34 Access to data

(1) Data subjects may request information about
1. recorded data relating to them, including information relating to the source of the data,
2. the recipients or categories of recipients to which the data are transferred, and
3. the purpose of recording the data.
Data subjects should specify the type of personal data on which information is to be
given. If the personal data are commercially recorded for the purpose of transfer,
data subjects may request information about the source and recipients only if there is
no overriding interest in protecting trade secrets. In this case, data subjects shall be
given information about the source and recipients even if this information was not
recorded.
(2) Data subjects may request information about their personal data from bodies
which commercially record personal data for the purpose of providing information
even when the data are not recorded in an automated processing system or a nonautomated
filing system. Data subjects may request information about the source
and recipients only if there is no overriding interest in protecting trade secrets.

(3) Information shall be provided in writing unless special circumstances warrant any

other form.
(4) There shall be no obligation to provide information if Section 33 (2) first sentence
nos. 2, 3 and 5 through 7 do not require notifying the data subject.
(5) Information shall be provided free of charge. However, if personal data are commercially recorded for the purpose of transfer, a fee may be charged if the data
subject can use the information vis-à-vis third parties for commercial purposes. The
fee shall not exceed the costs resulting directly from the provision of information. No
fee may be charged in cases where special circumstances give reason to believe
that the data are incorrectly or unlawfully recorded, or where the information provided
indicates that the data shall be rectified or erased subject to Section 35 (2) second
sentence no. 1.
(6) Where a fee is charged for providing information, data subjects shall have the
option of personal access to the data and information concerning them within the
framework of their right of access. Data subjects shall be informed of this option in an
appropriate form.

Section 34 Access to data

(1) The controller shall provide information to data subjects at their request concerning
1. recorded data relating to them, including information relating to the source of the data,
2. the recipients or categories of recipients to which the data are transferred, and
3. the purpose of recording the data.
Data subjects should specify the type of personal data about which information is to
be given. If the personal data are commercially recorded for the purpose of transfer,
information shall be provided about the source and recipients even if this

information
is not recorded. Information about the source and recipients may be withheld if the
interest in protecting trade secrets overrides the data subject's interest in the information.
(1a) In the case of Section 28 (3) fourth sentence, the transferring body shall record
the source of the data and the recipient for two years following transfer and shall
provide the data subject with information about the source of the data and the recipient upon request. The first sentence shall apply to the recipient accordingly.
(2) In the case of Section 28b, the body responsible for the decision shall provide
information to data subjects at their request concerning
1. probability values calculated or recorded for the first time within the six months preceding the receipt of the information request,
2. the types of data used to calculate the probability values, and
3. how probability values are calculated and their significance, with reference to
the individual case and in generally understandable terms.
The first sentence shall apply accordingly if the body responsible for the decision

1. records the data used to calculate the probability values without reference to specific persons but creates such a reference when calculating the probability value, or
2. uses data recorded by another body.
If a body other than the body responsible for the decision calculates
1. the probability value or
2. a component of the probability value,
it shall provide the body responsible for the decision with the information necessary
to answer the request as referred to in the first and second sentences upon request.
In the case of the third sentence no. 1, in responding to a request for information, the

body responsible for the decision shall, without delay, provide the data subject with
the name and address of the other body as well as the information necessary to
reference the individual case, unless the body responsible for the decision provides
the requested information itself. In this case, the other body which calculated the
probability value shall provide the data subject with the desired information as referred to in the first and second sentences free of charge. The body responsible for
calculating the probability value shall not be subject to the obligation referred to in the
third sentence if the body responsible for the decision uses its right referred to in the
fourth sentence.
(3) A body which commercially records personal data for the purpose of transfer shall
provide data subjects with information about data relating to them, even if these data
are neither processed in automated form nor recorded in non-automated filing systems. Data subjects shall also be given information about data
1. which currently demonstrate no reference to specific persons although the controller is to create such a reference in connection with providing information,
2. which the controller does not record but uses for the purpose of providing information.
Information about the source and recipients may be withheld if the interest in protecting trade secrets overrides the data subject's interest in the information.
(4) A body which commercially collects, records or alters personal data for the purpose of transfer shall, upon request, provide data subjects with information about
1. probability values for certain future action by the data subject which were transferred within the twelve months preceding the receipt of the information request, as well as the names and last-known addresses of third parties to which the values were transferred,
2. the probability values at the time of the information request calculated according to the method used by the calculating body,

3. the types of data used to calculate the probability values referred to in nos. 1 and 2, and
4. how probability values are calculated and their significance, with reference to
the individual case and in generally understandable terms.
The first sentence shall apply accordingly if the controller

41
1. records the data used to calculate the probability value without reference to specific persons but creates such a reference when calculating the probability value, or
2. uses data recorded by another body.
(5) Data recorded for the purpose of providing information to data subjects in accordance with subsections 1a through 4 may be used only for this purpose and for
the purpose of monitoring data protection; they shall be blocked for other purposes.
(6) Information shall be provided in writing upon request unless special circumstances make another form appropriate.
(7) There shall be no obligation to provide information if Section 33 (2) first sentence
nos. 2, 3 and 5 through 7 do not require notifying the data subject.
(8) Information shall be provided free of charge. If the personal data are commercially
recorded for the purpose of transfer, the data subject may request information in
writing free of charge once per calendar year. A fee may be charged for each additional request if the data subject can use the information vis-à-vis third parties for
commercial purposes. The fee shall not exceed the costs resulting directly from the
provision of information. No fee may be charged if
1. special circumstances give reason to believe that the data are incorrectly or unlawfully recorded, or
2. the information provided indicates that the data shall be rectified in accordance with Section 35 (1) or erased in accordance with Section 35 (2) second sentence no. 1.
(9) Where a fee is charged for providing information, data subjects shall have

the
option of personal access to the data concerning them within the framework of their
right of access. Data subjects shall be informed of this option.[13]

Section 35 Correction, deletion and blocking of data

(1) Personal data shall be rectified when they are inaccurate.
Estimated data shall be clearly identified as such.[14]
(2) Personal data may be erased at any time, except in the cases referred to in subsection 3 nos. 1 and 2. Personal data shall be erased if
1. unlawfully recorded, or
2. they concern racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, punishable actions or administrative offences, and the controller is unable to prove their accuracy,
3. they are processed for own purposes, as soon as knowledge of them is no longer needed to carry out the purpose for which they were recorded, or

[13] In force from 1 April 2010.

[14] In force from 1 April 2010.

4. they are commercially processed for the purpose of transfer and an examination at the end of the fourth calendar year from their initial recording shows that further retention is unnecessary.
(2) Personal data may be erased at any time, except in the cases referred to in subsection 3 nos. 1 and 2. Personal data shall be erased if
1. unlawfully recorded, or
2. the data concern racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, punishable actions or administrative offences, and the controller is unable to prove their accuracy,
3. they are processed for own purposes, as soon as knowledge of them is no longer needed to carry out the purpose for which they were recorded, or
4. they are processed commercially for the purpose of transfer and an examination at the end of the fourth calendar year following their initial recording, or at the end of the third calendar year in the case of data concerning matters that have been concluded, shows that further retention is unnecessary.
Personal data recorded on the basis of Section 28a (2) first sentence or

Section 29

(1) first sentence no. 3 shall be erased after the termination of the contract, if the data

subject so requests.[15]

(3) Instead of being erased, data shall be blocked where

1. in the case of subsection 2 no. 3, erasure would violate retention periods set by law, statute or contract,

2. there is reason to believe that erasure would be detrimental to legitimate interests of the data subject, or

3. erasure would be impossible or would involve a disproportionate effort due to

the special category of recording.

(3) Instead of being erased, data shall be blocked where

1. in the case of subsection 2 second sentence no. 3, erasure would violate retention periods set by law, statute or contract,

2. there is reason to believe that erasure would be detrimental to legitimate interests of the data subject, or

3. erasure would be impossible or would involve a disproportionate effort due to

the special category of recording.[16]

(4) Further, personal data shall be blocked if the data subject disputes their accuracy

and their accuracy or inaccuracy cannot be verified.

(4a) The fact that the data are blocked shall not be disclosed.[17]

15 In force from 1 April 2010.

16 In force from 1 April 2010.

17 In force from 1 April 2010.

(5) Personal data may not be collected, processed or used for processing in automated form or in non-automated filing systems if the data subject lodges an

objection with the controller and examination indicates that legitimate interests of the

data subject due to his or her particular personal situation override the interest of the

controller in such collection, processing or use. The first sentence shall not apply if

collection, processing or use is required by law.
(6) Where they are commercially recorded for the purpose of transfer, except in
the cases referred to in subsection 2 no. 2, personal data which are incorrect or
whose accuracy is disputed need not be rectified, blocked or erased if they were
acquired from generally accessible sources and recorded for documentation
purposes. At the data subject's request, his or her counter-statement shall be kept
with these data for the duration of their retention. The data may not be transferred
without this counter-statement.
(7) The bodies to which these data are transferred for recording shall be informed
of the rectification of inaccurate data, the blocking of disputed data and erasure or
blocking due to unlawful recording, if this does not involve a disproportionate effort
and does not conflict with legitimate interests of the data subject.
(7) The bodies to which these data were transferred for recording shall be informed
of the rectification of inaccurate data, the blocking of disputed data and erasure or
blocking due to unlawful recording, if this does not involve a disproportionate effort
and does not conflict with legitimate interests of the data subject.[18]
(8) Blocked data may be transferred or used without the data subject's consent only if
1. it is vital for scientific purposes, to supply necessary evidence, or for other reasons in the overriding interest of the controller or a third party, and
2. the transfer or use of the data for this purpose would be allowed if the data were not blocked.

Chapter 3

Supervisory authority
Section 36 (deleted)
Section 37 (deleted)

Section 38 Supervisory authority

(1) The supervisory authority shall monitor the implementation of this Act and other data protection provisions governing the automated processing of personal data or the processing or use of personal data in or from non-automated filing systems, including the rights of the Member States in the cases of Section 1 (5). It shall advise and support the data protection officials and controllers with due regard to their typical requirements. The supervisory authority may process and use data it has recorded for supervisory purposes only; Section 14 (2) nos. 1 through 3, 6 and 7 shall apply accordingly. In particular, the supervisory authority may transfer data to

[18] In force from 1 April 2010.

other supervisory authorities for supervisory purposes. On request, it shall provide supplementary assistance (administrative assistance) to the supervisory authorities of other Member States of the European Union. If the supervisory authority finds that this Act or other data protection provisions have been violated, it shall be authorized to notify the data subjects, to report the violation to the bodies responsible for prosecution or punishment, and, in case of serious violations, to notify the trade supervisory authority in order to initiate measures under trade law. It shall publish an activity report regularly and at least every two years. Section 21 first sentence and Section 23 (5) fourth through seventh sentences shall apply accordingly.

(2) The supervisory authority shall keep a register of the automated processing operations subject to the obligation to notify under Section 4d, to include the information specified in Section 4e first sentence. The register may be

inspected by
any person. The right to inspection shall not extend to the information referred to in
Section 4e first sentence no. 9, nor to the identity of the persons entitled to access.
(3) The bodies subject to monitoring and the persons responsible for their management shall provide the supervisory authority, on request and without delay,
the information necessary to perform its duties. The person required to provide information may refuse to answer those questions which would expose him-/herself
or a relative as referred to in Section 383 (1) nos. 1 through 3 of the Code of Civil
Procedure to the risk of criminal prosecution or proceedings under the Administrative
Offences Act. The person required to provide information shall be informed accordingly.
(4) Persons appointed by the supervisory authority to conduct monitoring shall be
authorized, where necessary for them to perform the duties assigned by the supervisory authority, to enter the property and premises of the body during business
hours and to carry out checks and inspections there. They may inspect business
documents, especially the list referred to in Section 4g (2) first sentence and the
recorded personal data and data processing programs. Section 24 (6) shall apply
accordingly. The person required to provide information shall allow these measures.
(5) To ensure compliance with this Act and other data protection provisions, the
supervisory authority may order measures to remedy violations identified in the collection, processing or use of personal data, or technical or organizational problems. In case of serious violations or problems, especially those related to a
special threat to privacy, the supervisory authority may prohibit collection, processing

or use, or the use of particular procedures if the violations or problems are not remedied within a reasonable time despite orders as referred to in the first sentence
and despite the imposition of a fine. The supervisory authority may demand the
dismissal of a data protection official if he or she does not have the necessary specialized knowledge and reliability to perform his or her duties.
(6) The *Land* governments or the bodies authorized by them shall designate the
supervisory authorities responsible for monitoring the implementation of data protection within the scope of this part.
(7) The application of the Industrial Code to commercial enterprises subject to the
provisions of this Part shall remain unaffected.

**Section 38a Codes of conduct to facilitate the application of data protection
provisions**

(1) Trade associations and other bodies representing specific categories of controllers may submit to the responsible supervisory authority draft codes of conduct to facilitate the application of data protection provisions.
(2) The supervisory authority shall examine the drafts submitted for compliance with
applicable data protection law.

Part IV

Special provisions

**Section 39 Restrictions on use of personal data subject to professional or
special official secrecy**

(1) Personal data subject to professional or special official secrecy and provided by
the body obligated to secrecy in the performance of its professional or official duties
may be processed or used by the controller only for the purpose for which they were
received. The body obligated to secrecy must give its consent to any transfer

to a
private body.
(2) The data may be processed or used for another purpose only if the change of
purpose is permitted by special legislation.

Section 40 Processing and use of personal data by research institutions

(1) Personal data collected or recorded for purposes of scientific research may be
processed or used only for purposes of scientific research.
(2) Personal data shall be rendered anonymous as soon as the research purpose
allows. Until then, the features enabling the attribution of information concerning
personal or material circumstances to an identified or identifiable person shall be kept
separately. They may be combined with the information only to the extent required by
the research purpose.
(3) Bodies conducting scientific research may publish personal data only if
1. the data subject has consented,
2. this is essential to present research findings concerning events of contemporary history.

Section 41 Collection, processing and use of personal data by the media

(1) In their legislation, the *Länder* shall ensure that regulations corresponding to the
provisions of Sections 5, 9 and 38a, including rules on liability in accordance with
Section 7, apply to the collection, processing and use of personal data by media
enterprises and auxiliary media enterprises exclusively for their own journalistic,
editorial or literary purposes.
(2) If the journalistic-editorial collection, processing or use of personal data by

Deutsche Welle leads to the publication of counter-statements by the data subject, these counter-statements shall be added to the recorded data and retained for the same length of time as the data themselves.

(3) If reporting by *Deutsche Welle* infringes the privacy of an individual, this person may request information about the recorded data relating to him/her on which the reporting was based. This information may be refused after considering the legitimate interests of the parties concerned, where
1. the data allow the identification of persons who are or were professionally involved as journalists in preparing, producing or disseminating broadcasts,
2. the data allow the identification of the supplier or source of contributions, documents and communications for the editorial part,
3. disclosure of the data obtained by research or other means would compromise *Deutsche Welle*'s journalistic duty by divulging its information resources.
The data subject may request that inaccurate data be corrected.
(4) In all other respects, Sections 5, 7, 9 and 38a shall apply to *Deutsche Welle*. Section 42 shall apply in place of Sections 24 through 26, even where administrative matters are concerned.

Section 42 Data protection official of *Deutsche Welle*

(1) *Deutsche Welle* shall appoint a data protection official who shall take the place of the Federal Commissioner for Data Protection and Information Freedom. The data protection official shall be nominated by the director-general and appointed by the administrative board for a term of four years; the appointment may be renewed. The office of data protection official may be held in combination with other duties within the broadcaster.
(2) The data protection official shall monitor compliance with this Act and other data protection provisions. He or she shall be independent in performing the duties of this office and subject only to the law. In all other respects, he or she shall be subject to the administrative and legal supervision of the administrative board.
(3) Anyone may appeal to the data protection official in accordance with Section 21 first sentence.
(4) The data protection official of *Deutsche Welle* shall submit an activity report to the organs of *Deutsche Welle* every two years, starting on 1 January 1994. In addition, the data protection official shall submit special reports at the decision of an organ of *Deutsche Welle*. The data protection official shall provide a copy of his or her activity reports to the Federal Commissioner for Data Protection and Freedom of Information as well.
(5) *Deutsche Welle* shall make further arrangements for its area of activity in accordance with Sections 23 through 26 of the Act. Sections 4f and 4g shall remain

unaffected.

Section 42a Obligation to notify in case of unlawful access to data

If a private body as defined in Section 2 (4) or a public body as referred to in Section 27 (1) first sentence no. 2 determines that

1. special categories of personal data (Section 3 (9)),
2. personal data subject to professional secrecy,

3. personal data referring to criminal or administrative offences or to suspected criminal or administrative offences, or
4. personal data concerning bank or credit card accounts

it has recorded have been unlawfully transferred or otherwise unlawfully disclosed to third parties, threatening serious harm to the rights or legitimate interests of data subjects, then the private body shall notify the competent supervisory and the data subjects without delay in accordance with the second through fifth sentences. Data subjects shall be informed as soon as appropriate measures to safeguard the data have been taken and notification would no longer endanger criminal prosecution. The notification of data subjects shall describe the nature of the unlawful disclosure and recommend measures to minimize possible harm. The notification of the competent supervisory authority shall in addition describe possible harmful consequences of the unlawful disclosure and measures taken by the body as a result. Where notifying the data subjects would require a disproportionate effort, in particular due to the large number of persons affected, such notification may be replaced by public advertisements of at least one-half page in at least two national daily newspapers, or by another equally effective measure for notifying data subjects. Notification distributed by the body required to provide notification may be used against that body in criminal proceedings or proceedings under the Administrative Offences Act, or against an associate of the body required to provide notification as defined in Section 52 (1) of the Code of Criminal Procedure only with the consent of the body required to provide notification.

Part V

Final provisions

Section 43 Administrative offences

(1) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence

1. in violation of Section 4d (1), also in conjunction with Section 4e second sentence, fails to notify, fails to do so within the prescribed time limit or fails to provide complete information,

2. in violation of Section 4f (1) first or second sentence, in each case also in conjunction with the third and sixth sentences, fails to appoint a data protection official or fails to do so within the prescribed time limit or in the prescribed manner,
2 a. in violation of Section 10 (4) third sentence fails to ensure that the transfer of data can be ascertained and checked,
2 b. in violation of Section 11 (2) second sentence fails to assign work correctly, completely or in accordance with the rules, or in violation of Section 11 (2) fourth sentence fails to verify compliance with the technical and organizational measures taken by the processor before data processing begins,
3. in violation of Section 28 (4) second sentence fails to notify the data subject, or fails to do so correctly or within the prescribed time limit, or fails to ensure that the data subject may obtain the relevant information,

3 a. in violation of Section 28 (4) fourth sentence requires a stricter form,
4. in violation of Section 28 (5) second sentence transfers or uses personal data,
4 a. in violation of Section 28a (3) first sentence fails to notify, or fails to do so correctly, completely or within the prescribed time limit,19
5. in violation of Section 29 (2) third or fourth sentence fails to record the evidence described there or the means of presenting it in a credible way,
6. in violation of Section 29 (3) first sentence, incorporates personal data into electronic or printed address, telephone, business or similar directories,
7. in violation of Section 29 (3) second sentence fails to ensure the inclusion of identifiers,
7 a. in violation of Section 29 (6) fails to treat a request for information properly,20
7 b. in violation of Section 29 (7) first sentence fails to notify a consumer, or fails to do so correctly, completely or within the prescribed time limit,21
8. in violation of Section 33 (1) fails to notify the data subject, or fails to do so correctly or completely,
8 a. in violation of Section 34 (1) first sentence, also in conjunction with the third sentence, in violation of Section 34 (1a), in violation of Section 34 (2) first sentence, also in conjunction with the second sentence, or in violation of Section 34 (2) fifth sentence, (3) first sentence or second sentence or (4) first sentence, also in conjunction with the second sentence, fails to

provide information, or fails to do so correctly, completely or within the prescribed time limit, or in violation of Section 34 (1a) fails to record data,22
8 b. in violation of Section 34 (2) third sentence fails to provide information, or fails to do so correctly, completely or within the prescribed time limit,23
8 c. in violation of Section 34 (2) fourth sentence fails to provide the data subject with the information referred to, or fails to do so within the prescribed time limit,24
9. in violation of Section 35 (6) third sentence transfers data without providing the counter-statement,
10. in violation of Section 38 (3) first sentence or (4) first sentence fails to provide information, or fails to do so correctly, completely or within the prescribed time limit, or fails to allow a measure, or
19 In force from 1 April 2010.
20 In force from 11 June 2010.
21 In force from 11 June 2010.
22 In force from 1 April 2010.
23 In force from 1 April 2010.
24 In force from 1 April 2010.

11. fails to comply with an executable instruction under Section 38 (5) first sentence.
(2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence
1. collects or processes personal data which are not generally accessible without authorization,
2. makes available personal data which are not generally accessible by means of automated retrieval without authorization,
3. retrieves personal data which are not generally accessible without authorization, or obtains such data for themselves or others from automated processing operations or non-automated files without authorization,
4. obtains transfer of personal data which are not generally accessible by providing false information,
5. in violation of Section 16 (4) first sentence, Section 28 (5) first sentence, also in conjunction with Section 29 (4), Section 39 (1) first sentence or Section 40 (1), uses transferred data for other purposes,
5 a. in violation of Section 28 (3b) makes the conclusion of a contract

dependent on the consent of the data subject,
5 b. in violation of Section 28 (4) first sentence processes or uses data for purposes of advertising or market or opinion research,
6. in violation of Section 30 (1) second sentence, Section 30a (3) third sentence or Section 40 (2) third sentence combines a feature referred to there with specific information, or
7. in violation of Section 42a first sentence, fails to notify or fails to do so correctly, completely or within the prescribed time limit.
(3) Administrative offences may be punished by a fine of up to € 50,000 in the case of subsection 1, and a fine of up to € 300,000 in the cases of subsection 2. The fine should exceed the financial benefit to the perpetrator derived from the administrative offence. If the amounts mentioned in the first sentence are not sufficient to do so, they may be increased.

Section 44 Criminal offences

(1) Anyone who wilfully commits an offence described in Section 43 (2) in exchange for payment or with the intention of enriching him-/herself or another person, or of harming another person shall be liable to imprisonment for up to two years or to a fine.
(2) Such offences shall be prosecuted only if a complaint is filed. Complaints may be filed by the data subject, the controller, the Federal Commissioner for Data Protection and Freedom of Information and the supervisory authority.

Part VI

Federal Data Protection Act (BDSG) As at 1 September 2009 with amendments 2010 50

Transitional provisions

Section 45 Current applications

The collection, processing or use of personal data already under way on 23 May 2001 shall be brought into compliance with the provisions of this Act within three years of that date. Where provisions of this Act are applied in legal provisions outside the scope of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the collection, processing or use of personal data already under way on 23 May 2001 shall be brought into compliance with the provisions of this Act within five years of that date.

Section 46 Continued validity of definitions

(1) Where used in special federal law, the term “filing system” shall mean
1. a collection of personal data which can be evaluated with reference to specific features using automated procedures (automated filing system), or

2. any other collection of personal data which is similarly structured and which can be arranged, re-arranged and evaluated according to specific characteristics (non-automated filing system).
This shall not include files and sets of files unless they can be rearranged and evaluated using automated procedures.
(2) Where used in special federal law, the term “file” shall mean any document serving official purposes to which the definition of a filing system under subsection 1 does not apply; this shall include image and sound recording media. It shall not include preliminary drafts and notes that are not intended to be part of an operation.
(3) Where used in special federal law, the term “recipient” shall mean any person or body other than the controller. Recipients shall not mean the data subject or persons or bodies collecting, processing or using personal data in Germany, in another European Union Member State or another state party to the Agreement on the European Economic Area on behalf of another.

Section 47 Transitional provision

For the processing and use of data collected or recorded prior to 1 September 2009, Section 28 in the version in force until that date shall continue to apply
1. to purposes of market or opinion research until 31 August 2010,
2. to advertising purposes until 31 August 2012.

Section 28 in the version previously in force

Section 28 Storage, communication and use of data for own purposes

(1) The collection, storage, modification or transfer of personal data or their use as a means of
fulfilling one’s own business purposes shall be admissible
1. in accordance with the purposes of a contract or a quasi-contractual fiduciary relationship
with the data subject,

2. in so far as this is necessary to safeguard justified interests of the controller of the filing
system and there is no reason to assume that the data subject has an overriding legitimate
interest in his data being excluded from processing or use,
3. if the data is generally accessible or the controller of the filing system would be entitled to
publish them, unless the data subject's legitimate interest in his data being excluded from

processing or use clearly outweighs the justified interest of the controller of the filing system.
In connection with the collection of personal data, the purposes for which the data are to be processed
or used are to be stipulated in concrete terms.
(2) Transfer or use for another purpose shall be admissible only if the requirements of Section 1,
sentence 1, Nos. 2 and 3 are met.
(3) Transfer or use for another purpose shall also be admissible:
1. in so far as it is necessary to protect the justified interests of a third party or
2. to avert threats to the state security and public safety and to prosecute criminal offences or
3. for purposes of advertising, market and opinion research if the data, compiled in lists or
otherwise combined, concern members of a group of persons and are restricted to
a) the data subject's membership of this group of persons,
b) occupation or type of business,
c) name,
d) title,
e) academic degrees,
f) address and
g) year of birth
and if there is no reason to assume that the data subject has a legitimate interest in his data
being excluded from transfer, or
4. if this is necessary in the interest of a research institute for the conduct of scientific research,
if scientific interest in conduct of the research project substantially outweighs the interest of
the data subject in excluding the change of purpose and if the research purpose cannot be
attained by other means or can be attained thus only with disproportionate effort.
In the cases referred to in the first sentence of No. 3, it is to be assumed that such interest exists
where data are to be transferred which were stored for the purposes of a contract or a quasicontractual
fiduciary relationship and which concern
1. criminal offences,

2. administrative offences and,
3. when transferred by the employer, to the legal status under labour law.
(4) If the data subject objects vis-à-vis the controller of the filing system to the use or transfer of his
data for purposes of advertising or of market opinion research, use or transfer for such purposes shall
be inadmissible. In approaching the data subject for the purpose of advertising or market or opinion
research, the data subject shall be informed of the identity of the controller and the right of objections
in accordance with sentence 1 above; in so far as the party approaching the data subject uses
personal data of the latter which are stored by a body which is unknown to him, he shall also ensure
that the data subject is able to obtain information on the origin of the data. If the data subject lodges
an objection to the processing or use of the data for the purpose of advertising or market or opinion
research with the third party to whom the data are transferred pursuant to sub-section 3, the latter
shall block the data for these purposes.
(5) The third party to whom the data have been transferred may process or use the transferred data
only for the purpose for which they were transferred to him. Processing or use for other purposes shall
be admissible for private bodies only if the requirements of sub-sections 1 and 2 above are met and
for public bodies only if the requirements of Section 14 (2) are met. The transferring body shall point
this out to the third party.
Federal Data Protection Act (BDSG) As at 1 September 2009 with amendments 2010
52
(6) The collection, processing and use of special types of personal data (Section 3 (9)) for own
business purposes shall be admissible when the data subject has not consented in accordance with
Section 4a (3) if
1. this is necessary in order to protect vital interests of the data subject or of a third

party, in so
far as the data subject is unable to give his consent for physical or legal reasons,
2. the data concerned has evidently been made public by the data subject,
3. this is necessary in order to assert, exercise or defend legal claims and there is no reason to
assume that the data subject has an overriding legitimate interest in excluding such collection, processing or use, or
4. this is necessary for the purposes of scientific research, where the scientific interest in
carrying out the research project substantially outweighs the data subject's interest in excluding collection, processing and use and the purpose of the research cannot be achieved in any other way or would otherwise necessitate disproportionate effort.
(7) The collection of special types of personal data (Section 3 (9)) shall further be admissible if this is
necessary for the purposes of preventive medicine, medical diagnosis, health care or treatment or the
administration of health services and the processing of these data is carried out by medical personnel
or other persons who are subject to an obligation to maintain secrecy. The processing and use of data
for the purposes stated in sentence 1 shall be subject to the obligations to maintain secrecy which
apply to the persons stated in sentence 1. The collection, processing or use of data on the health of
persons by members of a profession other than those stipulated in Section 203 (1) and (3) of the
Penal Code, the exercising of which profession involves determining, curing or alleviating illnesses or
producing or selling aids shall be admissible only under those conditions according to which a doctor
would also be authorised for these purposes.
(8) Special types of personal data (Section 3 (9)) may be transferred or used only if the requirements
of sub-section 6, Nos. 1 to 4 or the first sentence of sub-section 7 are met. Transfer or use shall also
be admissible if necessary to avert substantial threats to state security or public safety and to
prosecute major criminal offences.

(9) Organisations of a political, philosophical or religious nature and trade union organisations may
collect, process or use special types of personal data (Section 3 (9)) in so far as this is necessary for
the organisation's activities. This shall apply only to personal data of their members or of persons who
maintain regular contact with the organisations in connection with the purposes of their activities. The
transfer of these personal data to persons or bodies outside of the organisation concerned shall be
admissible only if the requirements of Section 4a (3) are met. Sub-section 3, No. 2 shall apply mutatis
mutandis.

Section 48 Report of the Federal Government

The Federal Government shall report to the German Bundestag
1. by 31 December 2012 on the impacts of Sections 30a and 42a,
2. by 31 December 2014 on the impacts of the amendments to Sections 28 and 29.

If the Federal Government is of the view that legislative measures are advisable, the report shall contain a recommendation.

Annex (to Section 9, first sentence)

Where personal data are processed or used in automated form, the internal organization of authorities or enterprises is to be such that it meets the specific requirements of data protection. In particular, measures suited to the type of personal data or categories of data to be protected shall be taken

1. to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
2. to prevent data processing systems from being used without authorization (access control),
3. to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
4. to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and

check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
5. to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
6. to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
7. to ensure that personal data are protected against accidental destruction or loss (availability control),
8. to ensure that data collected for different purposes can be processed separately.
One measure in accordance with the second sentence Nos. 2 to 4 is in particular the use of the latest encryption procedures.

附錄五、德國聯邦電信法

Telecommunications Act (TKG)*

of 22 June 2004

The German Bundestag, with the consent of the German Bundesrat, has adopted the following

Act–

Contents

This Act serves to transpose the following Directives–

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory

framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33);

Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of

electronic communications networks and services (Authorisation Directive) (OJ L 108 page 21);

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) (OJ L 108

page 7);

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users'

rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51);

and

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of

personal data and the protection of privacy in the electronic communications sector (Directive on privacy and

electronic communications) (OJ L 108 page 37).

2

7

PART 1

GENERAL PROVISIONS

Section 1

Legislative Purpose

The purpose of this Act is, through technology-neutral regulation, to promote competition and efficient infrastructures in telecommunications and to guarantee appropriate and adequate services throughout the Federal Republic of Germany.

Section 2

Regulation and Aims

(1) Telecommunications regulation shall be under federal authority.

(2) The aims of regulation shall be–

1. to safeguard user, most notably consumer, interests in telecommunications and to safeguard telecommunications privacy;
2. to secure fair competition and to promote telecommunications markets with sustainable competition in services and networks and in associated facilities and services, in rural areas as well;
3. to encourage efficient investment in infrastructure and to promote innovation;
4. to promote development of the internal market of the European Union;
5. to ensure provision throughout the Federal Republic of Germany of basic telecommunications services (universal services) at affordable prices;
6. to promote telecommunications services in public institutions;
7. to secure efficient and interference-free use of frequencies, account also being taken of broadcasting interests;
8. to secure efficient use of numbering resources;
9. to protect public safety interests.

(3) Unless this Act expressly makes definitive arrangements, the provisions of the Competition Act remain applicable. The duties and responsibilities of the cartel authorities remain unaffected.

(4) The sovereign rights of the Federal Minister of Defence remain unaffected.

(5) Broadcasting and comparable telemedia interests shall be taken into account. The provisions of the media legislation of the federal states remain unaffected.

8

Section 3

Definitions

For the purposes of this Act

1. "call" means a connection established by means of a publicly available telephone service, supporting two-way communication in real time;
2. "application programming interface" means the software interface between applications and the operating functions of digital television receivers;
3. "customer data" means the data of a subscriber collected for the purpose of establishing, framing the contents of, modifying or terminating a contract for telecommunications services;
4. "significant market power" ("SMP") of one or more undertakings is deemed present where the criteria laid down in section 11(1) sentences 3 to 5 apply;
5. "value added service" means a service which requires the collection and use of traffic data or location data beyond that which is necessary for the transmission or billing of a communication;
6. "service provider" means a person who, on a wholly or partly commercial basis,

a) provides a telecommunications service, or

b) contributes to the provision of such service;

7. "digital television receiver" means a television set with an integrated digital decoder or a digital decoder designed for connection to the television set for the use of digitally transmitted television signals which can be enriched with additional signals, including conditional access;
8. "end-user" means a legal entity or a natural person not operating a public telecommunications network or providing a publicly available telecommunications service;
9. "frequency usage" means any wanted emission or radiation of electromagnetic waves between 9 kHz and 3000 GHz for use by radio services or other applications of electromagnetic waves. Frequency usage for the purposes of this Act also means the routing of electromagnetic waves in and along conductors in respect of which free use as provided for by section 53(2) sentence 3 is not given;
10. "commercial provision of telecommunications services" means telecommunications offered to third parties on a sustained basis, with or without profit-making intent;
11. "customer cards" means cards through the agency of which telecommunications connections can be established and personal data collected;
12. "sustainable competitive market" means a market in which competition has been secured such that it continues even after sector-specific regulation has been withdrawn;
13. "numbers" means character sequences which in telecommunications networks serve the purpose of addressing;
9
14. "user" means a natural person using a telecommunications service for private or business purposes, without necessarily having subscribed to that service;
15. "public pay telephone" means a telephone available to the general public, for the use of which the means of payment may include coins and/or credit/debit cards and/or prepayment cards, including cards for use with dialling codes;
16. "public telephone network" means a telecommunications network used to provide publicly available telephone services and which, in addition, supports other services such as facsimile and data communications, and functional Internet access;
17. "publicly available telephone service" means a service available to the public for originating and receiving national and international calls, including a facility for making emergency calls; publicly available telephone service also includes the following services: provision of operator assistance, directory enquiry services, directories, provision of public pay telephones, provision of service under special terms and provision of non-geographic services;
18. "telephone number" means a number, the dialling of which in the public telephone service allows a connection to a specific destination to be set up;
19. "location data" means any data collected or used in a telecommunications network, indicating the geographic position of the terminal equipment of an end-user of a publicly

available telecommunications service;

20. "subscriber" means a natural person or a legal entity who or which is party to a contract with a provider of telecommunications services for the supply of such services;

21. "local loop" means the physical circuit connecting the network termination point at the subscriber's to the main distribution frame or equivalent facility in public fixed telephone networks;

22. "telecommunications" means the technical process of sending, transmitting and receiving signals by means of telecommunications systems;

23. "telecommunications systems" means technical facilities or equipment capable of sending, transmitting, switching, receiving, steering or controlling electromagnetic or optical signals identifiable as messages;

24. "telecommunications services" means services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks used for broadcasting;

25. "telecommunications-based services" means services which do not invoke a service delivered in a different place or at a different time but whose content service is delivered in the course of the telecommunications connection;

26. "telecommunications lines" means underground or overhead telecommunications cable plant, including the associated switching and distribution equipment, poles and supports, cable chambers and ducts;

10

27. "telecommunications network" means transmission systems and, where applicable, switching and routing equipment and other resources in their entirety which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

28. "transmission path" means telecommunications systems in the form of cable or wireless links with the associated transmission equipment, as point-to-point or point-to-multipoint links with a given information throughput (bandwidth or bit rate), including their network terminations;

29. "undertaking" means the undertaking itself or affiliated undertakings within the meaning of section 36(2) and section 37(1) and (2) of the Competition Act;

30. "traffic data" means data collected, processed or used in the provision of a telecommunications service;

31. "effective competition" means the absence of significant market power within the meaning of section 11(1) sentences 3 to 5;

32. "access" means the provision of services and/or the making available of facilities to another undertaking, under defined conditions, for the purpose of providing telecommunications services;

33. "conditional access systems" means technical procedures and/or arrangements making the legitimate use of protected broadcasting programmes conditional upon subscription or individual authorisation;

34. "interconnection" means the access providing the physical and logical linking of public telecommunications networks for the purpose of enabling the users of one undertaking to communicate with users of the same or another undertaking or to make use of services provided by another undertaking; services may be provided by the parties concerned or by other parties that have access to the network. Interconnection is a special type of access implemented between public telecommunications network operators.

Section 4

International Reporting Requirements

Public telecommunications network operators and providers of publicly available telecommunications services shall provide the Regulatory Authority, upon request, with all such information as it requires to fulfil its reporting requirements in relation to the European Commission and other international bodies.

11

Section 5

Means of Publication

Publications and notifications which the Regulatory Authority is required to effect under this Act shall be placed in its Official Gazette and on its website, unless otherwise provided for. Technical directives are also to be published in the Regulatory Authority Official Gazette.

Section 6

Notification Requirement

(1) Any person operating a public telecommunications network on a profit-oriented basis or providing a publicly available telecommunications service on a profit-oriented basis shall notify the Regulatory Authority without undue delay of beginning to provide, of providing with differences or of ceasing to provide his activity and of any changes in his undertaking. Such notification requires written form.

(2) The notification shall include the information required to identify the operator or provider according to subsection (1), in particular the company register number, the address, a short description of the network or service being provided and the date on which provision of the activity is due to begin. The notification is to be made on a form prescribed and published by the Regulatory Authority.

(3) Upon request, the Regulatory Authority shall within a period of one week confirm that the notification according to subsection (2) is complete and certify that the undertaking has the rights

granted by or under this Act.

(4) The Regulatory Authority shall at regular intervals publish a list of notified undertakings.

(5) Where it is clear that the activity has ceased and the Regulatory Authority has not been notified in writing of such cessation within a period of six months, the Regulatory Authority may establish ex officio that the activity has ceased to be provided.

Section 7

Structural Separation

Undertakings operating public telecommunications networks or providing publicly available telecommunications services and having special or exclusive rights within the European Union for the provision of services in other sectors shall be required

1. structurally to separate the activities associated with the making available of public telecommunications networks and the provision of publicly available telecommunications services; or

2. to keep separate accounts for the activities associated with the making available of public telecommunications networks or the provision of publicly available telecommunications services to the extent that would be required if these activities were carried out by legally independent undertakings, so as to identify all elements of cost and revenue of these activities, with the basis for their calculation and the detailed allocation methods used, including an itemised breakdown of fixed assets and structural costs.

12

Section 8

International Status

(1) Undertakings providing international telecommunications services or, under their service offer, operating radio equipment which may cause harmful interference to the radio services of other countries, are deemed recognised operating agencies within the meaning of the Constitution and the Convention of the International Telecommunication Union. These undertakings are subject to the obligations arising from the Constitution of the International Telecommunication Union.

(2) Under the provisions of the Constitution of the International Telecommunication Union undertakings providing international telecommunications services shall

1. give absolute priority to all telecommunications concerning safety of life at sea, on land, in the air or in space, as well as to epidemiological telecommunications of exceptional urgency of the World Health Organisation;

2. accord priority to government telecommunications over other telecommunications to the extent practicable upon specific request by the originator.

PART 2

MARKET REGULATION

C h a p t e r 1

Section 9

Principles

(1) Markets meeting the conditions of section 10 and shown by a market analysis according to section 11 not to be effectively competitive are subject to regulation in accordance with the provisions of this Part.

(2) Undertakings having significant market power ("SMP undertakings") in markets within the meaning of section 11 are subject to measures imposed by the Regulatory Authority in accordance with this Part.

(3) Section 18 remains unaffected.

Section 10

Market Definition

(1) The Regulatory Authority shall identify, for the first time without undue delay after the entry into force of this Act, the relevant product and geographic telecommunications markets warranting regulation in accordance with the provisions of this Part.

13

(2) Warranting regulation in accordance with the provisions of this Part are markets with high, non-transitory entry barriers of a structural or legal nature, markets which do not tend towards effective competition within the relevant time horizon and markets in respect of which the application of competition law alone would not adequately address the market failure(s) concerned. Such markets shall be identified by the Regulatory Authority within the limits of its power of interpretation. In doing so, it shall take the utmost account of the recommendation on relevant product and service markets which the Commission publishes under Article 15(1) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33), as amended.

(3) The Regulatory Authority shall, following the procedure set out in section 12, submit to the Commission its proposals for market definitions in all cases in which such definitions would affect trade between Member States.

Section 11

Market Analysis

(1) After identifying markets which, under section 10, warrant regulation in accordance with this Part, the Regulatory Authority shall determine whether there is effective competition in the market being analysed. Effective competition is deemed absent if one or more undertakings have significant market power in this market. An undertaking is deemed to have significant market power if, either individually or jointly with others, it enjoys a position equivalent to dominance, ie a position of economic strength affording it the power to behave to an appreciable extent independently of competitors and end-users. In determining whether there is effective

competition, the Regulatory Authority shall take the utmost account of the criteria established by the Commission, published in the Commission guidelines on market analysis and the assessment of significant market power referred to in Article 15(2) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33), as amended. Where an undertaking has significant market power in a relevant market, it may also be deemed an SMP undertaking in a closely related relevant market identified in accordance with section 10(2) where the links between the two markets are such as to allow the market power held in one market to be leveraged into the other, thereby strengthening the overall market power of the undertaking.

(2) In the case of transnational markets within the area of application of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33), the Regulatory Authority shall determine whether significant market power within the meaning of subsection (1) is present together with the national regulatory authorities of the Member States comprised in these markets.

(3) The proposals for determinations according to subsections (1) and (2), including designations of SMP undertakings, shall be submitted to the Commission following the procedure set out in section 12 inasmuch as trade between Member States would be affected.

14

Section 12

Consultation and Consolidation Procedure

(1) The Regulatory Authority shall give interested parties the opportunity to make representations, within a fixed period, on the proposals referred to in sections 10 and 11. The consultation procedures and their outcomes shall be published by the Regulatory Authority. This does not affect protection of the trade and operating secrets of the parties concerned. For this purpose the Regulatory Authority shall establish a single information point through which all current consultations can be accessed.

(2) Where sections 10(3) and 11(3) provide for a submission, the following procedure applies–

1. After carrying out the consultation procedure according to subsection (1) the Regulatory Authority shall make the proposals referred to in sections 10 and 11 and the underlying reasoning available to the Commission and to the regulatory authorities of every other Member State at the same time, informing the Commission and the regulatory authorities of every other Member State accordingly. The Regulatory Authority may not give effect to the proposals referred to in sections 10 and 11 prior to the expiry of a period of one month or longer as determined under subsection (1).

2. The Regulatory Authority shall take the utmost account of the representations of the

Commission and the other national regulatory authorities according to para 1. It shall communicate the resulting draft to the Commission.

3. Where a draft according to sections 10 and 11 identifies a relevant market which differs from those defined in the prevailing version of the recommendation on relevant product and service markets published by the Commission under Article 15(1) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33) or where such draft determines the extent to which one or more undertakings have significant market power in this market and where the Commission indicates within the representations period according to para 1 sentence 2 that the draft would create a barrier to the single market or has serious doubts as to its compatibility with Community law and, in particular, the objectives of Article 8 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33), the Regulatory Authority shall not give effect to the proposals before the end of a further two months. Where the Commission takes a decision within this period requiring the Regulatory Authority to withdraw the draft, the Regulatory Authority is bound by such decision. It may again consult the parties concerned on the Commission's decision following the procedure set out in subsection (1). Where the Regulatory Authority wishes to accept the amendments proposed by the Commission, it shall amend the draft in accordance with the Commission's decision and submit the amended draft to the Commission. Otherwise it shall inform the Federal Ministry of Economics and Labour of the Commission's decision.

4. In exceptional circumstances where the Regulatory Authority considers there is an urgent need to act – in derogation of the procedure according to subsection (1) and paras 1 to 3 – in order to safeguard competition and protect user interests, it may adopt proportionate and provisional measures immediately. It shall without undue delay communicate such measures, with full reasons, to the Commission and the regulatory authorities of every other Member State. A decision by the Regulatory Authority to make such measures permanent or

15

to extend the time for which they are applicable is subject to the provisions of subsection (1) and paras 1 to 3.

Section 13

Remedies

(1) As far as the Regulatory Authority (by order) imposes, amends, maintains or withdraws obligations as referred to in sections 19, 20, 21, 24, 30, 39, 40 or 41(1) as a result of market analysis according to section 11, the procedure set out in section 12(1) and (2) paras 1, 2 and 4 applies accordingly inasmuch as the measure would affect trade between Member States. Undertakings affected are to be given an appropriate period of notice of the withdrawal of any

such obligations. The procedure according to sentence 1 may be carried out by the Regulatory Authority together with or subsequent to the procedure set out in section 12. Sentences 1 and 2 likewise apply to obligations as referred to in section 18.

(2) In the case of section 11(2) the Regulatory Authority shall, in agreement with the national regulatory authorities concerned, determine those obligations which are to be fulfilled by the SMP undertaking(s). The procedure set out in section 12(1) and (2) paras 1, 2 and 4 applies accordingly.

(3) Decisions as referred to in sections 18, 19, 20, 21, 24, 30, 39, 40 and 41(1) are issued together with the outcomes of the procedures set out in sections 10 and 11 as a single administrative act.

Section 14

Review of Market Definitions and Analyses

(1) Where the Regulatory Authority becomes aware of facts warranting the assumption that the outcomes reached under sections 10 to 12 no longer reflect the market as it currently is or where the recommendation referred to in Article 15(1) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33) has been amended, the arrangements of sections 10 to 13 apply accordingly.

(2) Apart from the cases referred to in subsection (1) the Regulatory Authority shall submit every two years the findings of its review of market definitions according to section 10 and of market analyses according to section 11.

Section 15

Procedure For Other Relevant Measures

Apart from the cases referred to in sections 10, 11 and 13 the Regulatory Authority shall, in respect of all measures having a significant impact on the relevant market, follow the procedure set out in section 12(1) prior to taking a decision, unless this is otherwise regulated by law.

16

C h a p t e r 2

A c c e s s R e g u l a t i o n

Section 16

Interconnection Agreements

Every public telecommunications network operator shall, upon request, undertake to make an interconnection offer to other public telecommunications network operators in order to secure user communication, the provision of telecommunications services and service interoperability throughout the Community.

Section 17

Confidentiality of Information

Information obtained from public network operators in the process of negotiating access or

interconnection may be used solely for the purposes for which it was provided. Such information shall not be passed on to any other party, in particular other departments, subsidiaries or partners of the negotiating parties, for whom such information could provide a competitive advantage.

Section 18

Control of End-User Access

(1) The Regulatory Authority may, in justified cases, impose obligations on public telecommunications network operators controlling access to end-users and not having significant market power to interconnect, upon request, their networks with those of other public telecommunications network operators, as far as may be necessary to secure user communication, the provision of services and service interoperability. Additionally, the Regulatory Authority may impose further access obligations on public telecommunications network operators controlling access to end-users and not having significant market power as far as may be necessary to secure end-to-end connectivity.

(2) With a view to developing sustainable competition in the retail market the Regulatory Authority may require public telecommunications network operators controlling access to endusers not to treat particular requesting public telecommunications network operators differently, directly or indirectly, without objectively justifiable reason, from other requesting public telecommunications network operators with regard to the availability and billing of telecommunications services, of services according to section 78(2) paras 3 and 4 and of telecommunications-based services. Where the Regulatory Authority imposes obligations under sentence 1, section 42(4) applies accordingly.

(3) The measures set out in subsection (1) shall be objective, transparent and nondiscriminatory. Section 21(1) sentence 2 and (4) apply accordingly.

17

Section 19

Prohibition on Discrimination

(1) The Regulatory Authority may impose obligations on a public telecommunications network operator with significant market power requiring access agreements to be based on objective criteria, to be transparent, to grant equally good access and to meet the requirements of fairness and reasonableness.

(2) Obligations of non-discrimination shall ensure, in particular, that the operator applies equivalent conditions in the same circumstances to other undertakings providing like services, and provides services and information to others under the same conditions and of the same quality as it provides for its own services or those of its subsidiaries or partners.

Section 20

Transparency Obligation

(1) The Regulatory Authority may impose an obligation on an SMP public telecommunications

network operator to publish, for undertakings with access entitlements, all such information as is required for use of the relevant access services and/or facilities, in particular accounting information, information on technical specifications, network characteristics, terms and conditions of supply and use, and the charges payable.

(2) The Regulatory Authority is authorised to specify the information an SMP operator is to make available and in which form the information is to be made available, as far as this is proportionate.

Section 21

Access Obligations

(1) The Regulatory Authority may, upon request or on its own initiative, impose obligations on SMP public telecommunications network operators to grant other undertakings access, including unbundled access that properly reflects their requirements, in particular if otherwise, the development of a sustainable competitive downstream retail market would be hindered or this development would run counter to the interests of the end-users. In considering whether an access obligation is justified and proportionate to the regulatory aims according to section 2(2), the Regulatory Authority has to take into account, in particular, the following factors–

1. the technical and economic viability, having regard to the pace of market development, of using or installing alternative facilities, bearing in mind the nature and type of interconnection or access proposed;
2. the feasibility of providing the access proposed, in relation to the capacity available;
3. the initial investment by the facility owner, bearing in mind the risks involved in making the investment;
4. the need to secure competition in public telecommunications networks and publicly available telecommunications services in the long term, most notably by creating incentives for efficient investment in facilities which will secure more competition in the long term;

18

5. industrial property rights and intellectual property rights;
6. the provision of services that are available throughout Europe; and
7. whether already imposed obligations as referred to in this Part or non-mandated services available in and taken up by a large part of the market are sufficient to ensure the regulatory aims according to section 2(2).

(2) The Regulatory Authority may, having regard to subsection (1), require SMP public telecommunications network operators, amongst other things,

1. to grant access to specified network elements and/or facilities, including unbundled broadband access;
2. not to withdraw access to facilities;
3. to grant access on a wholesale basis to particular services offered by the operator as offered to end-users, for the purpose of resale by third parties in their own name and for their own

account. In doing so, past and future investment in innovative services is to be taken into consideration;

4. to create the necessary prerequisites for the interoperability of end-to-end communication, including the provision of facilities for intelligent network services and roaming (enabling the use of other operators' mobile networks outside the coverage area of the requesting mobile operator, for the requesting operator's end-users);

5. to grant access to operational support systems or similar software systems required to secure fair competition in the provision of services, while ensuring the efficient use of existing facilities;

6. to allow, in meeting the access obligations imposed under this subsection or under subsection (3), the use of access services and facilities and cooperation between undertakings with access entitlements, unless an SMP operator shows in the given instance that, for technical reasons, such use or cooperation is not possible or is possible to a limited extent only;

7. to grant access to single billing services and to the acceptance or first-time collection of receivables in accordance with the following, as far as the bill-issuers have not entered into an agreement with the predominant part of the hence relevant market of the providers of publicly available telecommunications services to whom their access customers are able to connect, and to grant other providers who have not entered into such agreement non-discriminatory access to these services under the terms and conditions laid down in the agreement–

a) End-users who have not agreed anything else with other providers of publicly available telecommunications services are to be issued a bill by the bill-issuer which, independently of the tariff structures, presents the charges for telecommunications services, for services according to section 78(2) para 3 and for telecommunicationsbased services from other providers taken via the network termination point of the enduser. This also applies to charges for authorisation codes transmitted during the telephone connection when these are concerned solely with services. Payment to the

19

bill-issuer of these charges is effected by means of a single bill for the whole of the service taken and for the charges payable to him.

b) A billing obligation cannot be imposed in respect of unmetered services within the meaning of subpara a) sentences 1 and 2 whose charges exceed 30 euros (10 euros from 1 January 2008), metered telecommunications-based services and services according to subpara a) sentence 2 with charges exceeding 2 euros per minute in each case or for any services for which authorisation is required. Nor can an obligation to handle complaints relating to services billed for third parties, to send reminders or to collect charges payable to third parties be imposed.

c) Customer data required for the purpose of handling complaints, sending reminders or collecting charges for services within the meaning of subpara a) sentences 1 and 2 are to be transmitted by the bill-issuer to providers of publicly available telecommunications services. Providers billing customers themselves for services within the meaning of subpara a) sentence 2 are, from 1 April 2005, to be provided by the bill-issuer with the customer data required.

d) Providers of publicly available telecommunications services have to ensure in relation to the bill-issuer that no data records for services for which billing is to be effected which are not in compliance with the legal provisions or with consumer protection legislation are transmitted to him. The bill-issuer is not responsible or liable for services billed on behalf of third parties.

e) In his reminders the bill-issuer has to include an insert, given prominence by the way it is printed, stating that the customer may pay not only the amount of the reminder, but also the original, possibly higher, amount to the bill-issuer with discharging effect.

(3) The Regulatory Authority should impose the following obligations under subsection (1) on SMP public telecommunications network operators–

1. the granting of fully unbundled access to the local loop and shared access to the local loop (provision of access to the local loop or to the local sub-loop in such manner as to enable use of the entire frequency spectrum of the twisted metallic pair);

2. the interconnection of telecommunications networks;

3. the granting of open access to technical interfaces, protocols and other key technologies essential for service interoperability and virtual network services;

4. the provision of colocation and other forms of facility sharing, including building, duct and mast sharing, and the granting, to the users or their agents, of access to these facilities at any time.

(4) Where an operator shows that use of the facility would endanger the maintenance of network integrity or the safety of network operations, the Regulatory Authority shall not impose the access obligation relating to the facility or shall impose the obligation in different form. The maintenance of network integrity and the safety of network operations are to be judged on the basis of objective standards.

20

Section 22

Access Agreements

(1) An SMP public telecommunications network operator in relation to whom an access obligation according to section 21 has been imposed is to submit to other undertakings requesting these services and facilities in order to provide telecommunications services themselves, without undue delay but in any case not later than three months after the access obligation has been imposed, an offer for such access.

(2) Access agreements concluded by an SMP public telecommunications network operator require written form.

(3) An SMP public telecommunications network operator shall submit to the Regulatory Authority agreements on access services and facilities to which he is party as a provider without undue delay after their conclusion. The Regulatory Authority shall publish the place in which and the hours during which an agreement according to sentence 1 is available for inspection to persons requesting access services and facilities.

Section 23

Reference Offer

(1) The Regulatory Authority should require an SMP public telecommunications network operator who is subject to an access obligation according to section 21 to publish, normally within three months, a reference offer for the access service and/or facility for which there is general demand. This decision may be issued together with a decision on the imposition of an access obligation according to section 21.

(2) Where an SMP public telecommunications network operator does not submit a reference offer, the Regulatory Authority shall identify the access services and/or facilities for which there is general demand. For this purpose the Regulatory Authority shall give actual and potential users of such services and facilities the opportunity to comment. It shall subsequently give the SMP operator the opportunity to comment on which of the services and facilities thus identified should, in his view, constitute part of a reference offer.

(3) The Regulatory Authority shall, having regard to the comments referred to in subsection (2), determine the access services the SMP operator has to provide and the access facilities the SMP operator has to make available in a reference offer. The Regulatory Authority shall request the operator to submit, within a specified period, a corresponding reference offer with terms and conditions of supply and use, including the rates. It may attach to this request requirements relating to particular conditions, most notably with regard to fairness, reasonableness and timeliness. The reference offer shall be sufficiently comprehensive to enable acceptance by all users without further negotiations. The above sentences also apply in the event of the SMP operator having submitted an inadequate reference offer.

(4) The Regulatory Authority shall check and, in the event of failure to comply with the requirements relating to particular conditions, most notably with regard to fairness, reasonableness and timeliness, amend the reference offers submitted. The Regulatory Authority generally determines a minimum duration for reference offers. The SMP operator shall notify the Regulatory Authority three months prior to the expiry of this minimum duration of any intended modifications to or cessation of the reference offer. The decisions referred to in subsections (3)

21

and (4) sentences 1 and 2 may be challenged in their entirety only. Sections 27 to 37 apply in respect of rates regulation.

(5) Where an access service or facility is already the subject matter of an access agreement according to section 22, the Regulatory Authority may oblige the SMP public telecommunications network operator to offer, on a non-discriminatory basis, this service or facility to other users as well, if general demand for such service or facility is likely to develop. This also applies to access services and facilities an SMP public telecommunications network operator has been obliged to provide or make available under an order according to section 25.
(6) The Regulatory Authority may oblige an SMP public telecommunications network operator to modify his reference offer if general demand has changed significantly. This may refer both to the services and facilities themselves and to the main conditions for their supply. Subsections (2) to (5) apply with regard to modifications to the reference offer.
(7) The operator is obliged to include the reference offer in his general terms and conditions.

Section 24

Accounting Separation

(1) The Regulatory Authority may require an SMP public telecommunications network operator to keep separate accounts for certain activities related to access services and facilities. In particular, the Regulatory Authority as a rule requires a vertically integrated undertaking to make its wholesale prices and its internal transfer prices transparent. This is to prevent, amongst other things, a breach of the prohibition on discrimination and unlawful cross-subsidies. The Regulatory Authority may specify the format to be used and the accounting method to be applied.
(2) The Regulatory Authority may require submission, in prescribed form, of the cost accounting and bookkeeping records referred to in subsection (1), including all related information and documents, upon request. The Regulatory Authority may publish such information in suitable form insofar as this would contribute to achieving the aims set out in section 2(2). In doing so it shall have regard to the provisions on the maintenance of trade and operating secrets.

Section 25

Regulatory Authority Orders

(1) Where an access agreement according to section 22 or an agreement on access services and facilities according to section 18 has not been brought about either wholly or in part and the conditions specified in this Act for imposing an obligation to grant access are given, the Regulatory Authority shall, after hearing the parties concerned, order access within a period of ten weeks from referral by one of the parties to the intended agreement. In cases which have to be specially justified the Regulatory Authority may, within the period referred to in sentence 1, extend the procedure to a maximum of four months.
(2) An order is permissible only insofar as and for as long as the parties concerned fail to reach an access or interconnection agreement.

22

(3) The referral according to subsection (1) shall be in written form; it shall be substantiated. In particular, the following is to be set out–

1. the precise content of the Regulatory Authority order;
2. when access was requested and for which concrete services and/or facilities;
3. that serious negotiations have been held or that the other party has declined to enter into any such negotiations;
4. the points on which agreement has not been reached; and
5. explanatory remarks on the technical feasibility of any specific technical measures requested.

The referral may be withdrawn until such time as the order is issued.

(4) For the purpose of achieving the aims set out in section 2(2) the Regulatory Authority may also open a case on its own initiative.

(5) The subject matter of such order may be any of the terms and conditions of an access agreement, or the rates. The Regulatory Authority may attach to such order conditions with regard to fairness, reasonableness and timeliness. Sections 27 to 38 apply in respect of determining the rates.

(6) Where both the terms and conditions of an access agreement and the rates payable for the services and/or facilities requested are disputed, the Regulatory Authority should take partial decisions with regard to the terms and conditions and to the rates. The periods referred to in subsection (1) apply to any partial decisions taken by the Regulatory Authority. The Regulatory Authority order may be challenged in its entirety only.

(7) Documents submitted in the course of proceedings are considered only if this does not compromise observance of the period specified in subsection (1).

(8) Operators affected shall follow a Regulatory Authority order without undue delay unless the Regulatory Authority has specified a period in the order for giving effect to the order. To enforce such order the Regulatory Authority may set a penalty not exceeding one million euros in accordance with the Administrative Enforcement Act.

Section 26

Publication

The Regulatory Authority shall, having regard to the maintenance of the trade and operating secrets of the undertakings concerned, publish measures taken under this Chapter.

23

C h a p t e r 3

R a t e s R e g u l a t i o n

Subchapter 1

General Provisions

Section 27

Aim of Rates Regulation

(1) The aim of rates regulation is to prevent the anti-competitive exploitation of, hindrance to and discrimination of end-users and competitors as a result of the pricing measures of SMP undertakings.

(2) The Regulatory Authority shall take care that rates regulation measures in their entirety are coordinated (consistency requirement). In particular, the Regulatory Authority shall coordinate the timeframes and the content of its measures and consider whether each measure is proportionate to the aims according to section 2(2).

(3) The Regulatory Authority shall, insofar as broadcasting and comparable telemedia interests according to section 2(5) sentence 1 are concerned, inform the state media authority with competence accordingly and include it in proceedings initiated. Upon application by the state media authority the Regulatory Authority shall, with reference to this Act, look into the matter of initiating proceedings and ordering measures in accordance with the following provisions.

Section 28

Anti-Competitive Conduct

by an SMP Undertaking in Levying and Agreeing Rates

(1) No SMP telecommunications service provider and no SMP public telecommunications network operator may abuse his position when levying and agreeing rates. Abuse is constituted, in particular, by the undertaking levying rates which

1. prevail solely as a result of his having significant market power in the particular telecommunications market;
2. considerably prejudice the competitive opportunities of other undertakings in a telecommunications market; or
3. create advantages for particular users in relation to other users of the same or similar telecommunications services,

unless it has been shown that the conduct referred to in paras 2 and 3 is objectively justified.

(2) Abuse within the meaning of subsection (1) para 2 is presumed where

1. the price for the service in question does not cover its long run incremental costs, including a reasonable return on capital employed;

24

2. the margin between the price the SMP public telecommunications operator charges competitors for an access service or facility and the corresponding retail price is not enough to enable an efficient undertaking to achieve a reasonable return on capital employed in the retail market (margin squeeze); or
3. an undertaking bundles its products in objectively unreasonable manner. In determining whether or not this is the case, the Regulatory Authority has to consider in particular whether efficient competitors of the SMP undertaking could offer the bundled product on comparable terms.

Section 29

Rates Regulation Orders

(1) The Regulatory Authority may, as part of or in preparation for rates regulation procedures, order that

1. it be provided by an SMP undertaking with detailed information on its service offer, on its current and expected sales, on its current and expected sales volumes and costs, on the foreseeable effects on both end-users and competitors and with such other documents and information as it deems necessary for the proper exercise of its rates regulation rights under this Act; and

2. an SMP undertaking structure its cost statements in such a way as enables the Regulatory Authority to obtain the data required for rates regulation under this Act.

In addition, the Regulatory Authority may order that the documents referred to in paras 1 and 2 be transmitted on data carrier. The undertaking has to provide an assurance of conformity with the written documents.

(2) The Regulatory Authority may impose obligations on an SMP undertaking with regard to cost accounting systems. In such case it may oblige the SMP undertaking to make a description of the compliant cost accounting system publicly available, showing at least the main categories under which costs are grouped and the rules used to allocate costs, provided it does not effect such publication itself. Compliance of the cost accounting system is verified by the Regulatory Authority; the Regulatory Authority may also charge an independent body with verification. A statement concerning compliance is published annually.

(3) The Regulatory Authority may, by separate decision, oblige an SMP undertaking to offer access on the basis of particular tariff systems and to apply particular cost recovery mechanisms as far as may be necessary to achieve the regulatory aims according to section 2(2). In imposing such obligations the Regulatory Authority has to ensure the promotion of economic efficiency and sustainable competition and maximum benefit to the end-user from such obligations. Where the Regulatory Authority takes a decision as referred to in sentence 1, the SMP provider has to submit a rates proposal within a period of two weeks. The Regulatory Authority shall take a decision within a period of four weeks of submission of the proposal or of expiry of the time limit.

(4) To enforce orders according to subsections (1) and (2) a penalty not exceeding one million euros may be set in accordance with the Administrative Enforcement Act.

(5) The Regulatory Authority may prescribe the form in which rates and changes in rates, including service specifications and other rates-related components, are to be published.

25

(6) The Regulatory Authority may also require undertakings not having significant market power to provide information as referred to in subsection (1) para 1 and proceed in accordance with subsection (4) where necessary for the proper exercise of rates regulation under this Part.

Subchapter 2

Regulation of Rates for Access Services and Facilities

Section 30

Rates Regulation

(1) Save as provided in the subsections below, the rates charged by an SMP public telecommunications network operator for access services and/or facilities mandated under section 21 are subject to approval by the Regulatory Authority in accordance with section 31. In derogation of sentence 1 the Regulatory Authority should subject such rates to ex post regulation in accordance with section 38(2) to (4) when

1. the operator does not also, at the same time, have significant market power in the retail market in which he is active;
2. significant market power has been determined after the entry into force of this Act without the operator having been designated by the Regulatory Authority as having dominance prior to the entry into force of this Act;
3. this measure is sufficient to achieve the regulatory aims according to section 2(2).

(2) In derogation of subsection (1) rates for access services according to section 21(2) para 7 are subject to ex post regulation in accordance with section 38(2) to (4). Regulation of these rates under this Act is ruled out where an agreement according to section 21(2) para 7 has come about or where services which the bill-issuer cannot be obliged to provide are concerned.

(3) Rates charged by an SMP public telecommunications network operator for access services or facilities not mandated under section 21 are subject to ex post regulation in accordance with section 38.

(4) Rates charged under obligations according to section 18 by an operator who controls access to end-users and who does not have significant market power are subject to ex post regulation. Section 38(2) to (4) apply accordingly.

(5) Charges levied by an SMP public telecommunications network operator for access on a wholesale basis to particular services offered by him for the purpose of resale by third parties in their own name and for their own account shall, in derogation of section 31(1), be calculated on a retail minus basis to allow an efficient provider of telecommunications services to achieve a reasonable return on capital employed in the retail market. The charges shall be equivalent to the costs of efficient service provision at least.

26

Section 31

Approval

(1) Rates which require approval under section 30(1) sentence 1 are eligible for approval when they do not exceed the costs of efficient service provision. In justified cases the Regulatory Authority may review eligibility in accordance with the comparable markets principle as set out in section 35(1) sentence 1 para 1.

(2) The costs of efficient service provision are derived from the long run incremental costs of

providing the service and an appropriate mark-up for volume-neutral common costs, inclusive of a reasonable return on capital employed, as far as these costs are required to provide the service. Section 79 remains unaffected.

(3) Expenditure exceeding that referred to in subsection (2) is taken into account only insofar as and for as long as such expenditure derives from a legal obligation or the undertaking seeking approval demonstrates other proper justification for it. Where the Regulatory Authority, in examining the cost statements, deems essential components of the stated costs inefficient, it shall request the operator, without undue delay, to explain whether and to what extent these cost components constitute expenditure within the meaning of sentence 1.

(4) In determining a reasonable return on capital employed the Regulatory Authority takes into account, in particular, the following factors–

1. the capital structure of the regulated undertaking;
2. the situation in the national and international capital markets and the rating of the regulated undertaking in these markets;
3. the requirements concerning the return on equity capital employed, whereby the service-specific risks of equity capital employed may also be acknowledged; and
4. the long term stability of the economic environment, also with a view to the situation as regards competition in the telecommunications markets.

(5) Rates subject to approval charged by an SMP public telecommunications network operator for access services and facilities are to be submitted to the Regulatory Authority prior to their intended effective date, together with all such documents as are required for approval to be granted. Where approval has been granted for a limited period only, the submission has to be effected not later than ten weeks before such limited period expires.

(6) The Regulatory Authority may require the submission of rates proposals. Where such request is not met within one month of its having been received, the Regulatory Authority shall commence proceedings on its own initiative. The Regulatory Authority shall decide on rates proposals within a period of ten weeks of receiving the submission or of commencing owninitiative proceedings. In derogation of sentence 3 the Regulatory Authority should decide on rates proposals submitted under the procedure set out in section 34 within a period of two weeks.

27

Section 32

Forms of Approval

The Regulatory Authority shall approve rates

1. on the basis of the costs of efficient service provision for individual services; or
2. on the basis of the benchmarks prescribed by it for the average rate of change in the prices of a basket of combined services (price cap) in accordance with section 34.

Section 33

Cost Statements

(1) Together with any rates proposal according to section 31(5) or (6) the undertaking has to submit all such documents as are required to consider the submission, in particular–

1. current cost statements, to be made available on data carrier also;

2. detailed service specifications, including details of quality of service and the draft general terms and conditions; and

3. details of sales, sales volumes, the level of the different costs referred to in subsection (2) and the contribution margins, and the development of user structures for the service concerned for the two years prior to submission, for the year of submission and for the following two years.

(2) Cost statements according to subsection (1) para 1 comprise costs that can be directly allocated (direct costs) and costs that cannot be directly allocated (common costs). To be included, in particular, in the cost statements according to sentence 1 is an account of–

1. the input volumes on which cost accounting is based, the relevant prices, in each instance both separately and averaged, target and actual capacity utilisation in the documentation period; and

2. the method used to determine costs and investment values, and information on plausible keys for allocating costs to each of the undertaking's services individually.

(3) In addition, the undertaking has to submit, regularly at the beginning of every financial year, information on its total costs and on their allocation to cost centres and to the individual services (cost units), broken down into direct costs and common costs. Information relating to non-regulated services may be summarised.

(4) In the transparency and presentation of their data, the cost statements shall be such as to enable an examination by the Regulatory Authority, quantification of the costs of efficient service provision and a decision to be taken within the period referred to in section 31(6).

(5) Documents not submitted together with the proposal are taken into account only if observance of the time limits is not compromised by later submission. Any additional documents or information requested by the Regulatory Authority during proceedings need be taken into account only if submitted by the undertaking within a time limit set by the Regulatory Authority.

28

(6) The same cost accounting methods are to be applied by the undertaking for each rates proposal submitted.

(7) The powers referred to in section 29 remain unaffected.

Section 34

Price Cap

(1) The Regulatory Authority shall determine the content of the baskets. Access services may be combined in one and the same basket only when the level of competition for these services is not expected to differ significantly.

(2) The Regulatory Authority shall establish the initial rate level for the access services grouped in a basket. It shall proceed from any rates that have already been approved.

(3) The benchmarks for approval under section 32 para 2 encompass

1. the rate of price increases in the economy overall;

2. the expected rate of growth in productivity of the SMP operator; and

3. suitable secondary conditions for preventing abuse as set out in section 28.

(4) To be taken into account in the specification of benchmarks, in determination of the rate of growth in productivity in particular, is the relationship between the initial rate level and the cost of efficient service provision as set out in section 31(2).

(5) To be taken into account in the specification of benchmarks are the rates of growth in productivity of undertakings in comparable competitive markets.

(6) The Regulatory Authority shall stipulate the period for which benchmarks will remain unchanged, the historic reference periods against which compliance with benchmarks will be examined and the conditions under which the content of baskets may be changed or price differentiation within a basket made.

Section 35

Procedures for Approval

(1) Besides the cost information submitted to it, the Regulatory Authority may, in addition,

1. refer, for the purpose of comparison, to the prices of such undertakings as offer like services in comparable competitive markets; any special features of the reference markets are to be taken into account in doing so; and

2. apply, for the purpose of costing efficient service provision, cost accounting methods independent of those used by the undertaking, and refer to cost models in doing so.

Where the cost information submitted to the Regulatory Authority is not sufficient for an examination of the rates requiring approval as referred to in section 32 para 1 in conjunction with 29

section 33, the Regulatory Authority's decision may be based on an examination according to sentence 1 paras 1 or 2.

(2) In the case of approval as referred to in section 32 para 1 the Regulatory Authority shall examine compliance with the requirements of sections 28 and 31 for each rate separately. In the case of approval as referred to in section 32 para 2 the requirements of section 28 and, for the particular basket, of section 31 are deemed satisfied given compliance with the prescribed benchmarks.

(3) Approval is to be granted wholly or in part when the rates meet the requirements of sections 28 and 31 in accordance with subsection (2) and there are no grounds for denial as set out in sentences 2 and 3. Approval is to be denied when the rates are inconsistent with this Act, in particular with section 28, or with other legal provisions. The Regulatory Authority may also deny approval when the undertaking has failed to submit in full the documentation specified in

section 33.

(4) The Regulatory Authority should approve rates for a limited period.

(5) Any approvals wholly or partially approving rates already contractually agreed shall have retroactive effect from the time the SMP undertaking first provided service. In proceedings under section 123 of the Code of Administrative Court Procedure, the court may order payment for the time being of higher rates in respect of which rate proposals have been submitted when it is probable, for the most part, that there is a right to the higher rates being approved; the grounds for such order need not be stated. Where the court requires the Regulatory Authority to approve higher rates, such approval has the retroactive effect referred to in sentence 1 only when an order as referred to in sentence 2 has been issued.

(6) The Regulatory Authority shall publish all approved rates.

Section 36

Publication

(1) The Regulatory Authority shall publish decisions it intends to take on the grouping of services and on specification of the benchmarks according to section 32 para 2 and section 34. Prior to publication it shall give the undertaking to whom the decision is addressed the opportunity to make representations.

(2) In respect of submissions for approval as provided for by section 32 para 1 and in the event of proceeding as provided for by section 31(6) sentences 1 and 2 the Regulatory Authority shall publish all rates measures submitted and planned.

Section 37

Divergence from Approved Rates

(1) An SMP public telecommunications network operator may not charge any rates other than those approved by the Regulatory Authority.

(2) Contracts for services containing rates other than those approved shall become effective subject to the proviso that the approved rates apply in place of the agreed rates.

30

(3) A contractual or legal obligation to provide service shall continue to apply irrespective of whether or not the rates have been approved. The Regulatory Authority may prohibit advertising for, the conclusion, the preparation or the development of a legal transaction applying rates other than those approved or applying rates not approved but subject to approval.

Section 38

Ex Post Rates Regulation

(1) Rates subject to ex post regulation shall be submitted to the Regulatory Authority two months prior to their planned effective date. Where planned rates would clearly not be compatible with section 28 the Regulatory Authority shall, within a period of two weeks of receiving notice of the measure, prohibit introduction of the rates until such time as it has completed its examination. The Regulatory Authority is to be informed, immediately after

conclusion of the contract, of any rates measures for individually agreed services not easily applicable to a number of other users.

(2) Where the Regulatory Authority becomes aware of facts warranting the assumption that rates for access services provided or facilities made available by SMP undertakings are not in compliance with the requirements of section 28, the Regulatory Authority shall open an investigation of the rates without undue delay. It shall inform the undertaking concerned, in writing, that an investigation has been opened. Should the Regulatory Authority not be able to investigate on the basis of the comparable markets principle set out in section 35(1) para 1, it may also proceed as set out in section 33.

(3) The Regulatory Authority shall take a decision within a period of two months of the investigation being opened.

(4) Where the Regulatory Authority establishes that rates do not meet the requirements of section 28, it shall forbid such conduct as is prohibited under this Act and declare the rates objected to invalid as from such time non-compliance was established. At the same time, the Regulatory Authority may order the application of rates which meet the requirements of section 28. Where the SMP provider subsequently submits his own rates proposals the Regulatory Authority shall examine, within a period of one month, whether these rates rectify the breaches of the requirements of section 28 which have been established. Section 37 applies accordingly. Where the Regulatory Authority has established abuse of an SMP position within the meaning of section 28(2) para 3 it shall also issue an order stating how the SMP undertaking has to effect unbundling.

Subchapter 3

Regulation of Rates for Retail Services

Section 39

Rates Regulation for Retail Services

(1) Where facts warrant the assumption that obligations imposed in connection with access issues or with carrier selection and carrier preselection according to section 40 would not result in achievement of the regulatory aims according to section 2(2), the Regulatory Authority may make the rates SMP undertakings charge for retail telecommunications services subject to

31

approval. The Regulatory Authority should limit the approval requirement to those markets in which sustainable competition is not expected to develop in the foreseeable future. In the event of an approval requirement, sections 31 to 37 apply accordingly. Rates for retail services may not under section 32 para 2 be placed in a basket with rates for access services.

(2) Services according to section 78(2) paras 3 and 4 are subject to ex post regulation; section 38(2) to (4) apply accordingly.

(3) Rates for retail services supplied by SMP telecommunications service providers which are not subject to approval shall be subject to ex post regulation; section 38(2) to (4) apply

accordingly. In addition, the Regulatory Authority may, having regard to subsection (1) sentence 1, require SMP undertakings to inform it of rates measures two months prior to their planned effective date. Where planned rates would clearly not be compatible with section 28 the Regulatory Authority shall, within a period of two weeks of notice of the measure, prohibit introduction of the rates until such time as it has completed its examination. The Regulatory Authority is to be informed, immediately after conclusion of the contract, of any rates measures for individually agreed services not easily applicable to a number of other users.

(4) Any undertaking having significant market power in a retail market and obliged to grant access to a service and/or facility according to section 21 which includes components that are likewise essential to a service offer in the retail market shall be obliged to submit at the same time as its planned rates measure for the retail service an offer for the wholesale product which meets, in particular, the requirements of section 28. Where the SMP undertaking fails to submit any such wholesale offer, the Regulatory Authority may, without further examination, forbid it from asking the retail price.

C h a p t e r 4

O t h e r O b l i g a t i o n s

Section 40

Carrier Selection and Carrier Preselection

(1) The Regulatory Authority shall require undertakings designated as having significant market power in the provision of connection to and use of the public telephone network at fixed locations, in accordance with sentence 4, to enable their subscribers to access the services of all directly interconnected providers of publicly available telecommunications services. This may be done on a call-by-call basis by dialling a carrier selection code, or by means of preselection, with a facility to override any preselected choice on a call-by-call basis by dialling a carrier selection code. It should also be possible for the subscriber to preselect different carriers for local and national calls. In providing the interconnection required to fulfil this obligation it shall be ensured that, in decisions taken under Part 2, incentives for efficient investment in facilities which will secure more competition in the long term are maintained and that efficient use of the existing network is made by handing over calls at a point in the network close to the subscriber. Any charges to end-users for use of the above-mentioned services and facilities are subject to ex post regulation in accordance with section 38(2) to (4).

(2) Obligations according to subsection (1) should be imposed on other SMP undertakings only when the regulatory aims set out in section 2(2) would not otherwise be achieved. Provided there is sustainable services competition in the retail mobile market, the obligations according to subsection (1) should not be imposed for the mobile market. Sustainable services competition in

32

the retail mobile market is fair competition between services supplied by public mobile network operators and publicly available services supplied by mobile service providers at the retail level;

such fair competition presupposes that providers of publicly available mobile services who are independent of public mobile network operators contribute to a sustainable competitive retail mobile market by means of services based also on wholesale products from the public mobile network operators.

Section 41

Set of Leased Lines

(1) The Regulatory Authority shall require undertakings having significant market power in the provision of part or all of the set of leased lines to provide the minimum set of leased lines as identified in the applicable list of standards drawn up by the Commission on the basis of Article 17 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33).

(2) Such undertakings have to publish conditions 3.1. to 3.3. as set out in Annex VII to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51). If necessary, the Regulatory Authority may set targets in respect of the supply conditions referred to in condition 3.3.

(3) Sections 27 to 39 apply with regard to rates regulation. The provisions on access regulation laid down in sections 16 to 26 remain unaffected.

C h a p t e r 5

S p e c i a l C o n t r o l o f A n t i - C o m p e t i t i v e P r a c t i c e s

Section 42

Anti-Competitive Conduct by an SMP Undertaking

(1) No SMP provider of telecommunications services, of services according to section 78(2) paras 3 and 4 or of telecommunications-based services and no SMP public telecommunications network operator may abuse his position. Abuse is constituted, in particular, by conduct consisting in, directly or indirectly, unreasonably obstructing other undertakings or materially affecting their competitive opportunities without objectively justifiable reason.

(2) Abuse within the meaning of subsection (1) is presumed where an SMP undertaking gives itself, its subsidiaries or partners access to services or facilities it uses internally or offers in the marketplace on more favourable conditions or of a better quality than it applies to other undertakings using the service or facility to provide their own telecommunications or related services, unless the undertaking provides evidence of facts objectively justifying the grant of less favourable conditions.

(3) Abuse within the meaning of subsection (1) is also presumed where an SMP public telecommunications network operator fails to comply with an obligation imposed on him under section 22(1) by delaying the processing of access applications without objective reason.

33

(4) The Regulatory Authority shall take a decision to end the abuse of significant market power upon application or on its own initiative. For this purpose it may, in relation to an undertaking abusing its position of significant market power, impose or prohibit certain practices and declare agreements wholly or partially invalid. Such decision shall generally be taken within a time limit of four months from the commencement of proceedings. Where an application as referred to in sentence 1 is made, the time limit begins running when the application is received. An application as referred to in sentence 1 may be made by any telecommunications service provider who can assert that his rights have been prejudiced.

Section 43

Surrender of Gain to the Regulatory Authority

(1) Where an undertaking has infringed a Regulatory Authority order according to section 42(4) or intentionally or negligently infringed a provision of this Act and thereby obtained economic gain, the Regulatory Authority should order surrender of the economic gain and impose on the undertaking payment of a corresponding sum of money.

(2) Subsection (1) does not apply where such economic gain has been cancelled out by payment of damages or by the imposition or order of forfeiture. Any undertaking paying damages as referred to in sentence 1 only after the surrender of gain is to be reimbursed with the sum of money up to the level of payments proven.

(3) Where enforcing surrender of gain would result in undue hardship, the order should be limited to a reasonable sum of money or be waived entirely. It should also be waived if the economic gain is insignificant.

(4) The level of economic gain may be estimated. The sum of money to be transferred is to be stated in figures.

(5) Surrender of gain may be ordered only within a period of five years of cessation of the infringement and for a maximum period of five years.

PART 3

CUSTOMER PROTECTION

Section 44

Right to Damages and Injunctive Relief

(1) Any undertaking infringing this Act, an ordinance having the force of law issued under this Act, an obligation imposed under this Act in an assignment, or an administrative order of the Regulatory Authority shall be obliged, in relation to the person affected, to eliminate the harmful practice and, where there is danger of further harmful practices, to cease and desist. Such right exists as soon as there is danger of an offence. A person affected is any consumer or competitor harmed by the infringement. Any undertaking to which intent or negligence can be imputed shall also be liable, in relation to a consumer or competitor, to reparation of any damage caused by the infringement. The undertaking has to pay interest on financial debts according to sentence 4 from such time as the damage occurred. Sections 288 and 289 sentence 1 of the Civil Code

apply accordingly.

34

(2) Any person infringing, in a manner other than by using or recommending general terms and conditions, provisions of this Act or provisions of an ordinance having the force of law issued under this Act whose purpose is to protect the consumer, may, in the interest of consumer protection, be required to cease and desist by the bodies named in section 3 of the Injunctions Act. Where offences in a business are committed by an employee or an agent, the right to injunctive relief also applies in relation to the owner of the business. The Injunctions Act remains unaffected in all other respects.

Section 45

Customer Protection Ordinance

(1) The Federal Government shall be empowered, for the special protection of end-users (customers), consumers in particular, to issue, by ordinance having the force of law and requiring the consent of the German Bundestag and the German Bundesrat, framework provisions for using telecommunications services and for ensuring metering and billing accuracy. Particular account is to be taken in doing so of the interests of persons with disabilities. The ordinance shall detail the powers of the Regulatory Authority. Account is to be taken most notably of Articles 21 and 22 of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51).

(2) The ordinance may, in particular, make arrangements about the conclusion, the subject matter and the termination of contracts and the rights and obligations of the contracting parties and of the other parties engaged in telecommunications traffic, including the information requirements according to Annex II to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51). The ordinance may also stipulate that particular measurement methods be applied in relation to quality of service and that undertakings' general terms and conditions include details of delivery periods and quality of service.

(3) Detailed arrangements, in particular, are to be made in the ordinance with regard to

1. the liability of undertakings;
2. the way in which reference is made to general terms and conditions and to rates and the possibility of their inclusion;
3. information requirements and regulations applicable in the event of non-compliance with these requirements;
4. requirements deriving from Annex I Part A to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108

page 51) to be met by undertakings in order that their customers can monitor and control their expenditure;

5. entries in directories and directory enquiry service databases;

6. out-of-court dispute resolution procedures for customers; and

35

7. declarations from property owners.

Section 46

Number Portability, European Telephone Numbering Space

(1) Public telephone network operators shall make provision in their networks to enable subscribers to retain their telephone number, independently of the undertaking providing the telephone service, as follows–

1. in the case of geographic numbers, at a specific location; and

2. in the case of non-geographic numbers, at any location.

The arrangement in sentence 1 applies only within the numbering ranges and subranges designated for a telephone service. In particular, the porting of telephone numbers for telephone services provided at a fixed location to those not provided at a fixed location and vice versa is not permitted.

(2) Providers of publicly available telecommunications services shall ensure that their endusers can retain in conformity with subsection (1) telephone numbers allocated to them when changing to another provider of publicly available telecommunications services.

(3) Subscribers may be charged solely the one-time costs incurred for changing provider. The same applies to costs charged by a network operator to a provider of publicly available telecommunications services. All such rates are subject to ex post regulation as provided for by section 38(2) to (4).

(4) Public telephone network operators have to make provision in their networks for handling all calls to the European telephone numbering space.

Section 47

Provision of Subscriber Data

(1) Every undertaking providing publicly available telecommunications services and assigning telephone numbers to end-users shall be obliged, in observance of the requirements of the relevant data protection legislation, to provide, upon request, any other undertaking with subscriber data as referred to in subsection (2) sentence 4 for the purpose of providing publicly available directory enquiry services and directories. Such data has to be provided without undue delay and in non-discriminatory manner.

(2) Subscriber data are such data as are published in directories of subscribers in accordance with section 104. Besides the number this includes the actual data for publication, ie the subscriber's name and address and any additional information known to the undertaking such as occupation, branch, type of line and co-users. It also includes such information, links,

assignments and classifications, processed and presented in line with the state of the art, in observance of the requirements of the relevant data protection legislation and in appropriate form for the customer's use, as are required for the publication of such data in publicly available directory enquiry services and directories according to sentence 1. The data shall be complete and their content and technical form processed and presented in such manner as to allow, under 36
the state of the art, easy inclusion in a customer-friendly directory or corresponding directory enquiry service database.

(3) In the event of disputes arising between undertakings concerning rights and obligations under subsections (1) and (2), section 133 applies accordingly.

(4) For the provision of subscriber data charges may be levied; such charges will typically be subject to ex post regulation as provided for by section 38(2) to (4). Such charges should be subject to approval under section 31 only when the undertaking has significant market power in the market for retail services.

PART 4

BROADCASTING

Section 48

Interoperability of Television Sets

(1) Every analogue television set with an integral viewing screen of visible diagonal greater than 42 centimetres offered for sale, rent or otherwise made available shall be fitted with at least one interface socket standardised by a recognised European standardisation body, permitting the connection of digital television receivers.

(2) Every digital television receiver offered for sale, rent or otherwise made available shall,

1. if it has an integral viewing screen of visible diagonal greater than 30 centimetres, be fitted with at least one interface socket, standardised by a recognised European standardisation body or conforming to a common, industry-wide, open specification, permitting the connection of digital television receivers and the possibility of conditional access;
2. if it is fitted with an application programming interface, fulfil the minimum requirements of such interface as adopted by a recognised European standardisation body or conforming to a common, industry-wide, open interface specification, enabling third parties to produce and operate their own applications irrespective of the transmission mode.

(3) Every digital television receiver offered for sale, rent or otherwise made available and intended for conditional access shall be capable of displaying signals

1. conforming to the common European scrambling algorithm as administered by a recognised European standardisation body;
2. that do not require conditional access. With regard to rented equipment this applies only inasfar as the rentee is in compliance with the relevant rental agreement.

Section 49

Interoperability of Digital Television Signal Transmissions

(1) Public telecommunications network operators transmitting digital television signals shall retransmit all such signals as are transmitted for representation wholly or partially in the 16:9 screen format, in this format.

37

(2) Rights holders of application programming interfaces are obliged to provide, on fair, reasonable and non-discriminatory terms and against appropriate remuneration, manufacturers of digital television receivers and third parties claiming a legitimate interest with all such information as is necessary to provide all the services supported by the application programming interface in fully functional form. The criteria referred to in sections 28 and 42 apply.

(3) In the event of a dispute arising between the parties concerned with regard to compliance with the provisions of subsections (1) to (2), either of the parties concerned may refer the matter to the Regulatory Authority. The Regulatory Authority shall take a decision, after hearing the parties concerned, within a period of two months. In proceeding, the Regulatory Authority shall give the authority responsible under state law the opportunity to comment. Where the authority responsible under state law raises objections to do with media legislation, it shall take a decision on the matter within the specified period. The two decisions may be taken in combined proceedings.

(4) Parties concerned shall comply with an order issued by the Regulatory Authority under subsection (3) without undue delay, except where the Regulatory Authority has stipulated a different period. To enforce such order, the Regulatory Authority may set a penalty not exceeding 500,000 euros in accordance with the Administrative Enforcement Act.

Section 50

Conditional Access Systems

(1) Providers of conditional access systems shall ensure that these have the necessary technical capability for the cost-effective transfer of control functions, allowing the possibility for full control by public telecommunications network operators at local or regional level of the services using such conditional access systems.

(2) Holders of industrial property rights to conditional access systems deciding to grant licences to manufacturers of digital television receivers or to third parties demonstrating a legitimate interest shall do so on fair, reasonable and non-discriminatory terms. The criteria referred to in sections 28 and 42 apply. Holders of such rights may take reasonable account of technical and commercial factors. However, licence grant may not be made subject to conditions hindering the installation of

1. a common interface allowing connection with other conditional access systems; or
2. components specific to another conditional access system, for reasons of transaction security with regard to the content to be protected.

(3) Providers and users of conditional access systems shall

1. enable all broadcasters to use the technical services they need to use their systems and to obtain the information they require on fair, reasonable and non-discriminatory terms;
2. where they are also responsible for billing end-users, give the end-user a tariff schedule prior to concluding with him a contract under which charges will be incurred;
3. keep separate accounts for their business as conditional access system providers;
38
4. prior to beginning to provide service and to providing service with differences, notify the Regulatory Authority of the details referred to in paras 1 to 3, the individual services offered to end-users and the rates charged.

(4) The Regulatory Authority shall inform, without undue delay, the authority responsible under state law of notifications according to subsection (3) para 4. Where the Regulatory Authority or the authority responsible under state law, each for its own area of responsibility, concludes on the basis of the notification within a period of two months that the service offer fails to comply with the requirements specified in subsection (3) paras 1 to 4, they shall require the service offer to be modified. Where the requirements cannot be satisfied despite the modifications or where the modifications have not been made despite the request, they shall prohibit the service offer.

(5) Where one or more providers or users of conditional access systems do not have significant market power, the Regulatory Authority may amend or withdraw conditions according to subsections (1) to (3) with respect to the party or parties concerned, provided that
1. the prospects for effective competition in the retail markets for the transmission of broadcasting signals and for conditional access systems and other associated facilities would not be adversely affected by such amendment or withdrawal; and
2. the authority responsible under state law has established that capacity determinations and must-carry obligations set out in state law would not be adversely affected by such amendment or withdrawal.

Sections 11 to 14(1) apply accordingly to the procedure referred to in sentence 1. Decisions as referred to in sentence 1 shall be reviewed by the Regulatory Authority every two years.

Section 51

Dispute Resolution

(1) Persons with entitlements or obligations under the provisions of this Part may jointly refer to the Dispute Resolution Panel for resolution any contentious issues concerning the application of these provisions. Such referral shall be in written form. The Regulatory Authority shall take a decision within a period of two months.

(2) The Dispute Resolution Panel shall be established at the Regulatory Authority. It shall comprise a Chairman and two Assessors. The Regulatory Authority shall be responsible for establishing the Dispute Resolution Panel, appointing its members and adopting its rules of procedure. The establishment and composition of the Dispute Resolution Panel and its rules of

procedure are to be published by the Regulatory Authority.

(3) In proceeding, the Dispute Resolution Panel shall give the authority responsible under state law the opportunity to comment. Where the authority responsible under state law raises objections to do with media legislation, it shall take a decision on the matter within the specified period. The two decisions may be taken in combined proceedings.

39

PART 5

GRANT OF FREQUENCIES, NUMBERS AND RIGHTS OF WAY

C h a p t e r 1

F r e q u e n c y R e g u l a t i o n

Section 52

Functions

(1) In order to secure efficient and interference-free use of frequencies and in consideration of the further aims set out in section 2(2), a National Table of Frequency Allocations and a Frequency Usage Plan shall be drawn up, frequencies assigned and frequency usages supervised.

(2) The Regulatory Authority shall issue orders with regard to the use of frequencies for the operation of radio equipment in foreign vehicles, watercraft and aircraft operating within the area of application of this Act.

(3) With regard to the use of frequencies within the area of responsibility of the Federal Ministry of Defence, the Federal Ministry of Economics and Labour shall reach agreement with the Federal Ministry of Defence.

Section 53

Frequency Band Allocation

(1) The Federal Government is empowered, by ordinance having the force of law but not requiring the consent of the German Bundesrat, to stipulate frequency band allocation for the Federal Republic of Germany in a National Table of Frequency Allocations and to amend such Table. Ordinances in which frequencies are allocated to broadcasting require the consent of the German Bundesrat. To be included in their preparation shall be all persons likely to be affected by the allocations.

(2) The National Table of Frequency Allocations allocates frequency bands to radio services and other applications of electromagnetic waves. Insofar as is necessary to secure efficient and interference-free use of frequencies, the Table also includes provisions on the use of frequencies and associated detailed determinations. Sentence 2 also applies to the use of frequencies in and along conductors; for the frequency bands concerned, geographic, time-related and technical determinations are to be made, compliance with which allows free use.

Section 54

Frequency Usage Plan

(1) The Regulatory Authority shall draw up the Frequency Usage Plan on the basis of the National Table of Frequency Allocations in consideration of the aims set out in section 2(2), European harmonisation, technological advance and the compatibility of frequency usages in the transmission media.

40

(2) The Frequency Usage Plan shall include further allocation of the frequency bands to frequency usages, and determinations on such usages. The Frequency Usage Plan may consist of subplans.

(3) The Frequency Usage Plan shall be drawn up with the participation of the public. The Federal Government is empowered to lay down, by ordinance having the force of law and requiring the consent of the German Bundesrat, the procedure for drawing up the Frequency Usage Plan.

Section 55

Frequency Assignment

(1) Each frequency usage requires prior frequency assignment, unless otherwise provided for by this Act. Frequency assignment means authorisation given by a public authority or by legal provisions to use particular frequencies under specified conditions. Frequencies are assigned for a particular purpose in accordance with the Frequency Usage Plan and in non-discriminatory manner on the basis of transparent and objective procedures. Assignment is not required where usage rights may be exercised by virtue of another statutory regulation. Where it is necessary for public authorities, in order to exercise legal powers, to use frequencies already assigned to other persons and significant interference to these usages is not anticipated as a result of doing so, this usage shall be permitted, subject to the framework conditions established in consultation with the law enforcement agencies, without an assignment being required.

(2) Frequencies are typically assigned ex officio by the Regulatory Authority as general assignments for the use of particular frequencies by the general public or a group of persons defined or capable of being defined by general characteristics. Such assignments are published.

(3) Where general assignment is not possible, frequencies for particular usages are assigned by the Regulatory Authority to natural persons, legal entities and associations of persons, insofar as they may be eligible, upon written application, as individual assignments. This applies in particular when the risk of harmful interference cannot otherwise be ruled out or when this is necessary in order to secure efficient use of frequencies.

(4) The application referred to in subsection (3) has to specify the area in which the frequencies are to be used. The applicant has to show that the subjective requirements for frequency assignment with regard to efficient and interference-free use of frequencies and other conditions as specified in Part B of the Annex to Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic

communications networks and services (Authorisation Directive) (OJ L 108 page 21) are satisfied. The Regulatory Authority shall take a decision on complete applications within a period of six weeks. This time limit shall not affect existing international agreements on the use of radio frequencies and orbit positions.

(5) Frequencies shall be assigned subject to

1. their designation for the planned usage in the Frequency Usage Plan;

2. their availability;

3. their compatibility with other frequency usages; and

41

4. their efficient and interference-free use by the applicant being secured.

Applicants are not entitled to any one particular frequency.

(6) The Regulatory Authority is to be notified without undue delay of the beginning and the cessation of usage. It shall also be notified of any change of name, change of address, change in ownership structure and any identity-preserving transformations.

(7) Applications for a change in the frequency assignment are to be submitted without undue delay to the Regulatory Authority, in writing, with supporting documents, when

1. frequency usage rights are to be transferred by singular or universal succession;

2. frequencies are to be transferred to an affiliated undertaking as defined in section 15 of the Stock Corporation Act;

3. frequencies are to be transferred from a natural person to a legal entity in which the natural person holds a share; or

4. an heir intends to continue using the frequencies.

In these cases, the frequencies may continue to be used until such time as a decision is taken on the application for a change in the assignment. The application shall be granted when the requirements for frequency assignment according to subsection (4) are satisfied, distortion of competition in the relevant product and geographic market is not to be feared and the efficient and interference-free use of frequencies is secured. Any frequencies no longer used are to be returned without undue delay by means of a written declaration. Where a legal entity that has been assigned frequencies is liquidated without there being a legal successor, the frequencies shall be returned by the liquidator. Where a natural person dies without an heir intending to continue using the frequencies, these shall be returned by the heir or by the estate administrator.

(8) Frequencies are typically assigned for a limited period, with the possibility of extension. The time limit shall be appropriate to the service concerned.

(9) Where frequencies are not available for assignment in sufficient numbers or where more than one application has been made for particular frequencies the Regulatory Authority may order, without prejudice to subsection (5), that assignment be preceded by award proceedings based on conditions according to section 61 as determined by the Regulatory Authority. Persons

likely to be affected are to be heard prior to such decision. The Regulatory Authority's decision is to be published.

(10) A frequency assignment may be denied in full or in part where the use intended by the applicant is incompatible with the regulatory aims according to section 2(2). Where the interests of the federal states relating to broadcasting within their jurisdiction are concerned, consultation is to be held with the state authority with competence, based on the broadcasting regulations.

42

Section 56

Orbit Positions and Frequency Usage by Satellites

(1) All exercise of German rights to orbit and frequency usage shall require, in addition to frequency assignment according to section 55(1), assignment of such rights by the Regulatory Authority. The Regulatory Authority shall, upon application, perform the advance publication, coordination and notification of satellite systems with the International Telecommunication Union and assign to the applicant the resulting rights to orbit and frequency usage. The preconditions for this are as follows–

1. the availability of frequencies and orbit positions;
2. compatibility with other frequency usages and other satellite system notifications;
3. no detriment to public interest.

(2) With regard to existing German entries in the Plan and other unused rights to orbit and frequency usage with the International Telecommunication Union, award proceedings may be conducted based on conditions as determined by the Regulatory Authority.

(3) Assignment may be revoked where such rights have not been exercised for more than one year or where the preconditions of subsection (1) sentence 3 are no longer given.

Section 57

Special Preconditions for Frequency Assignment

(1) The assignment of frequencies for broadcasting within the jurisdiction of the federal states requires, in addition to the preconditions of section 55, consultation with the state authority with competence, based on the broadcasting regulations. The relevant state authority notifies the Regulatory Authority of the coverage requirements for broadcasting within the jurisdiction of the federal states. The Regulatory Authority shall satisfy these notified requirements in assigning frequencies under section 55. Details of the procedure shall be laid down by the Regulatory Authority on the basis of the broadcasting regulations of the state authorities with competence. Frequencies allocated to the broadcasting service in the National Table of Frequency Allocations and designated in the Frequency Usage Plan may be used for purposes other than broadcasting within the jurisdiction of the federal states where the capacity allocated to broadcasting on the basis of the broadcasting regulations is available. For this purpose the Regulatory Authority shall bring about consultation with the state authorities with competence.

(2) Frequency usages of the Federal Ministry of Defence in the bands designated in the Frequency Usage Plan exclusively for military purposes shall not require assignment.
(3) Frequencies designated in the Frequency Usage Plan for maritime shipping, inland waterways shipping and the aeronautical service and used for such purposes on foreign watercraft or aircraft operating within the area of application of this Act shall be deemed assigned.
(4) With regard to frequencies designated in the Frequency Usage Plan for public safety radiocommunications, the Federal Ministry of the Interior shall, in consultation with the supreme state authorities responsible, determine in a directive the following matters–
43
1. the responsibilities of the authorities concerned;
2. the procedure for being recognised as qualified to participate in public safety radiocommunications;
3. the procedure for processing applications for the assignment of frequencies for public safety radiocommunications purposes and the responsibilities in this regard;
4. the principles of frequency planning and the procedures for frequency coordination for public safety radiocommunications purposes; and
5. the arrangements for radio operations for and cooperation between and among the authorities and organisations using frequencies for public safety radiocommunications purposes.
The directive is to be drawn up in agreement with the Regulatory Authority, in particular as far as paras 4 and 5 are concerned. The Federal Ministry of the Interior shall confirm in each instance, after hearing the supreme federal or state authorities responsible for the matter, that an applicant is one of the group recognised as qualified according to sentence 1.
(5) Frequencies for use by aeronautical stations in the aeronautical mobile service and aeronautical radionavigation land stations shall be assigned only when consent to install and operate such stations as required by section 81(1) and (2) of the Air Traffic Licensing Ordinance has been given.
(6) Frequencies for use by coast stations in the port operations service shall be assigned only when the consent of the waterways and shipping administration is to hand.
Section 58
Variant Frequency Usages
In justified particular cases, notably to test innovative technologies in telecommunications or to provide frequencies required at short notice, frequency assignments which are at variance with the determinations of the National Table of Frequency Allocations or the Frequency Usage Plan may be granted on a temporary basis, on condition that no degradation is caused to any frequency usage entered in the National Table of Frequency Allocations or the Frequency Usage Plan. No such variance may interfere with the further development of the Tables or Plans.

Where the interests of the federal states relating to broadcasting within their jurisdiction are concerned, consultation is to be held with the state authority with competence, based on the broadcasting regulations.

Section 59

Shared Use

Frequencies whose use by one party alone is not expected to be efficient may be assigned to more than one party for shared use. Such assignees shall tolerate any degradation arising from shared use of the frequency for the intended purpose.

44

Section 60

Constituent Parts of Frequency Assignment

(1) The frequency assignment is to specify, in particular, the type and extent of the frequency usage, insofar as is necessary to secure efficient and interference-free use of frequencies. Use of assigned frequencies may be made solely with radio equipment intended or marked for operation in the Federal Republic of Germany.

(2) In order to secure efficient and interference-free use of frequencies, secondary conditions may be attached to the frequency assignment. Where, after assignment, it is established that usage is being significantly restricted on account of increased use of the radio spectrum or that considerable efficiency gains are possible on account of technological advance, the type and extent of the frequency usage referred to in subsection (1) may be subsequently modified. Where the interests of the federal states relating to broadcasting within their jurisdiction are concerned, consultation is to be held with the state authority with competence, based on the broadcasting regulations.

(3) The frequency assignment should contain references to the parameters for the receiving equipment on which the Regulatory Authority has based its specifications on the type and extent of the frequency usage. The Regulatory Authority takes no measures of any kind to counteract detrimental effects resulting from non-compliance with the parameters notified.

(4) Frequencies for broadcasting within the jurisdiction of the federal states shall be assigned, in consultation with the state authority with competence, subject to conditions ensuring that the broadcasting interests of the federal states are taken into account.

Section 61

Award Proceedings

(1) Where an order has been issued under section 55(9) requiring frequency assignment to be preceded by award proceedings, the Regulatory Authority may, after hearing the parties concerned, conduct an auction in accordance with subsection (5) or invite tenders in accordance with subsection (6). Decisions on the choice of proceedings and the determinations and rules for the conduct of proceedings are to be published by the Regulatory Authority. Frequency assignment shall be effected in accordance with section 55 following completion of the award

proceedings referred to in sentence 1.

(2) As a general rule, the proceedings laid down in subsection (5) are to be conducted, except where such proceedings are not likely to secure the regulatory aims according to section 2(2). This may be the case, in particular, when frequencies have already been assigned, without a prior auction, in the relevant product and geographic market for which the radio frequencies may be used in observance of the Frequency Usage Plan, or where an applicant can claim a legal right to preference for the frequencies to be assigned. The proceedings laid down in subsection (5) are not applicable in respect of frequencies intended for broadcasting services.

(3) An applicant may be excluded from participation in award proceedings where a successful bid according to subsection (5) by him or a successful tender according to subsection (6) from him is expected to prejudice fair competition in the relevant product and geographic market for which the radio frequencies to be assigned may be used in observance of

45

the Frequency Usage Plan. Any such decision shall take due account of the legitimate interests of the particular applicant in the deployment of new technologies.

(4) The aim of award proceedings is to determine which of the applicants is or are best placed to make efficient use of the frequencies to be assigned. Prior to carrying out award proceedings, the Regulatory Authority shall determine the following matters–

1. the minimum specialist and other requirements to be met by applicants in order to qualify for the award proceedings;

2. the relevant product and geographic market for which the frequencies to be assigned may be used in observance of the Frequency Usage Plan;

3. the basic spectrum package required for commencement of the telecommunications service, where necessary;

4. the frequency usage conditions, including the degree of coverage with the frequency usage and the time required to achieve such degree.

(5) In the case of an auction, the Regulatory Authority shall, prior to the award proceedings, detail the rules for conducting auctions; such rules shall be objective, transparent and nondiscriminatory and have regard to the interests of small and medium-sized enterprises. The Regulatory Authority may stipulate a minimum bid for participation in the auction.

(6) In the case of tendering, the Regulatory Authority shall, prior to the award proceedings, determine the criteria against which tenderers' eligibility will be assessed. Such criteria are the tenderers' specialist knowledge and efficiency, the suitability of their plans for providing the telecommunications service for which the tender has been invited, and the promotion of sustainable competition in the market. Preference is to be given in the selection procedure to tenderers ensuring a higher degree of coverage with the particular telecommunications services. The Regulatory Authority shall also detail the rules for tendering; such rules shall be objective,

transparent and non-discriminatory. Where the outcome of tendering shows several tenderers to be equally well placed, the decision shall be made by drawing lots.

(7) Any commitments entered into by bidders in the course of an auction or by tenderers in the course of tendering shall become constituent parts of the frequency assignment.

(8) In the case of an auction according to subsection (5) or tendering according to subsection (6), the maximum period of six weeks referred to in section 55(4) may be extended by as long as necessary, but by no more than eight months, however, in order to ensure a fair, reasonable, open, and transparent procedure for all concerned. Such time limits shall be without prejudice to existing international agreements on spectrum use and satellite coordination.

Section 62

Spectrum Trading

(1) The Regulatory Authority may, after hearing the parties concerned, release frequency bands for trading and stipulate the framework conditions of and the procedure for trading when there is interest in trading usage rights for the spectrum concerned. The procedure shall include termination of the frequency assignment and the issue of a new assignment.

46

(2) The framework conditions of and the procedure for trading shall ensure, in particular, that

1. spectrum efficiency is increased or maintained;
2. the original award proceedings do not preclude frequency assignment after spectrum trading;
3. no distortion of competition in the relevant product and geographic market is to be feared;
4. other legal framework conditions, in particular the conditions of use and international agreements on spectrum use, are complied with; and
5. the regulatory aims according to section 2(2) are secured.

Decisions on the framework conditions of and the procedure for spectrum trading are to be published. With regard to frequencies intended for the broadcasting services, decisions shall be taken in agreement with the authority responsible under state law.

(3) Proceeds from spectrum trading, less the administrative costs incurred, are due to the party selling the usage rights.

Section 63

Revocation of Frequency Assignment, Relinquishment

(1) A frequency assignment may be revoked where use of the assigned frequency for the intended purpose has not commenced within one year of the assignment or where the frequency has not been used for the intended purpose for more than one year.

(2) The frequency assignment may also be revoked, apart from in the cases specified in section 49(2) of the Administrative Procedures Act, where

1. one of the preconditions according to section 55(5) and section 57(4) to (6) is no longer given;

2. an obligation arising from the assignment is repeatedly violated or has not been fulfilled despite repeated requests for fulfilment;
3. competition or the introduction of new spectrum-efficient technologies is prevented or unreasonably hindered as a result of a scarcity of frequencies which arises after the assignment; or
4. distortion of competition in the relevant product and geographic market is to be feared as a result of a change in ownership structure in the person of the assignee.
The period of time until revocation becomes effective shall be appropriate. Where frequencies for broadcasting within the jurisdiction of the federal states are concerned, the Regulatory Authority shall consult the state authority with competence, on the basis of the broadcasting regulations.
(3) The frequency assignment should be revoked where, in respect of a frequency assigned for broadcasting within the jurisdiction of the federal states, all the broadcasting regulations from 47
the state authority with competence concerning transmissions on the given frequency have ceased to apply. In place of the revocation according to sentence 1, the Regulatory Authority may, when, in respect of a frequency according to sentence 1, one or all of the broadcasting regulations according to sentence 1 has or have ceased to apply and no new broadcasting regulation has been issued within a period of six months, assign, in accordance with the Frequency Usage Plan, in consultation with the state authority with competence, such frequency to the previous assignee – possibly even in derogation of the previous award proceedings – with a limited obligation or with no obligation to use it for broadcasting within the jurisdiction of the federal states.
(4) Section 49(6) of the Administrative Procedures Act is not applicable to revocation according to subsections (2) and (3).
(5) The Regulatory Authority should revoke frequency assignments for analogue broadcast transmissions on the basis of the broadcasting regulations of the state authority with competence, in accordance with the Frequency Usage Plan, not later than 2010 for television broadcasting and not later than 2015 for VHF sound broadcasting. Sound broadcast transmissions in the low, medium and high frequency bands remain unaffected. The frequency assignment shall expire after an appropriate period of time as specified in the revocation but in no case of less than one year.
(6) The frequency assignment shall expire upon relinquishment. Relinquishment is to be declared to the Regulatory Authority in writing, with the exact designation of the frequency assignment being stated.
Section 64
Monitoring, Orders to Take Equipment Out of Service
(1) The Regulatory Authority shall monitor frequency usage in order to secure the aims of

frequency regulation. Insofar as is necessary and reasonable for this purpose, most notably to identify a particular frequency user, Regulatory Authority staff are authorised to obtain information on the detailed circumstances of a telecommunications activity and also, in special cases, to listen in to emissions. Information obtained as a result of the measures referred to in sentence 2 may be used solely for the purpose of securing the aims of frequency regulation. In derogation of this, information may be transmitted to the authorities responsible where this is necessary to prosecute a criminal offence as set out in section 100a of the Code of Criminal Procedure. The basic right of privacy of telecommunications laid down in Article 10 of the Basic Law shall be restricted in accordance with sentences 2 to 4.

(2) The Regulatory Authority may, to secure the aims of frequency regulation, order that equipment be operated with restrictions or be taken out of service. To enforce such administrative orders, a penalty not exceeding 500,000 euros may be set in accordance with the Administrative Enforcement Act.

Section 65

Restrictions on Frequency Assignments

Use of assigned frequencies may be restricted on a temporary basis where such frequencies are required by the authorities responsible to perform their duties in a state of tension or defence, in connection with alliance commitments, in connection with cooperation with the

United Nations, in connection with international emergency management or in the event of a natural disaster or a particularly serious accident.

C h a p t e r 2

Numbering

Section 66

Numbering

(1) The Regulatory Authority shall discharge numbering functions. It shall be responsible, in particular, for structuring and configuring the numbering space with the aim of satisfying the requirements of end-users, telecommunications network operators and telecommunications service providers. The Regulatory Authority shall also allocate numbers to telecommunications network operators, telecommunications service providers and end-users. Not included in its responsibilities is the administration of the country code top level and lower level domains.

(2) In order to implement international obligations and recommendations and to ensure sufficient availability of numbers, the Regulatory Authority may modify the structure and configuration of the numbering space and the national numbering plan. In doing so, it shall take reasonable account of the interests of the parties concerned, most notably of the conversion costs incurred by operators, telecommunications service providers and users. Proposed modifications are to be made known in good time prior to becoming effective. Telecommunications network operators and telecommunications service providers affected by

such modifications are required to take all implementation measures necessary.
(3) The Regulatory Authority may issue orders to enforce the obligations referred to in subsection (2). To enforce such orders, a penalty not exceeding 500,000 euros may be set in accordance with the Administrative Enforcement Act.
(4) The Federal Government shall be empowered to lay down, by ordinance having the force of law and requiring the consent of the German Bundestag and the German Bundesrat, the criteria and guidelines for the structuring, configuration and administration of numbering space, for the acquisition, the extent and the loss of rights to use numbers including the requirements for telecommunications-based services, and to transpose international recommendations and obligations into national legislation. In doing so it shall take account, in particular, of an efficient use of numbers, the interests of the market players including their interest in a sound basis for planning, the economic implications for the market participants, the requirements in respect of the use of numbers and of meeting demand in the long term, and the interests of the end-users. The powers of the Regulatory Authority and the rights and obligations of the market participants and of the end-users are to be detailed in the ordinance. Subsection (1) sentence 4 applies accordingly.

Section 67

Powers of the Regulatory Authority

(1) The Regulatory Authority may, under its responsibility for numbering administration, issue orders and take any other suitable measures to secure compliance with the legal provisions and with the conditions it has imposed in connection with the allocation of numbers. In particular, the Regulatory Authority may, where statutory obligations or obligations imposed by public

49

authorities have not been fulfilled, withdraw the unlawfully used number. Further, where it has reliable information on the unlawful use of a telephone number, it should issue an order in relation to the operator of the network in which the number is activated to deactivate the telephone number. The Regulatory Authority may, where it has reliable information on unlawful use, request the bill-issuer not to issue bills for the number concerned. In justified exceptional cases the Regulatory Authority may prohibit certain categories of dialler; the Regulatory Authority shall lay down details of the procedure governing such prohibition.
(2) The rights of the federal states and the powers of other public authorities are not affected.
(3) The Regulatory Authority shall notify the public prosecutor or the administrative authority of any facts giving reason to suspect a criminal or an administrative offence.

C h a p t e r 3

R i g h t s o f W a y

Section 68

Principle of the Use of Public Ways

(1) The Federation shall have the power to use trafficways free of charge for

telecommunications lines serving public purposes, provided that their dedication as trafficways is not thereby restricted on a lasting basis (right of use). Trafficways shall include public ways, squares, bridges and public waters.

(2) Telecommunications lines are to be installed and maintained in such a way as to satisfy the requirements of public safety and order and to comply with the recognised rules of engineering.

(3) The installation of new and the modification of existing telecommunications lines shall require the written consent of the authorities responsible for the construction and maintenance of public ways. With regard to the installation of overhead lines the interests of the above authorities, of public telecommunications network operators and the requirements of town planning shall be weighed. Where installation can be coordinated under a comprehensive building project to be carried out close in time to the application for consent, lines should typically be installed underground. Consent may be given subject to secondary conditions which are to be framed in non-discriminatory manner; consent may also be made dependent on payment of a reasonable security. Such secondary conditions may make stipulations solely on the way in which a telecommunications line is to be installed, the rules of engineering to be observed in doing so, the safety and ease of traffic, the records, consistent with the local practices of the above authority, on the location of a telecommunications line by geographic coordinates, and traffic safety obligations.

(4) Where the authority responsible for the construction and maintenance of public ways is itself the operator of a telecommunications line or has merged within the meaning of section 37(1) or (2) of the Competition Act with an operator, consent according to subsection (3) is to be given by an administrative body which is independent of the administrative body responsible for operation of the telecommunications line or for the exercise of corporate rights, as the case may be.

50

Section 69

Transfer of Rights of Way

(1) The Federation shall, upon written application, transfer to public telecommunications network operators its rights of use according to section 68(1) through the Regulatory Authority.

(2) The area for which the right of use is to be transferred is to be named in the application referred to in subsection (1). The Regulatory Authority shall grant the right of use where the applicant has the proven specialist knowledge, reliability and efficiency to install telecommunications lines and the right of use is consistent with the regulatory aims set out in section 2(2). The Regulatory Authority shall grant the right of use for the duration of the public activity. The Regulatory Authority shall decide on complete applications within a period of six weeks.

(3) The beginning and cessation of use and any change of name, change of address or

identity-preserving transformations of the undertaking are to be notified without undue delay to the Regulatory Authority. The Regulatory Authority shall provide the authority responsible for the construction and maintenance of public ways with this information. The party enjoying the right of use shall be liable for any damage arising from changes not being notified in time.

Section 70

Shared Use

Insofar as it is not possible, or is possible only at disproportionately high expense, to exercise the right according to section 68 for the installation of further telecommunications lines, acquiescence in the shared use of other installations intended for the accommodation of telecommunications cables can be required where shared use is economically reasonable and no major additional construction work is needed. In this case the party enjoying the right of shared use shall pay adequate compensation in money's worth to the party obliged to grant shared use.

Section 71

Showing Consideration for Maintenance and Dedication

(1) With regard to the use of trafficways, any hindrance to their maintenance and any temporary restriction of their dedication as trafficways is to be avoided as far as possible.

(2) Where maintenance is hindered, the party enjoying the right of use is to reimburse the party liable for maintenance with the costs arising from such hindrance.

(3) After completion of work on the telecommunications lines, the party enjoying the right of use is to restore the trafficway without undue delay, provided the party liable for maintenance has not declared itself willing to undertake restoration itself. The party enjoying the right of use is to reimburse the party liable for maintenance with the expenses incurred for any restoration thus undertaken and to pay compensation for any damage incurred as a result of work on the telecommunications lines.

51

Section 72

Changes Required

(1) Where, following the installation of a telecommunications line, it emerges that the telecommunications line is restricting a trafficway's dedication as a trafficway more than temporarily or is preventing performance of the work required for its maintenance or is impeding the execution of any modification to the trafficway intended by the party liable for maintenance, the telecommunications line, to the extent necessary, is to be modified or removed.

(2) Where a trafficway is withdrawn, the right of use of the party enjoying such right shall lapse.

(3) In all such cases the party enjoying the right of use is to bring about the required measures in respect of the telecommunications line at its own expense.

Section 73

Protection of Trees

(1) Trees planted on and around trafficways are to be protected where possible and their growth allowed for. Lopping may be required only to the extent necessary to install the telecommunications line or to prevent interruption of service; it is to be limited to the degree that is absolutely necessary.

(2) The party enjoying the right of use is to set the tree owner an appropriate period within which to carry out lopping himself. Where lopping has not been carried out or has not been carried out sufficiently within the specified period, the party enjoying the right of use shall bring about lopping. It shall also be entitled to do so when it is a matter of urgently preventing or eliminating interference.

(3) The party enjoying the right of use shall pay compensation for all damage to trees and repay the costs of all lopping carried out at its request.

Section 74

Special Installations

(1) Telecommunications lines are to be configured in such a way that they do not adversely affect existing special installations (installations serving to maintain public ways, drains, water and gas pipelines, tracks, electrical installations and the like). The party enjoying the right of use is to bear the costs incurred for the implementation of any necessary protective measures.

(2) The relocation or modification of existing special installations may be requested only against compensation and only where the trafficway, otherwise, could not be used for the telecommunications line and the special installation can be placed elsewhere in suitable manner for its intended purpose.

(3) Even if these prerequisites are met, the trafficway shall not be used for the telecommunications line where the damage arising from relocation or modification of the special installation would be disproportionately high in relation to the costs the party enjoying the right of use would incur for use of any other trafficway available to it.

52

(4) Subsections (1) to (3) apply accordingly with regard to special installations in the preparatory stage whose construction lies in the public interest. Compensation by reason of subsection (2) shall be granted only up to the level of the expenses incurred in the preparations. Installations shall be deemed in a preparatory stage as soon as they have been approved by the client by virtue of the detailed plan of the installation, and, insofar as is necessary, by the competent authorities and by the owner or any other party enjoying the right of use of the way.

Section 75

Subsequent Special Installations

(1) Subsequent special installations are, where possible, to be configured in such a way that they do not adversely affect existing telecommunications lines.

(2) A request to relocate or modify a telecommunications line shall be complied with at the

expense of the party enjoying the right of use where a subsequent special installation, the construction of which, for reasons of public interest, in particular for economic or traffic considerations, is to be carried out by the party liable for the maintenance of public ways or with its majority participation, would otherwise not be able to be constructed or the construction of which would be significantly hindered. The relocation of a cable-based telecommunications line not used just for local, suburban or neighbouring area traffic may be required only when such cable-based telecommunications line can be placed elsewhere in suitable manner for its intended purpose without disproportionately high costs being incurred.

(3) Where, as a result of any such subsequent special installation, protective measures on an existing telecommunications line have to be carried out, the costs arising are to be borne by the party enjoying the right of use.

(4) Where a party liable for the maintenance of public ways transfers its share to a third party not liable for maintenance, the party enjoying the right of use is to be reimbursed with the costs incurred for the relocation or modification or for the implementation of protective measures, as far as these concern its share.

(5) Operators of special installations other than those referred to in subsection (2) shall bear the costs incurred for the relocation or modification of existing telecommunications lines or for the implementation of any protective measures required.

(6) With regard to any subsequent modification of existing special installations, subsections (1) to (5) apply accordingly.

Section 76

Detriment to Property

(1) The owner of a property that does not constitute a trafficway within the meaning of section 68(1) sentence 2 cannot prohibit the installation, operation or renewal of telecommunications lines on his property insofar as,

1. on his property, a line or installation that is secured by right is used also for the installation, operation or renewal of a telecommunications line and the usability of the property is not thereby additionally restricted on a lasting basis; or

53

2. the property is not, or is not significantly, affected by such use.

(2) A property owner having to acquiesce in actions according to subsection (1) may claim appropriate pecuniary compensation from the operator of the telecommunications line or the owner of the network if use of his property or the income from it is affected beyond reasonable measure by the installation, the renewal or by maintenance work, repair work or comparable measures directly connected with the operation of the telecommunications line. In addition, one-time pecuniary compensation for extended use for telecommunications purposes may be claimed, provided there were no lines hitherto that could be used for telecommunications purposes. In the event of damage to the property or its movables from exercise of the rights

ensuing from this provision, the operator or the owner of the network shall remove the damage at his expense. Section 840(1) of the Civil Code applies.

Section 77

Damage Claims

The limitation period for claims arising from sections 70 to 76 follows the arrangements on the normal limitation periods set out in the Civil Code.

PART 6

UNIVERSAL SERVICE

Section 78

Universal Services

(1) Universal services are a minimum set of publicly available services of specified quality to which every end-user, irrespective of his place of residence or work, shall have access at an affordable price and whose provision to the public as a basic service has become indispensable.

(2) The following have been determined as universal services–

1. connection at a fixed location to a public telephone network and access to publicly available telephone services at a fixed location including – subject to technical feasibility – the features call waiting, call forwarding and call hold/broker's call;
2. the availability of at least one printed public directory of subscribers (section 104) approved by the Regulatory Authority, which satisfies general requirements and is updated on a regular basis, once a year at least;
3. the availability, to users of public pay telephones as well, of at least one comprehensive public telephone directory enquiry service, including provision of the area codes of domestic subscribers and of subscribers in other countries, as far as the subscriber data are available and in observance of the requirements of the relevant data protection legislation;
4. provision throughout the Federal Republic of Germany, in accordance with general demand, of public pay telephones in general locations accessible to everyone at all times; public pay telephones are to be kept in working order; and

54

5. the possibility to make emergency calls from all public pay telephones free of charge and without the use of any means of payment by simple use of the number "112" and the national emergency call numbers determined in the ordinance as provided for under section 108(2) sentence 1 para 1.

(3) Undertakings providing the universal services referred to in subsection (2) paras 2 and 3 are to apply the principle of non-discrimination to the treatment of information provided to them by other undertakings.

(4) The Regulatory Authority may, after consulting the undertaking with universal service obligations (designated universal service provider), identify general demand for the universal services referred to in subsection (2) in terms of the needs of end-users with regard to, in

particular, geographical coverage, number of telephones, accessibility and quality of service. The Regulatory Authority has the power to impose obligations on undertakings in order to secure provision of the service and of service features. The Regulatory Authority may choose not to impose such obligations for all or part of its territory if it is satisfied, after consulting the interested parties, that these service features or comparable services are deemed widely available.

Section 79

Affordability

(1) The price for the universal service referred to in section 78(2) para 1 is deemed affordable if it does not exceed the real price of the telephone services required on average by a household situated outside a town or city with a population of more than 100,000 on 1 January 1998. The assessment of affordability takes into account the quality of service levels, including supply times, at that time and the rate of growth in productivity up to 31 December of the year prior to the previous one.

(2) The universal services referred to in section 78(2) paras 2 to 4 are deemed affordable if the rates comply with the criteria set out in section 28.

Section 80

Obligation to Provide Universal Service

Where a universal service as referred to in section 78 is not being adequately or appropriately provided by the market or where there is reason to fear that such provision will not be secured, each provider operating in the relevant product market and achieving, within the area of application of this Act, at least four percent of total sales in this market or having significant market power in the relevant geographic market shall be obliged to contribute to making possible provision of the universal service. An obligation as referred to in sentence 1 is to be fulfilled in accordance with the provisions of this Chapter.

Section 81

Imposition of Universal Service Obligations

(1) The Regulatory Authority shall publish its findings of any relevant product and geographic market or of any place in which a universal service as referred to in section 78(2) is not being adequately or appropriately provided or in which there is reason to fear that such provision will

55

not be secured. It shall announce its intention to proceed as provided for by sections 81 to 87, unless an undertaking declares itself willing, within a period of one month of the publication of notice, to provide such universal service without compensation according to section 82.

(2) The Regulatory Authority may, after consulting the undertakings likely to be concerned, decide whether, and to what extent, to oblige one or more of these undertakings to provide the universal service. Any such obligation may not unduly prejudice the undertakings thus designated in relation to the other undertakings.

(3) Where an undertaking that is to be obliged under subsection (2) to provide a universal service substantiates by prima facie evidence that, in the case of such obligation, it will be able to claim compensation according to section 82, the Regulatory Authority shall, instead of designating one or more undertakings, invite tenders for the universal service and award it to the applicant proving himself well placed to provide, and requiring the least financial compensation for providing, the universal service in compliance with the terms laid down in the provisions of this Act. The Regulatory Authority may, taking into account the criteria of sentence 1, designate different undertakings or groups of undertakings to provide different elements of the universal service or to cover different parts of the federal territory.

(4) Prior to inviting tenders for the universal service, the Regulatory Authority is to determine the criteria against which the eligibility of the universal service provider will be assessed. It is also to detail the rules for inviting tenders; such rules shall be objective, transparent and nondiscriminatory.

(5) Where a suitable applicant is not found by tendering, the Regulatory Authority shall oblige the undertaking identified under subsection (2) to provide the universal service in accordance with this Act.

Section 82

Compensation for Universal Service Provision

(1) Where an undertaking is obliged under section 81(3) to provide a universal service, the Regulatory Authority shall grant the financial compensation as recognised in the tendering procedure for the provision of such service.

(2) Where an undertaking is obliged under section 81(5) to provide a universal service, the Regulatory Authority shall determine the compensation payable for such provision by calculating the difference between the cost for a designated undertaking of operating without the universal service obligation and the cost of operating in observance of the obligation. Benefits and proceeds accruing to the universal service provider, including intangible benefits, are also to be taken into account.

(3) The Regulatory Authority shall determine whether the costs identified constitute an unfair burden. In such case the Regulatory Authority shall grant the undertaking, upon application, the financial compensation calculated.

(4) To calculate the amount of compensation, the Regulatory Authority may ask the designated universal service provider for the necessary documentation. The Regulatory Authority is to examine the documentation submitted in particular with a view to the need for service provision. The results of the cost calculation and of the examination are to be published,

56

the protection of trade and operating secrets of the undertakings concerned being taken into account.

(5) Compensation shall be paid after expiry of the calendar year in which a deficit in

providing the universal service was incurred.

Section 83

Universal Service Contributions

(1) Where the Regulatory Authority grants compensation according to section 82 for provision of a universal service, each undertaking obliged under section 80 to provide the universal service shall share, by means of a universal service contribution, in funding the compensation. The sharing mechanism is assessed on the basis of the proportion of the sales of the particular undertaking to the total sales of all those with obligations according to sentence 1 in the relevant product market. Where it is not possible to recover such contribution from an undertaking with liability to pay, the shortfall is to be made up for by the others with obligations on the basis of the proportion of their shares in relation to each other.

(2) After expiry of a calendar year for which compensation according to section 82 subsections (1) or (3) has been granted, the Regulatory Authority shall determine the level of compensation and the shares due from the contributing undertakings and communicate this to the undertakings concerned. The level of compensation is derived from the amount of compensation calculated by the Regulatory Authority plus interest at market rates. Interest is paid as from the day following the date of expiry of the calendar year referred to in sentence 1.

(3) All undertakings contributing in accordance with subsection (1) to compensation are required to pay to the Regulatory Authority the share falling to them as assessed by the Regulatory Authority within a period of one month of receiving the notice of assessment.

(4) Where an undertaking liable to pay compensation is more than three months in arrears with payment of its contribution, the Regulatory Authority shall issue a notice of arrears and enforce collection.

Section 84

Availability, Unbundling and Quality of Universal Services

(1) Where undertakings provide universal services, end-users shall, within the limits of the legislation and general terms and conditions, have a right to the provision of such services.

(2) Undertakings providing universal services are to offer universal services in such a way that the end-user is not obliged to pay for services or facilities which are not necessary or not required for the service requested.

(3) Undertakings providing universal services shall, upon request, supply the Regulatory Authority with and publish adequate and up-to-date information on their performance in the provision of universal service. Such information shall be based on the quality of service parameters, definitions and measurement methods set out in Annex III to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51).

57

Section 85

Suspension of Service

(1) Any undertaking obliged under section 81 to provide universal services or providing services under section 150(9) may suspend or restrict such service only temporarily on account of essential requirements conforming with Community law. It shall have regard to the interests of end-users and limit, as far as technically feasible, such suspension or restriction to the service concerned.

(2) Essential requirements justifying limited universal service are

1. security of network operations;

2. maintenance of network integrity, in particular the prevention of serious interference to the network or damage to software or stored data;

3. interoperability of services; and

4. data protection.

Section 86

Provision of Security

(1) Providers of publicly available telecommunications services obliged under section 81 to provide universal services and the undertaking providing services under section 150(9) shall have the right to make provision of universal services to the end-user conditional upon a reasonable amount of security where there are grounds to believe that the end-user will fail, or will fail within the prescribed period, to honour his contractual obligations. Security may be provided in the form of a surety bond from a financial institution registered in the European Economic Area. The provider shall have the right to limit the provision of security to such surety bond and a money deposit. The security shall be returned or cleared without undue delay as soon as the conditions requiring its provision cease to apply.

(2) Reasonable within the meaning of subsection (1) sentence 1 shall typically be the installation price plus six times the rental price. Any requirement to pay a higher amount shall be justified in relation to the end-user with reference to the circumstances of his particular case.

Section 87

Disclosure of Sales

(1) Where an obligation to provide universal service has been imposed under section 81 subsections (3) or (5), all undertakings operating in the relevant market for the applicable telecommunications services are to inform the Regulatory Authority annually, upon request, of their sales in this market. Otherwise the Regulatory Authority may make an estimate.

(2) With regard to the assessment of sales according to subsection (1), sections 36(2) and 38 of the Competition Act apply accordingly.

58

(3) The Regulatory Authority shall, taking into account the protection of trade and operating secrets of the undertakings concerned, publish a report annually which sets out the costs, as

calculated, of the universal service obligation and the contributions from all the undertakings and which identifies any market benefits that may have accrued to the designated undertaking.

PART 7

PRIVACY OF TELECOMMUNICATIONS, DATA PROTECTION, PUBLIC SAFETY

C h a p t e r 1

P r i v a c y o f T e l e c o m m u n i c a t i o n s

Section 88

Privacy of Telecommunications

(1) The content and detailed circumstances of telecommunications, in particular the fact of whether or not a person is or was engaged in a telecommunications activity, shall be subject to telecommunications privacy. Privacy shall also cover the detailed circumstances surrounding unsuccessful call attempts.

(2) Every service provider shall be obliged to maintain telecommunications privacy. The obligation to maintain privacy also applies after the end of the activity through which such commitment arose.

(3) All persons with obligations according to subsection (2) shall be prohibited from procuring, for themselves or for other parties, any information regarding the content or detailed circumstances of telecommunications beyond that which is necessary for the commercial provision of their telecommunications services, including the protection of their technical systems. Knowledge of facts which are subject to telecommunications privacy may be used solely for the purpose referred to in sentence 1. Use of such knowledge for other purposes, in particular, passing it on to other parties, shall be permitted only insofar as provided for by this Act or any other legal provision and reference is made expressly to telecommunications activities. The reporting requirement according to section 138 of the Penal Code shall have priority.

(4) Where the telecommunications system is located on board a ship or an aircraft, the obligation to maintain privacy does not apply in relation to the captain or his second in command.

Section 89

Prohibition to Intercept, Obligation on

Receiving Equipment Operators to Maintain Privacy

Interception by means of radio equipment shall be permitted only for communications intended for the radio equipment operator, radio amateurs within the meaning of the Amateur Radio Act of 23 June 1997 (Federal Law Gazette Part I page 1494), the general public or a non-defined group of persons. The content of communications other than those referred to in sentence 1 and the fact of their reception, even where reception has been unintentional, may not, even by persons not already committed to privacy under section 88, be imparted to others.

59

Section 88(4) applies accordingly. The interception and passing on of communications by special legal authorisation remain unaffected.

Section 90

Misuse of Transmitting Equipment

(1) It shall be prohibited to own, manufacture, market, import or otherwise introduce in the area of application of this Act transmitting equipment which, by its form, purports to be another object or is disguised under an object of daily use and, due to such circumstances, is particularly suitable for intercepting the non-publicly spoken words of another person without his detection or for taking pictures of another person without his detection. The prohibition on owning such transmitting equipment does not apply to any person obtaining or acquiring actual control of transmitting equipment

1. as an executive body, as a member of an executive body, as a legal representative or as a partner entitled to represent a person authorised under subsection (2);
2. from another or for another person authorised under subsection (2) if and for as long as he has to comply by virtue of service or employment relations with the directives given by the other party concerning exercise of the actual control of the transmitting equipment, or exercises actual control by virtue of a court order or an order from a public authority;
3. as a bailiff or an enforcement officer in enforcement proceedings;
4. temporarily, from a person authorised under subsection (2), for the purpose of safe custody or non-commercial conveyance to an authorised person;
5. for conveyance or storage for business purposes only;
6. by finding, provided that such person hands over the equipment without undue delay to the loser, the owner, any other party entitled to acquire the equipment or the office responsible for taking delivery of the lost property report;
7. causa mortis, provided that such person gives the transmitting equipment to an authorised person without undue delay or renders it permanently unusable; or
8. which has been rendered permanently unusable by the removal of a major component, provided that such person gives notice in writing to the Regulatory Authority of the acquisition without undue delay, stating his particulars, the type of equipment, its trademark and any manufacturing number given on the equipment, and presents prima facie evidence that the equipment has been acquired for collection purposes only.

(2) The supreme federal and state authorities with competence shall allow exceptions where these are required in the public interest, in particular for public safety reasons. Subsection (1) sentence 1 does not apply insofar as the Federal Office of Economics and Export Control (BAFA) has authorised export of the transmitting equipment.

(3) It shall be prohibited to advertise, in public or in communications intended for a relatively large group of persons, transmitting equipment by indicating that the equipment is suitable for intercepting the non-publicly spoken words of another person without his detection or for taking

pictures of another person without his detection.

60

C h a p t e r 2

D a t a P r o t e c t i o n

Section 91

Scope

(1) This Chapter regulates the protection of the personal data of telecommunications subscribers and users in respect of the collection and use of such data by undertakings and persons providing telecommunications services on a commercial basis or contributing to such provision. Details, subject to telecommunications privacy, of the circumstances of an identified or identifiable legal person or partnership, to the extent that it is capable of acquiring rights and undertaking commitments, shall have the same status as personal data.

(2) In respect of closed user groups at public authorities of the federal states, this Chapter applies subject to the proviso that the relevant state data protection legislation applies in place of the Federal Data Protection Act.

Section 92

Transfer of Personal Data to Foreign Private Bodies

Service providers shall transfer to foreign private bodies personal data as provided for by the Federal Data Protection Act solely to the extent required for the provision of telecommunications services, for the preparation or dispatch of bills and to combat fraud.

Section 93

Duty to Provide Information

When concluding contracts, service providers shall inform their subscribers of the nature, extent, place and purpose of the collection and use of personal data in such a way that the subscribers are given notice, in readily comprehensible form, of the basic data processing facts. The attention of subscribers shall also be drawn to the choices and options permitted. Users shall be informed by the service provider by means of generally available information about the collection and use of personal data. The right to provision of information as set out in the Federal Data Protection Act remains unaffected.

Section 94

Consent by Electronic Means

Consent may also be given electronically where the service provider ensures that

1. the subscriber or user has given his consent deliberately and unequivocally;

2. consent is recorded;

3. the subscriber or user can access his declaration of consent at any time; and

61

4. the subscriber or user can withdraw his consent at any time with effect for the future.

Section 95

Contractual Relations

(1) The service provider may collect and use customer data to the extent required to achieve the purpose referred to in section 3 para 3. Under a contractual relationship with another service provider, the service provider may collect and use the customer data of his subscribers and of the subscribers of the other service provider to the extent required for performance of the contract between the service providers. Transmission of the customer data to third parties, unless permitted by this Part or by another law, shall be carried out only with the subscriber's consent.

(2) The service provider may use the customer data of the subscribers referred to in subsection (1) sentence 2 for subscriber advisory purposes, for promoting his own offerings and for market research only to the extent required for such purposes and provided the subscriber has given his consent. A service provider who, under an existing customer relationship, has lawfully received notice of a subscriber's telephone number or postal address, including his electronic address, may use these for the transmission of text or picture messages to a telephone or postal address for the purposes referred to in sentence 1, unless the subscriber has objected to such use. Use of the telephone number or address according to sentence 2 shall be permitted only if the subscriber, when the telephone number or address is collected or first stored and on each occasion a message is sent to such telephone number or address for one of the purposes referred to in sentence 1, is given information in clearly visible and well readable form that he may object at any time, in writing or electronically, to the dispatch of further messages.

(3) When the contractual relationship ends, the customer data are to be erased by the service provider upon expiry of the calendar year following the year in which the contract terminated. Section 35(3) of the Federal Data Protection Act applies accordingly.

(4) In connection with the establishment of, or modification to, a contractual relationship or with the provision of telecommunications services, the service provider may require presentation of an official identity card where this is necessary to verify the subscriber's particulars. The service provider may make a copy of the identity card. The copy is to be destroyed by the service provider without undue delay once the particulars needed for the conclusion of the contract have been established. The service provider may not use data other than the data permitted under subsection (1).

(5) The provision of telecommunications services may not be made dependent upon the subscriber's consent to use of his data for other purposes where the subscriber is not able, or is not able in reasonable manner, to access such telecommunications services in another way.

Section 96

Traffic Data

(1) The service provider may collect and use the following traffic data to the extent required for the purposes set out in this Chapter–

62

1. the number or other identification of the lines in question or of the terminal, personal authorisation codes, additionally the card number when customer cards are used, additionally the location data when mobile handsets are used;
2. the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
3. the telecommunications service used by the user;
4. the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
5. any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

(2) Stored traffic data may be used after the termination of a connection only where required to set up a further connection or for the purposes referred to in sections 97, 99, 100 and 101. Otherwise, traffic data are to be erased by the service provider without undue delay following termination of the connection.

(3) The service provider may use subscriber-related traffic data used by the provider of a publicly available telecommunications service for the purpose of marketing telecommunications services, shaping telecommunications services to suit the needs of the market or for the provision of value added services for the duration necessary only where the data subject has given his consent to such use. The data of the called party are to be made anonymous without undue delay. Traffic data relating to the destination number may be used by the service provider for the purpose referred to in sentence 1 only with the consent of the called party. In such case, the called party data are to be made anonymous without undue delay.

(4) When obtaining consent, the service provider is to inform the subscriber of the data types which are to be processed for the purposes referred to in subsection (3) sentence 1 and of the storage duration. Additionally, the subscriber's attention is to be drawn to the possibility of withdrawing his consent at any time.

Section 97

Charging and Billing

(1) Service providers may use the traffic data set out in section 96(1) to the extent the data are required to charge and bill their subscribers. Where a service provider provides his services over the public telephone network of a third-party operator, such operator may transmit to the service provider the traffic data collected for the provision of his services. A service provider entering into a contract with a third party on the collection of charges may transmit to the third party the data referred to in subsection (2) to the extent required for collection of the charges and preparation of a detailed bill. The third party shall undertake contractually to maintain telecommunications privacy according to section 88 and data protection according to sections 93 and 95 to 97, 99 and 100. Section 11 of the Federal Data Protection Act remains

unaffected.
(2) The service provider may, for proper telecommunications service charging and billing and verification of the accuracy of the same, collect and use the following personal data subject to the provisions of subsections (3) to (6)–
63
1. traffic data according to section 96(1);
2. the address of the subscriber or recipient of the bill, the type of line, the total number of units of use incurred during the accounting period for a regular bill, the volumes of data transmitted, the total amount payable;
3. other relevant billing information such as advance payments, payments with date of entry, payments in arrears, reminders, disconnections and restorations, complaints submitted and handled, extensions of time for payment applied for and granted, payment by instalment and provision of security.
(3) The service provider shall, after termination of the connection, establish from the traffic data according to section 96(1) paras 1 to 3 and 5 without undue delay the data required for charging. All data not required shall be erased without undue delay. Traffic data may – subject to
subsection (4) sentence 1 para 2 – be stored for a period not exceeding six months after dispatch of the bill. Where, prior to expiry of the time limit referred to in sentence 3, the subscriber has raised objections to the amount billed, the traffic data may be stored until such time as the objections have been finally settled.
(4) Depending on how the subscriber chooses, the service provider issuing the bill shall, in respect of the destination number,
1. store it in full or with deletion of the last three digits; or
2. erase it completely upon dispatch of the bill to the subscriber.
The subscriber shall be informed of his right to choose; if he does not exercise this right, destination numbers shall be stored without deletion of the last three digits. Where a subscriber
is liable to pay, in full or in part, the charges for incoming calls on his line, the numbers of the calling lines may be transmitted only with deletion of the last three digits. Sentences 1 and 2 do not apply to service providers offering their services solely to the members of closed user groups.
(5) The service provider may use traffic data to the extent required for his billing with other service providers or with their subscribers, and for other service providers' billing with their subscribers.
(6) Where the bill from the service provider includes payment for third-party services supplied in connection with the provision of telecommunications services, the service provider may transmit to the third party customer data and traffic data to the extent that these are

required in a given instance to enforce third-party claims in relation to the subscriber.

Section 98

Location Data

(1) Location data relating to users of public telecommunications networks or publicly available telecommunications services may be processed only when they have been made anonymous or with the consent of the subscriber to the extent and for the duration necessary for
the provision of value added services. The subscriber shall inform his co-users of all such consent given. Consent may be withdrawn at any time.

64

(2) Where the consent of the subscriber to the processing of location data has been obtained, the subscriber shall continue to have the possibility, using a simple means and free of
charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

(3) In respect of calls to the emergency call number "112", to telephone numbers determined in the ordinance as provided for under section 108(2) and to the telephone number "124124", the service provider shall ensure that the transmission of location data is not ruled out on a per-call or a per-line basis.

Section 99

Itemised Billing

(1) The subscriber shall be informed of data stored under section 97(3) sentences 3 and 4 and subsection (4) until dispatch of the bill and relating to calls for which he is liable to pay only if
he has made a request, in text form, for an itemised bill prior to the relevant accounting period. In respect of residential lines, the disclosure of such information is permitted only if the subscriber has declared, in text form, that he has informed all co-users of the line, and will inform
future co-users without undue delay, of the disclosure to him of the traffic data underpinning the
bill. In respect of lines in businesses and public authorities, the disclosure of such information is
permitted only if the subscriber has declared, in text form, that the employees have been informed, and new employees will be informed without undue delay, and that the works council or the staff representation has been involved in accordance with the statutory requirements, or that such involvement is not necessary. Where public-law religious societies have issued their own employee representation regulations for their domain, sentence 3 applies, it being understood that the respective employee representation acts in place of the works council or

the
staff representation. Furthermore, the subscriber may be informed of data stored under section 97(3) sentences 3 and 4 and subsection (4) after dispatch of the bill if he has raised objections to the amount billed. Where a subscriber is liable to pay, in full or in part, the charges
for incoming calls on his line, the numbers of the calling lines may appear on the itemised bill issued to him only with deletion of the last three digits. Sentence 6 does not apply to service providers who, as providers for closed user groups, offer their services solely to the members of
these.
(2) The itemised bill according to subsection (1) sentence 1 may not allow calls to persons, public authorities or organisations in the social or the church domain who or which offer anonymous counselling wholly or predominantly by telephone to callers in emotional or social distress and who or which themselves or whose employees therefore have a special duty not to
disclose confidential information, to be identified. This applies only to the extent that the Regulatory Authority has entered such called lines on its register. Serving to provide counselling
as defined in sentence 1, besides the groups referred to in section 203(1) paras 4 and 4a of the
Penal Code, are, notably, telephone crisis counselling services and healthcare organisations. The Regulatory Authority enters the holders of these lines on its register, upon application, when
they have evidenced their remit as set out in sentence 1 by certification from a public authority or
corporation, a public-law agency or foundation. The register is kept available for retrieval in an automated procedure. The service provider shall access the register every quarter and incorporate in his billing procedures any changes without undue delay. Sentences 1 to 6 do not
apply to service providers who, as providers for closed user groups, offer their services solely to
the members of these.
65
(3) Customer cards, where used, shall carry clear indication of the possible disclosure of stored traffic data. Where such indication is not possible for technical reasons or could not reasonably be expected of the card issuer, the subscriber must have made a declaration according to subsection (1) sentence 2 or 3.
Section 100

Faults in Telecommunications Systems and Telecommunications Service Fraud

(1) Where required, the service provider may collect and use the customer data and traffic data of subscribers and users in order to detect, locate and eliminate faults and malfunctions in telecommunications systems.

(2) For purposes of changed implementations and the identification and location of faults in the network, the operator of the telecommunications system and his authorised representative shall be allowed to break in on existing connections, as far as this is operationally required. Break in shall be indicated by means of an acoustic signal and explicitly notified to the parties concerned.

(3) Where required, the service provider may collect and use the customer data and traffic data needed to detect and put a stop to the surreptitious use of services and other unlawful use
of telecommunications networks and services when there are grounds, to be recorded in writing,
to suppose such use. For the purpose referred to in sentence 1 the service provider may use collected traffic data in such a way as to identify, from the total traffic data not more than six months old, the data relating to those network connections in respect of which there are grounds
to suppose that unlawful use of telecommunications networks and services has been made. In particular, the service provider may set up a pseudonymised data file from the customer data and the traffic data collected under sentence 1 which provides information on the revenues generated by the individual subscribers and which, suitable fraud criteria being applied, allows network connections in respect of which there are grounds to suppose that surreptitious use of services has been made, to be found. Data relating to all other communications are to be erased
without undue delay. The Regulatory Authority and the Federal Data Protection Commissioner are to be notified without undue delay of the introduction of, and any modification to, the procedure according to sentence 1.

(4) Subject to the conditions referred to in subsection (3) sentence 1 the service provider may, in a given instance, collect and use control signals to the extent that this is indispensable to
clarify and put a stop to the acts specified there. Collection and use of any other communications content is not permitted. The Regulatory Authority is to be notified of measures
according to sentence 1 taken in a given instance. The parties concerned are to be advised as soon as it is possible to do so without the purpose of the measures being compromised.

Section 101

Information on Incoming Calls

(1) The service provider shall, upon written application, give any subscriber arguing conclusively in a procedure for documentation that he is the object of malicious or nuisance calls, information, for more than one network also, on the lines on which the calls originated. The
information may relate solely to calls made after submission of the application. The service provider may collect, use and disclose to his subscriber data relating to the telephone numbers,
names and addresses of the line holders and the date and time of the beginning of the calls and
66
call attempts. Sentences 1 and 2 do not apply to service providers offering their services solely to the members of closed user groups.
(2) Disclosure according to subsection (1) sentence 3 may be made only when the subscriber has narrowed down the calls beforehand in respect of date, time or any other suitable
criteria if misuse of this procedure cannot be ruled out in any other way.
(3) In the case of information for more than one network, the other service providers contributing to the connection are obliged to give the service provider of the subscriber receiving
malicious or nuisance calls the information required, provided they have such data.
(4) The holder of the line on which the identified calls originated is to be advised that information on these has been disclosed. An exception may be made if the applicant has argued
conclusively in writing that any such disclosure could bring him significant disadvantages, and these disadvantages, when compared with the legitimate interests of the calling parties, appear
considerably more serious. Subscribers on whose line the alleged malicious or nuisance calls originated receiving notice in another way of the disclosure of information are to be informed, upon request, of such disclosure.
(5) The Regulatory Authority and the Federal Data Protection Commissioner are to be notified without undue delay of the introduction of, and any modification to, the procedure to enforce subsections (1) to (4).

Section 102

Line Identification Presentation and Restriction

(1) Where the service provider offers calling line identification presentation, the calling and the called parties shall have the possibility, using a simple means and free of charge, of preventing presentation of the telephone number on a per-line or a per-call basis. Called parties

shall have the possibility, using a simple means and free of charge, of rejecting incoming calls from a calling party that has prevented presentation of its telephone number. Sentences 1 and 2
do not apply to service providers offering their services solely to the members of closed user groups.
(2) Upon application by the subscriber, the service provider shall provide lines on which presentation on the connected line of the telephone number of the calling line is ruled out, free of
charge. At the subscriber's request, these lines are to be indicated as such in the public directory
of subscribers (section 104) issued by his provider. Where an indication according to sentence 2
has been made, presentation of the telephone number of the calling line on a line thus indicated
shall be possible only when the indication has been taken out of the latest edition of the public directory.
(3) Where the subscriber has chosen not to apply for entry as provided for by section 104 in the directory of subscribers, presentation of the telephone number of his line shall not be made on the connected line unless the subscriber explicitly wishes such presentation.
(4) Where connected line identification presentation is offered, called parties shall have the possibility, using a simple means and free of charge, of preventing presentation of the connected line identification to the calling party. Subsection (1) sentence 3 applies accordingly.
67
(5) Subsections (1) and (4) also apply to calls to and from other countries, to the extent that they concern calling or called parties in the Federal Republic of Germany.
(6) In respect of calls to the emergency call number "112", to telephone numbers determined in the ordinance as provided for under section 108(2) and to the telephone number "124124", the service provider shall ensure that calling line identification presentation is not ruled out on a
per-call or on a per-line basis.
Section 103
Automatic Call Forwarding
The service provider shall undertake to give his subscribers the possibility, using a simple means and free of charge, of stopping calls being automatically forwarded to their terminal as a
result of action taken by a third party, to the extent that this is technically feasible. Sentence 1 does not apply to service providers who, as providers for closed user groups, offer their

services
solely to the members of these.
Section 104
Directories of Subscribers
Subscribers may have their name, address and additional information such as occupation, branch and type of line entered in public printed or electronic directories, where requested. Subscribers may specify what information is to be published in the directories. At the subscriber's request, co-users may be entered, provided they agree.
Section 105
Directory Information
(1) Information on telephone numbers included in directories may be provided subject to the restrictions set out in section 104 and in subsections (2) and (3).
(2) Information provided by means of a telephone system on the telephone numbers of subscribers may be given only if subscribers have been suitably informed that they may withhold
consent to their telephone number being passed on and have not exercised their right to withhold consent. Information on data published under section 104 other than telephone numbers may be provided only if the subscriber has given his consent to such additional data being passed on.
(3) Providing information by means of a telephone system on the names or names and addresses of subscribers in relation to whom solely the telephone number is known is permitted
if the subscriber whose data have been included in a directory of subscribers has not withheld consent after having been informed by his service provider of the possibility of doing so.
(4) All withholding of consent as provided for by subsection (2) sentence 1 and subsection (3) or giving of consent as provided for by subsection (2) sentence 2 shall be noted without undue delay in the customer files of the service provider or of the information provider according to subsection (1) on which the directories are based. Withholding or giving of consent
shall also be heeded by the other service providers as soon as they could reasonably be
68
expected to know that the withholding or giving of consent has been noted in the directories of the service provider and of the information provider according to subsection (1).
Section 106
Telegram Service
(1) Data and documents relating to the operational handling and the delivery of telegrams may be stored to the extent necessary to demonstrate proper provision of the telegram service under the contract concluded with the subscriber. The data and documents shall be erased by

the service provider after a period of six months at the latest.
(2) Data and documents relating to the content of telegrams may be stored beyond the date of delivery only if the service provider is answerable for transmission faults under the contract concluded with the subscriber. Data and documents relating to inland telegrams shall be erased
by the service provider after a period of three months at the latest, and data and documents relating to international telegrams shall be erased by the service provider after a period of six months at the latest.
(3) The time limits for erasure shall begin running on the first day of the month following that in which the telegram was tendered. Erasure may be suspended where the prosecution of claims or international agreements necessitate a longer storage period.
Section 107
Store and Forward Systems
(1) In respect of services the carrying out of which requires intermediate storage, the service provider may process the content of communications, notably the voice, sound, text and graphics messages of subscribers, as part of a service offer based on these, subject to the following conditions–
1. processing takes place solely in telecommunications systems of the service provider carrying
out intermediate storage, unless the content of the communication is re-routed to the telecommunications systems of other providers at the request of the subscriber or by subscriber input;
2. solely the subscriber determines, by his input, the content, scope and type of processing;
3. solely the subscriber determines who may input and access the content of communications (party having the right of access);
4. the service provider may inform the subscriber that the recipient has accessed the message;
5. the service provider may erase the content of communications only as provided for in the contract concluded with the subscriber.
(2) The service provider is to take the necessary technical and organisational measures to rule out transmission errors and the unauthorised disclosure, within his undertaking or to third parties, of the content of communications. Measures are required only if the time and effort expended is proportionate to the purpose of protection sought. Measures are to be adjusted to the state of the art if this is necessary to achieve the purpose of protection sought.
69
C h a p t e r 3
P u b l i c S a f e t y
Section 108

Emergency Calls

(1) Any person offering publicly available telephone services shall undertake to provide all users with access to emergency services by using, free of charge, the single European emergency call number "112" and the additional national emergency call numbers determined in
the ordinance as provided for under subsection (2) sentence 1 para 1. Any person operating telecommunications networks used for publicly available telephone services shall be required to
transmit to the local emergency service centre, without undue delay, emergency calls, including
1. the calling line identity or, where the calling line identity is not available, the data required to prosecute any misuse of emergency calls as provided for by the ordinance under subsection (2); and
2. the information required to identify the location from which the emergency call originated.

(2) The Federal Ministry of Economics and Labour shall be empowered to make arrangements by ordinance having the force of law and requiring the consent of the German Bundesrat, in agreement with the Federal Ministry of the Interior and the Federal Ministry of Health and Social Security, concerning
1. determination of the additional national emergency call numbers;
2. the setting up of emergency connections either as calls or telefaxes to the local emergency service centre;
3. the extent of the emergency call features to be provided by network operators for the single European emergency call number "112" and for the national emergency call numbers, including the provision and transmission of the information required to locate the emergency caller;
4. the provision and transmission of suitable data to enable emergency service centres to prosecute any misuse of emergency calls;
5. the setting up of emergency calls by means of automatic calling equipment; and
6. the responsibilities of the Regulatory Authority in the fields referred to in paras 2 to 5.

Federal state regulations on emergency service centres remain unaffected by the provisions of this subsection insofar as they do not relate to obligations for network operators within the meaning of subsection (1).

(3) The Regulatory Authority shall stipulate the technical details of the subject matter referred to in subsection (2) sentence 1 paras 2 to 5 in a technical directive to be drawn up with the participation of industry associations, the representatives of the emergency service centre operators nominated by the Federal Ministry of the Interior, and manufacturers. International 70
standards are to be taken into consideration; reasons for deviations from the standards are to

be
stated. The technical directive is to be published by the Regulatory Authority in its Official Gazette. All persons with obligations under subsection (1) sentence 2 are to meet the requirements of the technical directive not later than one year following its publication, unless a longer transitional period has been specified there for particular obligations. In the event of an amendment to the directive, defective-free technical facilities configured to the directive shall meet the modified requirements not later than three years following its taking effect.

Section 109

Technical Safeguards

(1) Every service provider shall make appropriate technical arrangements or take other measures in order to protect

1. the privacy of telecommunications and personal data; and
2. telecommunications and data processing systems against unauthorised access.

(2) Any person operating telecommunications systems serving to provide publicly available telecommunications services shall, additionally, make appropriate technical arrangements or take other measures in order to protect telecommunications and data processing systems operated for such purpose against any faults which would result in considerable harm to telecommunications networks, and against external attacks and the effects of natural disasters.

In doing so, regard shall be had to the state of the art and to the physical location of own and shared network elements. Where a site or technical facilities are shared, each operator of the telecommunications system shall meet the obligations according to subsection (1) and sentence 1 unless particular obligations can be assigned to a particular operator. Technical arrangements and other safeguards are deemed reasonable if the technical and economic effort
required is proportionate to the importance of the rights to be protected and to the importance of
the facilities to be protected for the general public.

(3) Any person operating telecommunications systems serving to provide publicly available telecommunications services shall nominate a security commissioner and draw up a security concept setting out

1. which telecommunications systems are to be used and which publicly available telecommunications services provided;
2. any potential hazards, and
3. which technical arrangements or other safeguards have been made or put in place or are planned in order to meet the obligations according to subsections (1) and (2).

The security concept is to be submitted to the Regulatory Authority by the operator without undue delay after the beginning of provision of the telecommunications services, along with a

declaration that the technical arrangements and other safeguards specified there have been, or
will be, implemented without undue delay. Where the Regulatory Authority establishes shortcomings in the security concept itself or in the course of its implementation, it may require the operator to eliminate them without undue delay. If the configuration of the system on which the security concept is based changes, the operator shall adapt and resubmit his concept to the
Regulatory Authority with reference to the changes made. Sentences 1 to 4 do not apply to 71
operators of telecommunications systems intended exclusively for the reception and distribution
of broadcasting signals. The obligation according to sentence 2 is deemed met in respect of security concepts submitted to the Regulatory Authority under section 87 of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120).

Section 110

Technical Implementation of Intercepts

(1) Any person operating a telecommunications system by means of which publicly available telecommunications services are provided, shall,

1. from the time of beginning operation, at his own expense, provide technical facilities with which to implement telecommunications interception measures provided for by law and make organisational arrangements for the implementation, without undue delay, of such measures;
2. without undue delay after beginning operation, vis-à-vis the Regulatory Authority,
a) declare that he has made the arrangements according to para 1; and
b) nominate a body located in the Federal Republic of Germany to receive judicial orders destined for him, relating to telecommunications interception;
3. demonstrate to the Regulatory Authority, at no charge, that the technical facilities and organisational arrangements according to para 1 are compliant with the provisions of the ordinance according to subsection (2) and the technical directive according to subsection (3); to this end, he shall, without undue delay but not later than one month after beginning operation,
a) send to the Regulatory Authority the documents needed to prepare the checks the Regulatory Authority carries out to verify compliance; and
b) agree with the Regulatory Authority a date for demonstrating and verifying compliance; he shall assist the Regulatory Authority in the checks required for verifying compliance;
4. allow the Regulatory Authority, at its special request in a given, justified instance, to re-check, at no charge, his technical and organisational arrangements; and
5. tolerate the installation and operation on his premises of equipment for the implementation

of
measures under sections 5 and 8 of the Article 10 Act and grant staff of the office responsible for such measures and members and staff of the G10 Commission (section 1(2) of the Article 10 Act) access to such equipment for the discharge of their legal functions.
Any person offering publicly available telecommunications services without themselves operating a telecommunications system to do so shall, when choosing the operator of the telecommunications system to be used for doing so, make certain that the latter can carry out judicial orders relating to telecommunications interception without undue delay as provided for by the ordinance according to subsection (2) and by the technical directive according to subsection (3), and notify the Regulatory Authority without undue delay after beginning to provide service of which telecommunications services he is offering, by whom judicial intercept
72
orders concerning his subscribers are to be carried out and to which body located in the Federal
Republic of Germany judicial orders relating to telecommunications interception are to be addressed. Any changes in the data on which the notifications according to sentence (1) para (2) b) and sentence 2 are based are to be notified to the Regulatory Authority without undue delay. In cases in which provisions according to subsection (3) are not yet available, the person with obligations shall configure the technical facilities according to sentence 1 para 1 in agreement with the Regulatory Authority. Sentences 1 to 4 do not apply where the ordinance according to subsection (2) provides for exemptions with regard to the telecommunications system. Section 100b(3) sentence 1 of the Code of Criminal Procedure, section 2(1) sentence 3
of the Article 10 Act and the relevant state regulations on preventive telecommunications interception by the police remain unaffected.
(2) The Federal Government shall be empowered
1. to make arrangements concerning
a) the technical essential requirements and the organisational key elements for the implementation of intercepts, including the implementation of intercepts by a person acting on behalf of the person with obligations;
b) the extent of the arrangements in the technical directive according to subsection (3);
c) demonstration of compliance as provided for by subsection (1) sentence 1 paras 3 and 4; and
d) details of the obligation of tolerance as required by subsection (1) sentence 1 para 5; and
2. to determine
a) the cases in which and the conditions under which compliance with certain technical requirements can be dispensed with on a temporary basis;
b) that the Regulatory Authority may, for technical reasons, allow exemptions in respect of

meeting particular technical requirements; and
c) in respect of which telecommunications systems and associated service offers technical facilities need not be offered or organisational measures need not be taken, in derogation of subsection (1) sentence 1 para 1, on account of basic technical considerations or for reasons of proportionality,
by ordinance having the force of law and requiring the consent of the German Bundesrat.
(3) The Regulatory Authority shall stipulate, in a technical directive to be drawn up in consultation with the authorised bodies and with the participation of industry associations and manufacturers, the technical details required to guarantee a full record of telecommunications intercepts and for configuration of the point of handover to the authorised bodies. International technical standards are to be taken into consideration; reasons for deviations from the standards
are to be stated. The technical directive is to be published by the Regulatory Authority in its Official Gazette.
(4) Any person manufacturing or distributing technical facilities for the implementation of intercepts may require the Regulatory Authority to verify, by testing the interworking of a type
73
sample with particular telecommunications systems, whether or not the legal and technical provisions of the ordinance according to subsection (2) and of the technical directive according to subsection (3) have been met. The Regulatory Authority may, after due assessment of the circumstances, allow deviations from the technical requirements on a temporary basis, provided
that implementation of the intercepts is secured in principle and only insignificant adjustments to
the technical facilities of the authorised bodies are required. The Regulatory Authority is to notify
the manufacturer or distributor in writing of the test results. The test results are noted by the Regulatory Authority in connection with the demonstration of compliance of the technical facilities with the applicable technical provisions which the person with obligations is required to
provide under subsection (1) sentence 1 para 3 or 4. Consent to the framework concepts presented by manufacturers given by the Federal Ministry of Economics and Labour prior to the
entry into force of this provision is deemed notification within the meaning of sentence 3.
(5) Any person obliged under subsection (1) in conjunction with the ordinance according to subsection (2) to make arrangements is to meet the requirements of the ordinance and the technical directive according to subsection (3) not later than one year following their publication,

unless a longer period has been determined there for particular obligations. Defective-free technical facilities configured to this directive for telecommunications services already offered by
the person with obligations shall, in the event of an amendment to the directive, meet the modified requirements not later than three years following its taking effect. Where shortcomings
in the technical or organisational arrangements of the person with obligations are found in the process of compliance according to subsection (1) sentence 1 para 3 being demonstrated or a re-check according to subsection (1) sentence 1 para 4 being made, the person with obligations
is to eliminate such shortcomings within a reasonable period of time as provided for by the Regulatory Authority; where shortcomings are found during operations, notably when intercepts
are carried out, the person with obligations is to eliminate such shortcomings without undue delay. If type samples have been tested under subsection (4) for the technical facilities and deadlines set for the elimination of shortcomings, the Regulatory Authority shall take these deadlines into account in its specifications on the elimination of shortcomings according to sentence 3.
(6) Every operator of a telecommunications system renting to third parties network termination points in his telecommunications system under his publicly available service offer shall undertake to make available to the bodies authorised by law to carry out telecommunications intercepts, without undue delay and as a matter of priority, at their request,
network termination points for transmission of the information obtained under an intercept. The technical configuration of such termination points may be laid down in the ordinance according to subsection (2). With the exception of special tariffs or surcharges for priority or early provision
or fault repair, the tariffs payable by the general public apply in respect of such provision and use. Any special contractually agreed discounts remain unaffected by sentence 3.
(7) Telecommunications systems operated by legally authorised bodies and by means of which intervention in the privacy of telecommunications or in network operation is to be brought
about, are to be technically configured in agreement with the Regulatory Authority. The Regulatory Authority is to comment on the technical configuration within a reasonable period of
time.
(8) Operators of telecommunications systems with obligations under sections 100a and 100b of the Code of Criminal Procedure are to prepare, and make available to the Regulatory

Authority at no charge, annual statistics of intercepts carried out under these provisions. The presentation of these statistics may be detailed in the ordinance according to subsection (2). Operators shall not disclose the statistics to third parties. The Regulatory Authority shall
74
aggregate the data provided by the undertakings and publish the result in its Official Gazette annually.
(9) The Federal Government shall be empowered to make arrangements, by ordinance having the force of law and requiring the consent of the German Bundestag and the German Bundesrat, with regard to appropriate compensation to be paid to service providers for services
supplied by them in
1. enabling intercepts under sections 100a and 100b of the Code of Criminal Procedure, section 2(1), section 5 or section 8 of the Article 10 Act, section 39 of the Foreign Trade and Payments Act or the relevant state regulations, and
2. providing information in accordance with section 113.
The costs of providing technical facilities as required to provide the services according to sentence 1 are not the subject of such compensation arrangements.
Section 111
Data for Information Requests from Security Authorities
(1) Any person commercially providing or assisting in providing telecommunications services and in so doing allocating telephone numbers or providing telecommunications connections for telephone numbers allocated by other parties is, for the information procedures according to sections 112 and 113, to collect, prior to activation, and store without undue delay the telephone
numbers, the name and address of the allocation holder, the effective date of the contract, the date of birth in the case of natural persons, and in the case of fixed lines, additionally the address for the line, even if such data are not required for operational purposes; where known, the date of termination of the contract is likewise to be stored. Sentence 1 also applies where the data are not included in directories of subscribers (section 104). A person with obligations according to sentence 1 receiving notice of any changes is to correct the data without undue delay; in this connection the person with obligations is subsequently to collect and store data according to sentence 1 not yet recorded if collecting the data is possible at no special effort. When the contractual relationship ends, the data are to be erased upon expiry of the calendar year following the year in which the contract terminated. Compensation for data collection and storage is not paid. The manner in which data for the information procedure according to section 113 are stored is optional.
(2) Where the service provider according to subsection (1) sentence 1 operates in conjunction with a sales partner, such partner shall collect data according to subsection (1)

sentence 1 and transmit to the service provider, without undue delay, these and data collected under section 95; subsection (1) sentence 2 applies accordingly. Sentence 1 also applies to data
relating to changes, inasmuch as the sales partner receives notice of them in the course of normal business transactions.
(3) Data within the meaning of subsection (1) sentence 1 need not be collected subsequently for contractual relationships existing on the date of entry into force of this provision, save in the cases referred to in subsection (1) sentence 3.
75
Section 112
Automated Information Procedure
(1) Any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111(1) sentences 1 and 3 and subsection (2) in customer data files in which the telephone numbers and quotas of telephone numbers allocated
to other telecommunications service providers for further marketing or other use and, with regard
to ported numbers, the current carrier portability codes, are also to be included. Section 111(1) sentences 3 and 4 apply accordingly with regard to the correction of customer data files. In the case of ported numbers the telephone number and associated carrier portability code are not to
be erased before expiry of the year following the date on which the telephone number was returned to the network operator to whom it had originally been allocated. The person with obligations shall ensure that
1. the Regulatory Authority can, at all times, retrieve from customer data files data for information requests from the authorities referred to in subsection (2) by means of automated procedures in the Federal Republic of Germany;
2. data can be retrieved using incomplete search data or searches made by means of a similarity function.
The requesting office is to consider, without undue delay, the extent to which it needs the data provided and erase, without undue delay, any data not needed. The person with obligations is to
ensure by technical and organisational measures that no retrievals can come to his notice.
(2) Information from the customer data files according to subsection (1) shall be provided to
1. the courts and criminal prosecution authorities;
2. federal and state police enforcement authorities for purposes of averting danger;
3. the Customs Criminological Office and customs investigation offices for criminal proceedings

and the Customs Criminological Office for the preparation and execution of measures under section 39 of the Foreign Trade and Payments Act;
4. federal and state authorities for the protection of the Constitution, the Federal Armed Forces Counter-Intelligence Office and the Federal Intelligence Service;
5. the emergency service centres according to section 108 and the service centre for the maritime mobile emergency number "124124";
6. the Federal Financial Supervisory Authority; and
7. the authorities responsible under state legislation for the prosecution of administrative offences as provided for by section 4(3) of the Undeclared Work Act, via central inquiry offices,
as stipulated in subsection (4), at all times, as far as such information is needed to discharge their legal functions and the requests are submitted to the Regulatory Authority by means of automated procedures.
76
(3) The Federal Ministry of Economics and Labour shall be empowered to issue, in agreement with the Federal Chancellery, the Federal Ministry of the Interior, the Federal Ministry
of Justice, the Federal Ministry of Finance and the Federal Ministry of Defence, an ordinance having the force of law and requiring the consent of the German Bundesrat, in which the following matters are regulated–
1. the essential requirements in respect of the technical procedures for
a) the transmission of requests to the Regulatory Authority;
b) the retrieval of data by the Regulatory Authority from persons with obligations, including the data types to be used for the queries; and
c) transmission by the Regulatory Authority to the requesting authorities of the data retrieved;
2. the security requirements to be observed; and
3. in respect of retrievals using incomplete search data and searches made by means of similarity functions for which specifications on the character sequences to be included in the search are provided by the Ministries contributing to the ordinance,
a) the minimum requirements in respect of the extent of the data to be entered in order to identify, as precisely as possible, the person to whom the search relates;
b) the permitted number of hits to be transmitted to the requesting authority; and
c) the requirements in respect of the erasure of data not needed.
In other respects, the ordinance may also restrict the query facility for the authorities referred to
in subsection (2) paras 5 to 7 to the extent that is required for such authorities. The Regulatory Authority shall determine the technical details of the automated retrieval procedure in a

technical
directive to be drawn up with the participation of the associations concerned and the authorised
bodies and to be brought into line with the state of the art, where required, and published by the
Regulatory Authority in its Official Gazette. The person with obligations according to subsection (1) and the authorised bodies are to meet the requirements of the technical directive
not later than one year following its publication. In the event of an amendment to the directive, defective-free technical facilities configured to the directive shall meet the modified requirements
not later than three years following its taking effect.
(4) At the request of the authorities referred to in subsection (2), the Regulatory Authority is to retrieve and transmit to the requesting authority the relevant data sets from the customer data
files according to subsection (1). It shall examine the admissibility of the transmission only where
there is special reason to do so. Responsibility for such admissibility lies with the authorities referred to in subsection (2). For purposes of data protection control by the competent body, the
Regulatory Authority shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, the person retrieving the data, the requesting authority and the reference number of the requesting authority. Use for any other purposes of data recorded is not
permitted. Data recorded are to be erased after a period of one year.
(5) The person with obligations according to subsection (1) is to make all such technical arrangements in his area of responsibility as are required for the provision of information under 77
this provision, at his expense. This also includes procurement of the equipment required to secure confidentiality and protection against unauthorised access, installation of a suitable telecommunications connection, participation in the closed user system and the continued provision of all such arrangements as are required under the ordinance and the technical directive according to subsection (3). Compensation for information provided by means of automated procedures is not paid to persons with obligations.
Section 113
Manual Information Procedure
(1) Any person commercially providing or assisting in providing telecommunications services shall, in a given instance, provide the competent bodies, at their request, without undue delay,

with information on data collected under sections 95 and 111 to the extent required for the prosecution of criminal or administrative offences, for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection
of the Constitution, the Federal Intelligence Service and the Federal Armed Forces Counter-Intelligence Office. The person with obligations according to sentence 1 shall provide information
on data by means of which access to terminal equipment or to storage devices or units installed
in such equipment or in the network is protected, notably personal identification numbers (PINs)
or personal unlocking keys (PUKs), by virtue of an information request under section 161(1) sentence 1 or section 163(1) of the Code of Criminal Procedure, data collection provisions in federal or state police legislation for averting danger to public safety or order, section 8(1) of the
Federal Constitution Protection Act, the corresponding provisions of the state constitution protection legislation, section 2(1) of the Federal Intelligence Service Act or section 4(1) of the Federal Armed Forces Counter-Intelligence Act; such data shall not be transmitted to any other
public or private bodies. Access to data which are subject to telecommunications privacy shall be permitted only under the conditions of the relevant legislation. The person with obligations shall maintain silence vis-à-vis his customers and third parties about the provision of information.

(2) The person with obligations according to subsection (1) is to make such arrangements as are required in his area of responsibility for the provision of information, at his expense. In respect of information provided, the person with obligations is granted compensation by the requesting authority, the level of which, in derogation of section 17a(1) para 2 of the Reimbursement of Witnesses and Experts Act, is determined by the ordinance referred to in section 110(9). Sentence 2 also applies in those cases in which, under the manual information procedure, merely data are requested which the person with obligations also keeps available for
retrieval under the automated information procedure according to section 112. Sentence 2 does
not apply in those cases in which the information was not provided completely or was not provided correctly under the automated information procedure according to section 112.

Section 114

Information Requests from the Federal Intelligence Service

(1) Any person providing publicly available telecommunications services or operating

transmission paths used for publicly available telecommunications services is to provide the Federal Ministry of Economics and Labour, upon request and at no charge, with information on the structures of telecommunications services and networks and on any forthcoming changes. Specific telecommunications activities and customer data of subscribers may not be the subject
of any information under this provision.
78
(2) Requests for information according to subsection (1) are permissible only when a request for such information has been made by the Federal Intelligence Service and the information is required to discharge functions according to sections 5 and 8 of the Article 10 Act. Use of information obtained under this provision for any other purposes is ruled out.
Section 115
Monitoring and Enforcement of Obligations
(1) The Regulatory Authority may give orders and take other measures to secure compliance with the provisions of Part 7 and the ordinances having the force of law issued by virtue of this Part and with the applicable technical directives. The person with obligations shall provide the necessary information at the request of the Regulatory Authority. To verify compliance with obligations the Regulatory Authority is authorised to enter and inspect, during normal business or working hours, business premises and production sites.
(2) The Regulatory Authority may set the following financial penalties in accordance with the Administrative Enforcement Act–
1. a fine not exceeding 500,000 euros to enforce obligations according to section 108(1), section 110(1), (5) or (6), an ordinance according to section 108(2), an ordinance according to section 110(2), an ordinance according to section 112(3) sentence 1, the technical directive according to section 108(3), the technical directive according to section 110(3) and the technical directive according to section 112(3) sentence 3;
2. a fine not exceeding 100,000 euros to enforce obligations according to sections 109, 112(1) and (3) sentence 4, subsection (5) sentences 1 and 2 and section 114(1); and
3. a fine not exceeding 20,000 euros to enforce obligations according to section 111(1) sentences 1 to 4 and subsection (2) and section 113(1) and (2) sentence 1.
In the event of repeated violations of the provisions of section 111(1) sentences 1 to 4 and subsection (2), section 112(1) and (3) sentence 4, subsection (5) sentences 1 and 2 or section 113(1) and (2) sentence 1, the activities of the person with obligations may be restricted
by order of the Regulatory Authority in such a way that his customer base may not be changed,
except as a result of contract expiry or notice of termination, until such time as the obligations ensuing from these provisions have been fulfilled.

(3) In the event of the non-fulfilment of obligations set out in Part 7, the Regulatory Authority may, in addition, wholly or partially prohibit operation of the telecommunications system concerned or commercial provision of the telecommunications service concerned if less severe
action to enforce proper conduct is insufficient.
(4) As far as the data of natural or legal persons are collected, processed or used for the commercial provision of telecommunications services, monitoring by the Federal Data Protection
Commissioner as provided for by sections 21 and 24 to 26(1) to (4) of the Federal Data Protection Act shall apply in place of monitoring as provided for by section 38 of the Federal Data Protection Act in respect of undertakings. The Federal Data Protection Commissioner shall
lodge his complaints with the Regulatory Authority and transmit to it any further results of monitoring after due assessment of the circumstances.
79
(5) The privacy of telecommunications as laid down in Article 10 of the Basic Law shall be restricted to the extent required for the monitoring specified in subsections (1) and (4).

PART 8

REGULATORY AUTHORITY

C h a p t e r 1

O r g a n i s a t i o n

Section 116

Headquarters and Legal Status

(1) The Regulatory Authority for Telecommunications and Posts shall discharge the functions and exercise the powers assigned to it under this Act and other laws. The Regulatory Authority is a higher federal authority responsible to the Federal Ministry of Economics and Labour with its
headquarters in Bonn.
(2) The Regulatory Authority shall be run by a President. The President shall represent the Regulatory Authority in and out of court and lay down the administration and order of business by rules of procedure; these shall require confirmation by the Federal Ministry of Economics and
Labour. Section 132(1) remains unaffected.
(3) The President and the two Vice Presidents shall be nominated by the Federal Government upon the proposal of the Advisory Council. Where, in spite of a request from the Federal Government, the Advisory Council fails to make a proposal within a period of four weeks, the right of nomination shall end. In the event of a proposal from the Advisory Council failing to meet with the approval of the Federal Government, the Advisory Council may submit

a
further proposal within a period of four weeks. The right of the Federal Government to take the final decision remains unaffected by this procedure.
(4) The President and the two Vice Presidents shall be appointed by the President of the Federal Republic of Germany.
Section 117
Publication of Directives from the Federal Ministry of Economics and Labour
All directives issued by the Federal Ministry of Economics and Labour shall be published in the Federal Gazette. This does not apply to such functions as are to be discharged by the Federal Ministry of Economics and Labour under its own jurisdiction by virtue of this Act or other
laws and the discharge of which it has transferred to the Regulatory Authority.
Section 118
Advisory Council
(1) There shall be constituted at the Regulatory Authority an Advisory Council. It shall consist of nine members of the German Bundestag and nine representatives of the German Bundesrat.
The representatives of the German Bundesrat shall be members or political representatives of 80
the government of a federal state. The members and deputy members of the Advisory Council shall be appointed by the Federal Government upon the proposal of the German Bundestag and
the German Bundesrat.
(2) Members proposed by the German Bundestag shall be appointed to the Advisory Council for the duration of the legislative period of the German Bundestag. They shall remain in office at
the end of this legislative period until such time as the new members have been appointed. Reappointment is permitted. The representatives proposed by the German Bundesrat shall be appointed to the Advisory Council for a period of four years; reappointment is permitted. They shall be removed from office if the German Bundesrat proposes another person in their place.
(3) Members may ask the Federal Ministry of Economics and Labour to release them from service, and resign from office. The declaration of release requires written form. Members proposed by the German Bundestag shall lose their membership when the requirements for their
appointment cease to apply.
(4) Should a member resign from office, a new member shall be appointed in his place without undue delay. Until such time as a new member has been appointed and in the event of a

member being temporarily prevented from performing his duties, the appointed deputy shall discharge his functions. Subsections (1) to (4) apply to deputy members accordingly.

Section 119

Rules of Procedure, Chairmanship, Meetings of the Advisory Council

(1) The Advisory Council shall adopt its rules of procedure, which require the approval of the Federal Ministry of Economics and Labour.

(2) The Advisory Council shall elect a Chairman and a Deputy Chairman from its members in accordance with its rules of procedure. The candidate obtaining the majority of votes shall be elected. If the required majority is not achieved in the first ballot, the majority of votes cast shall decide in the second. In the event of a tie in the second ballot, the matter shall be resolved by drawing lots.

(3) The Advisory Council shall constitute a quorum whenever more than half of the members nominated by the German Bundesrat and by the German Bundestag respectively are present. Resolutions shall be adopted by simple majority. In the event of a tied vote, a motion shall be dismissed.

(4) Where the Chairman considers debate of a resolution in draft unnecessary, the approval or comments of the members can be obtained by means of a written enquiry. Subsection (3) applies accordingly with regard to resolutions being effected. The enquiry should be made sufficiently early so that, at the request of a member or of the Regulatory Authority, the matter can still be debated in timely manner at a meeting.

(5) The Advisory Council should meet at least once a quarter. Meetings are to be convened when the Regulatory Authority or at least three members make a written request for such convocation. The Chairman of the Advisory Council may convene a meeting at any time.

(6) Ordinary meetings are not open to the public.

81

(7) The President of the Regulatory Authority and persons authorised by him or her may attend the meetings. They shall be consulted at all times. The Advisory Council may require the

presence of the President of the Regulatory Authority or, should the President be prevented from attending, that of a deputy.

(8) Members and persons representing them shall receive a refund of their travelling expenses and a commensurate attendance fee as determined by the Federal Minister of Economics and Labour.

Section 120

Functions of the Advisory Council

The Advisory Council shall have the following responsibilities–

1. making proposals to the Federal Government concerning the appointment of the President and Vice Presidents of the Regulatory Authority;

2. participating in Regulatory Authority decisions in the cases specified in section 61(4) paras 2 and 4 and section 81;
3. entitlement to request measures with which to implement the aims of regulation and to secure universal service. The Regulatory Authority shall undertake to decide on such requests within a period of six weeks;
4. entitlement in relation to the Regulatory Authority to obtain information and comments. The Regulatory Authority has the duty to provide information to the Advisory Council;
5. advising the Regulatory Authority in drawing up the Strategic Plan according to section 122(2) and, in particular, in making policy decisions of market relevance;
6. being consulted when the Frequency Usage Plan according to section 54 is drawn up.

Section 121

Activity Report

(1) The Regulatory Authority shall submit to the federal legislative bodies, along with the report according to subsection (2), a report on its activities and on the situation in and development of the telecommunications sector. This report shall also comment on the question
of whether or not modification of the determination of which telecommunications services have been deemed universal services within the meaning of section 78 is recommended.
(2) The Monopolies Commission shall, every two years, prepare an official report assessing the level and foreseeable development of competition and the question of whether or not there are sustainable competitive telecommunications markets in the Federal Republic of Germany, evaluating the application of the provisions of this Act concerning regulation and fair trading and
commenting on other current questions of competition policy, in particular, on the question of whether or not the ruling in section 21(2) para 3 needs to be adjusted in light of the development
of competition. The report should be completed by 30 November of the year in which a main report according to section 44 of the Competition Act is not submitted.

82

(3) The Federal Government shall submit to the federal legislative bodies, within a reasonable period of time, its comments on the report.

Section 122

Annual Report

(1) Once a year, the Regulatory Authority shall publish a report on the development of the telecommunications market presenting the main market data and consumer protection issues.
(2) To be included in the Annual Report, after public consultation, is a Strategic Plan listing matters of legal and economic policy to be addressed by the Regulatory Authority in the current

year. The findings are to be published in the Annual Report for the following year.
(3) The Regulatory Authority shall publish the principles of its administration on a regular basis.

Section 123

Cooperation with Other Authorities

(1) In the cases specified in sections 10, 11, 61(3) and section 62(2) para 3 the Regulatory Authority shall take decisions in agreement with the Federal Cartel Office. Where the Regulatory
Authority takes decisions in accordance with Part 2, Chapters 2 to 5, it shall give the Federal Cartel Office the opportunity to state its views in good time before closure of the case. Where the
Federal Cartel Office opens cases in the telecommunications sector under sections 19 and 20(1)
and (2) of the Competition Act, Article 82 of the EC Treaty or section 40(2) of the Competition Act, it shall give the Regulatory Authority the opportunity to state its views in good time before closure of the case. Both authorities shall seek to achieve a uniform interpretation of this Act and
one which is consistent with the Competition Act. They are to inform each other of all observations and findings which may be of significance to the discharge of their respective functions.
(2) The Regulatory Authority shall work together with the state media authorities. At their request, the Regulatory Authority shall inform these authorities of findings required for the discharge of their functions.

Section 124

Mediation

Where appropriate, the Regulatory Authority may, to resolve telecommunications disputes, propose that the parties affected seek to reach mutual agreement before a mediator (mediation
process).

Section 125

Specialist Consulting

(1) The Regulatory Authority may set up special commissions to prepare its decisions or to deliver opinions on regulatory issues. The members of such commissions shall, in the field of 83
telecommunications or postal services, have particular experience of economic, business management, socio-political, technological and legal matters, and possess proven expertise.
(2) The Regulatory Authority shall be given, on a continuing basis, specialist support in performing its functions. This concerns, in particular,

1. the regular assessment of national and international economic, business management, regulatory and social trends in telecommunications and postal services; and
2. the preparation and further development of the scientific basis for shaping universal service, the regulation of providers with significant market power, the rules governing open network provision and interconnection as well as numbering and customer protection.

C h a p t e r 2

Powers

Section 126

Prohibition

(1) Where the Regulatory Authority finds that an undertaking is failing to meet its obligations by or under this Act, it shall require the undertaking to state its views and to take remedial action.

It shall set a time limit for the undertaking to take remedial action.

(2) Where the undertaking fails to meet its obligations within the time limit set, the Regulatory Authority may order such measures as are necessary to secure adherence to the obligations. A

reasonable time limit is to be set to allow the undertaking to comply with the measures.

(3) In the case of serious or repeated breaches of obligations by the undertaking or failure to comply with measures for remedial action ordered by the Regulatory Authority under subsection (2), the Regulatory Authority may prohibit the undertaking acting in the capacity of telecommunications network operator or service provider.

4) Where such breach of obligations represents a direct and serious threat to public safety and order or such neglect of duty will create serious economic or operational problems for other

providers or users of telecommunications networks or services, the Regulatory Authority may, in

derogation of the procedures set out in subsections (1) to (3), take provisional measures. The Regulatory Authority shall decide, after it has given the undertaking concerned the opportunity to

state its views within a reasonable period, whether the provisional measures will be confirmed, withdrawn or modified.

(5) To enforce orders according to subsection (2), a penalty not exceeding 500,000 euros may be set in accordance with the Administrative Enforcement Act.

Section 127

Information Requests

(1) Without prejudice to other national reporting or information requirements, public telecommunications network operators and providers of publicly available telecommunications services are obliged, under the rights and obligations ensuing from this Act, to provide the

84

Regulatory Authority, upon request, with information required for execution of this Act. The Regulatory Authority may, in particular, require information for

1. the systematic or case-by-case verification of compliance with obligations ensuing from or by

virtue of this Act;

2. the case-by-case verification of compliance with obligations when the Regulatory Authority has received a complaint or has other reasons to assume non-compliance with obligations or when it has opened investigations on its own initiative;

3. the publication of comparative overviews of quality and price of service for the benefit of end-users;

4. clearly defined statistical purposes;

5. market definition or market analysis procedures according to sections 10 and 11;

6. procedures for the grant of rights of use and for the review of the relevant applications; and

7. the use of numbers.

Information as referred to in sentence 3, paras 1 to 5 may not be required prior to, or as a condition of, market access.

(2) As far as is necessary to discharge functions assigned to it under this Act, the Regulatory Authority may require telecommunications undertakings as referred to in subsection (1)

1. to provide information on their economic situation, in particular on their sales figures; and

2. to allow their business records to be inspected and audited within normal business or working hours.

(3) The Regulatory Authority shall request information as referred to in subsections (1) and (2) and arrange an audit as referred to in subsection (2) para 2 by written order. The legal basis, the subject matter and the purpose of the information request are to be stated in such order. In all information requests a reasonable time limit shall be determined for provision of the

information.

(4) Owners of undertakings or persons representing them and, in the case of legal persons, corporations or associations without legal capacity, those persons appointed representatives by

law or statutes, are obliged to provide information requested under subsections (1) and (2), to submit business records and to tolerate the auditing of their business records and access to business premises and property during normal business or working hours.

(5) Persons commissioned by the Regulatory Authority to conduct audits may have access to the offices and business premises of undertakings and associations of undertakings during normal business or working hours.

(6) Searches may be carried out solely by order of the local court in whose district the search

is to take place. With regard to appeals against such orders, sections 306 to 310 and 311a of the Code of Criminal Procedure apply accordingly. In cases of imminent danger, the persons designated in subsection (5) may carry out, during business hours, the necessary searches 85
without a judicial order. On site, a record of the search and its main findings shall be drawn up, from which, where a judicial order was not obtained, the facts leading to the assumption of imminent danger are also apparent.
(7) Objects and business records may be taken into custody as required or, where they are not handed over voluntarily, seized. With regard to seizure, subsection (6) applies accordingly.
(8) Persons with obligations to provide information under subsection (4) may refuse to answer any questions which would render themselves or relatives as specified in section 383(1)
paras 1 to 3 of the Code of Civil Procedure liable to prosecution or to proceedings under the Administrative Offences Act. Knowledge or records obtained as a result of information requests
or measures according to subsections (1) and (2) may not be used for taxation assessment proceedings or administrative fines proceedings involving an offence against tax laws or currency violations or for proceedings involving a fiscal or currency offence; sections 93, 97, 105(1), section 111(5) in conjunction with section 105(1) and section 116(1) of the Fiscal Code do not apply in this regard. Sentence 1 does not apply in respect of proceedings involving a fiscal offence or any related taxation assessment proceedings when there is an overriding public
interest in the institution of such proceedings, or in the event of the intentional provision of false
information by persons with obligations or by persons acting on their behalf.
(9) As far as audits reveal a violation of any conditions, orders or directions of the Regulatory Authority, the undertaking is to reimburse the Regulatory Authority with the expenses, including
any fees for experts, incurred by such audits.
(10) To enforce such orders, the Regulatory Authority may set a penalty not exceeding 500,000 euros in accordance with the Administrative Enforcement Act.
Section 128
Investigations
(1) The Regulatory Authority may conduct all investigations and take all evidence necessary.
(2) With regard to real evidence, testimonies and expert opinions, section 372(1),
sections 376, 377, 380 to 387, 390, 395 to 397, 398(1) and sections 401, 402, 404, 406 to 409, 411 to 414 of the Code of Civil Procedure apply accordingly; detention may not be imposed. The

higher regional court shall have jurisdiction to decide upon appeals.
(3) A record of the statements of the witnesses should be drawn up, to be signed by the investigating member of the Regulatory Authority and by a registrar also, if present. The record should include the place and date of the proceedings and the names of those assisting and of the parties concerned.
(4) The record is to be read to witnesses for their approval or presented for their own inspection. Approval given is to be noted and signed by the witnesses. In the event of the record
not being signed, the reason is to be stated.
(5) With regard to the questioning of experts, subsections (3) and (4) apply accordingly.
(6) The Regulatory Authority may request the local court to administer an oath to witnesses if it deems an oath necessary to bring about true statements. The court shall decide upon such confirmation by oath.
86
Section 129
Seizure
(1) The Regulatory Authority may seize objects which may be important as evidence in its investigations. Any such seizure is to be notified to the parties concerned without undue delay.
(2) The Regulatory Authority is, within a period of three days, to seek judicial confirmation from the local court of the district in which seizure took place when neither the parties concerned
nor adult relatives were present when seizure took place or when the parties concerned or, in their absence, adult relatives, expressly objected to such seizure.
(3) The parties concerned may at any time seek a judicial decision against seizure. They shall be instructed of this right. The court having jurisdiction according to subsection (2) shall decide on the motion.
(4) Appeals against judicial decisions are permissible. Sections 306 to 310 and 311a of the Code of Criminal Procedure apply accordingly.
Section 130
Provisional Orders
The Regulatory Authority may issue provisional orders pending a final decision.
Section 131
Conclusion of Proceedings
(1) Decisions of the Regulatory Authority are to be accompanied by a statement of reasons. They are to be served, along with the explanatory statement and information on permissible appeals, upon the parties concerned in accordance with the provisions of the Service in Administrative Procedure Act. Decisions issued in relation to an undertaking with its headquarters outside the area of application of this Act shall be served upon those designated

by the undertaking and notified to the Regulatory Authority as persons authorised to accept service. Where the undertaking has not designated any such persons, the Regulatory Authority
shall serve the decision by means of notice in the Federal Gazette.
(2) The closure of all proceedings not concluded by means of a decision served in accordance with subsection (1) sentences 2 to 4 upon the persons concerned is to be notified in
writing to the persons concerned.
(3) The Regulatory Authority may charge the persons concerned with the cost of taking evidence as appears fair.
87
C h a p t e r 3
Proceedings
Subchapter 1
Ruling Chambers
Section 132
Ruling Chamber Decisions
(1) The Regulatory Authority shall take decisions through its Ruling Chambers in the cases specified in Part 2, in section 55(9) and in sections 61, 62 and 81; subsection (3) sentence 1 remains unaffected. Decisions shall be taken by administrative act. Ruling Chambers shall, with
the exception of the Chamber referred to in subsection (3), be constituted as provided for by the
Federal Ministry of Economics and Labour.
(2) Chamber decisions shall be taken in the composition of Chairman and two Assessors. The Chairman and the Assessors shall be qualified to hold office in the senior administrative grade of the civil service. At least one member of the Ruling Chamber shall be qualified to exercise the
functions of a judge.
(3) In the cases specified in section 55(9) and in sections 61, 62 and 81 the Ruling Chamber shall take decisions in the composition of the President as Chairman and the two Vice Presidents as Assessors; accordingly, subsection (2) sentences 2 and 3 do not apply as far as these cases are concerned. The authority to act as a deputy in cases of absence is regulated in
the rules of procedure referred to in section 116(2). Decisions in the cases specified in section 61(4) paras 2 and 4 and in section 81 shall be taken in consultation with the Advisory Council.
(4) For the purposes of achieving a uniform ruling practice in comparable and related cases

and of securing the consistency requirement according to section 27(2), procedures are to be stipulated in the Regulatory Authority's rules of procedure imposing extensive coordination and information obligations on the Ruling Chambers and the departments concerned prior to decisions
being issued. Where Ruling Chamber decisions under sections 18, 19, 20, 21, 24, 30, 39, 40 and
41(1) are concerned, the rules of procedure shall ensure that determinations according to sections 10 and 11 are made by the President's Chamber.

Section 133

Other Disputes between Undertakings

(1) In the event of a dispute arising in connection with obligations ensuing from or by virtue of this Act between undertakings operating public telecommunications networks or offering publicly
available telecommunications services, the Ruling Chamber shall, unless otherwise provided for
by law, at the request of either party and after consultation with the parties concerned, issue a binding decision to resolve the dispute. The Ruling Chamber shall take its decision within a period not exceeding four months from the date of the request from one of the parties concerned
to resolve the dispute.

(2) In the event of a dispute arising in a field covered by this Act between undertakings in different Member States where the dispute falls within the competence of the national regulatory
authorities of at least two Member States, any of the parties may refer the dispute to the national
88
regulatory authority concerned. The Ruling Chamber is to take its decision in consultation with the national regulatory authority concerned within a period as referred to in subsection (1).

(3) Sections 126 to 132 and 134 to 137 apply accordingly.

Section 134

Institution of Proceedings, Parties Concerned

(1) Ruling Chambers shall institute proceedings on their own initiative or upon a motion.

(2) There shall take part in proceedings before the Chamber

1. the person presenting the motion;
2. the operators of public telecommunications networks and the providers of publicly available telecommunications services against whom the proceedings are directed; and
3. the persons and associations of persons whose interests are likely to be affected by the decision and to whom the Regulatory Authority has sent a summons to attend proceedings

in response to their request.

Section 135

Hearings, Oral Proceedings

(1) The Chamber is to give parties concerned the opportunity to state their views.

(2) Where appropriate, the Chamber may give persons representing business circles affected by the proceedings the opportunity to state their views.

(3) The Chamber shall decide on the matter in question on the basis of public oral proceedings; subject to the agreement of the parties concerned, it can take its decision without oral proceedings. At the request of any of the parties concerned or on the Chamber's own initiative the public is to be excluded from part or all of the proceedings if it poses a threat to public order, specifically to national security, or to an important trade or operating secret.

Section 136

Trade and Operating Secrets

Without undue delay when documents are submitted for Ruling Chamber proceedings, all parties concerned are to mark those parts containing trade or operating secrets. In this case they shall submit an additional copy which, from their point of view, can be inspected without such secrets being disclosed. Where this does not happen, the Ruling Chamber may assume their agreement to inspection, unless it is aware of any special circumstances that do not justify
such assumption. Where the Ruling Chamber considers marking the documents as confidential
to be unjustified, it shall, prior to taking a decision on allowing inspection by third parties, consult
with the submitting parties.

89

Subchapter 2

Legal Proceedings

Section 137

Appeals

(1) Protests and action against Regulatory Authority decisions shall not have suspensory effect.

(2) In the case of section 132, there shall be no preliminary proceedings.

(3) In the case of section 132, appeals (on issues of fact and law) against judgments and appeals (on procedural issues) against other decisions of the administrative court shall be ruled
out. This does not apply with regard to appeals against decisions according to section 138(3), appeals against denial of leave to appeal on questions of law under section 135 in conjunction with section 133 of the Code of Administrative Court Procedure and appeals against decisions

on jurisdiction under section 17a(2) and (3) of the Courts Constitution Act. Section 17a(4) sentences 4 to 6 of the Courts Constitution Act apply accordingly with regard to appeals against
decisions on jurisdiction.

Section 138

Submission and Information Duties of the Regulatory Authority

(1) Section 99(1) of the Code of Administrative Court Procedure applies with regard to the submission of documents or files, the transmission of electronic documents and the provision of
information (submission of documents) by the Regulatory Authority. The Regulatory Authority shall act in place of the supreme supervisory authority.

(2) Upon the motion of a party, the court dealing with the main issue shall decide by order whether the documents are to be submitted or whether they may not be submitted. Where trade
or operating secrets will be affected as a result of the submission of documents according to subsection (1), the court shall require the authority to submit the documents insofar as this is of relevance to the decision, there are no other ways of clarifying the matter and, after due assessment of all the circumstances of the particular case, the interest in submission of the documents outweighs the interest in confidentiality of the person concerned.

(3) The motion is to be filed within a period of one month of the notification by the court to the parties concerned of the Regulatory Authority's decision on submission of the documents. The Regulatory Authority is to submit the documents at the court's request; section 100 of the Code of Administrative Court Procedure does not apply. The members of the court have a duty to observe secrecy; the reasons for the decision may not allow the nature or content of confidential
documents to be ascertained. The court's decision on whether the documents are to be submitted or whether they may be submitted is appealable to the Federal Administrative Court. The appellate court division dealing with the main issue shall decide on the appeal. Sentences 2
and 3 apply accordingly with regard to the appeal proceedings.

(4) If, under the court's unappealable decision, the documents are not to be submitted or may not be submitted, the court or, in appeal proceedings, the court of appeal, shall return the documents submitted under subsection (3) sentence 2 to the Regulatory Authority immediately.

90

The court decision shall not be based on the content of any such documents unless all the parties concerned have given their consent.

Section 139

Participation of the Regulatory Authority in Civil Proceedings

Section 90(1) and (2) of the Competition Act apply accordingly with regard to civil proceedings ensuing from this Act. In all such cases the Regulatory Authority and its President shall act in place of the Federal Cartel Office and its President.

Subchapter 3

International Affairs

Section 140

International Affairs

The Regulatory Authority shall act on behalf of the Federal Ministry of Economics and Labour in the field of European and international telecommunications policy, in particular as regards participation in European and international institutions and organisations. This does not apply in respect of functions discharged by the Regulatory Authority under its own jurisdiction by virtue of this Act or other laws or by virtue of regulations of the European Communities.

Section 141

Recognised Accounting Authority in the Maritime Mobile Service

(1) The Federal Ministry of Economics and Labour shall be empowered to stipulate, by ordinance having the force of law but not requiring the consent of the German Bundesrat, the requirements and the procedure for recognition as a recognised accounting authority in the international maritime mobile service as provided for by the International Telecommunication Union. The procedure shall also specify the conditions for denial or revocation of such recognition.

(2) The authority responsible for the recognition of accounting authorities in the area of application of this Act shall be the Regulatory Authority.

91

PART 9

CHARGES

Section 142

Fees and Expenses

(1) The Regulatory Authority shall charge fees and expenses for the following official acts–

1. decisions on the grant of rights of use for frequencies according to section 55;
2. decisions on the grant of rights of use for telephone numbers by virtue of the ordinance according to section 66(4);
3. processing of applications for the registration of diallers using premium rate numbers;
4. case-by-case coordination, advance publication, assignment and notification of satellite systems according to section 56;
5. other official acts closely related to decisions taken under paras 1 to 4;

6. measures to counteract violations of this Act or of ordinances having the force of law issued by virtue of this Act;
7. decisions on the transfer of rights of way according to section 69; and
8. activities in connection with the procedure for recognition as a recognised accounting authority in the international maritime mobile service according to section 141.
Fees and expenses are also payable when an application for performance of an official act as specified in sentence 1
1. is rejected for reasons other than that of the authority not being responsible for the matter in question; or
2. is withdrawn after the beginning, but prior to completion, of processing.
(2) The Federal Ministry of Economics and Labour shall be empowered to stipulate in greater detail, in agreement with the Federal Ministry of Finance, by ordinance having the force of law but not requiring the consent of the German Bundesrat, chargeable acts and the level of the fees, including the mode of payment. The fee scales are to be calculated in such a way as to recover the costs incurred by the official acts. The provisions of the Administrative Expenses Act
apply additionally. In derogation of sentence 2, the fees payable for decisions on the grant of rights of use according to subsection (1) paras 1 and 2 are to be determined in such a way that they serve, as a steering mechanism, to secure optimal and efficient use of these commodities in line with the aims of this Act. Sentences 2 to 4 do not apply when numbers or frequencies of exceptionally great economic value are allocated by means of competitive or comparative selection procedures. The Federal Ministry of Economics and Labour may transfer to the Regulatory Authority the power referred to in sentence 1 by ordinance having the force of law, securing the arrangement on agreement between the authorities concerned when it does so. An
ordinance as referred to in sentence 6, including its repeal, requires the agreement of the Federal Ministry of Economics and Labour and the Federal Ministry of Finance.
92
(3) In derogation of the provisions of the Administrative Expenses Act, ordinances as referred to in subsection (2) sentence 1 may regulate the following matters–
1. the extent of the expenses to be refunded; and
2. the fees payable in respect of revocation or withdrawal of a grant of rights of use according to subsection (1) paras 1 or 2 or of a transfer of rights of way according to subsection (1) para 7 where this is attributable to the parties concerned.
(4) Fees and expenses may be assessed until the close of the fourth calendar year following creation of the debt (limitation of assessment period). Where an application for cancellation of or
modification to the assessment is submitted prior to expiry of the time limit, the running of the

assessment period is interrupted until such time as an unappealable decision on the application
has been taken. The right to payment of fees and expenses shall lapse at the close of the fifth calendar year following assessment (lapse of right to enforce payment). In other respects, section 20 of the Administrative Expenses Act applies.
(5) In the case of auctions according to section 61(5) a fee for the grant of rights of use according to subsection (1) para 1 shall be payable only when it exceeds the proceeds from the
auction.
(6) Authorities responsible for the construction and maintenance of public ways may, within their area of responsibility, adopt arrangements under which solely fees and expenses that cover the administrative costs of issuing notices of consent according to section 68(3) to the use
of public ways may be charged. Flat-rate fees are permitted.
Section 143
Frequency Usage Contribution Charges
(1) The Regulatory Authority shall levy annual contribution charges to recover costs it incurs for the management, control and enforcement of general assignments and rights of use for spectrum and orbit usage under this Act and the ordinances issued by virtue of this Act. This includes, in particular, costs incurred by the Regulatory Authority for the following activities–
1. the planning and further development of frequency usages, including the necessary measurements, tests and compatibility studies to secure efficient and interference-free use of frequencies; and
2. international cooperation, harmonisation and standardisation.
(2) Liable to make contributions are all those who have been assigned frequencies. The share of the costs shall be allocated to the separate user groups produced by frequency allocation, as far as possible on an expenditure-related basis. Within these groups, the costs shall be split in accordance with the use of frequencies. Contributions are also payable when a frequency is used by virtue of another administrative act or on a lasting basis without an assignment. This applies, in particular, with regard to rights granted before 1 August 1996, insofar as they include determinations on frequency usage.
(3) Not to be included in the costs to be recovered under subsection (1) are costs for which fees according to section 142 or fees according to section 16 of the Radio Equipment and
93
Telecommunications Terminal Equipment Act of 31 January 2001 (Federal Law Gazette Part I page 170) or fees or contributions according to sections 10 or 11 of the Electromagnetic Compatibility Act of 18 September 1998 (Federal Law Gazette Part I page 2882) or the ordinances issued by virtue of these provisions have already been levied.

(4) The Federal Ministry of Economics and Labour shall be empowered to determine, in agreement with the Federal Ministry of Finance, by ordinance having the force of law but not requiring the consent of the German Bundesrat, and as provided for by the above subsections, details of the category of persons liable to pay contribution charges, the rates of contribution charge and the procedure for the collection of contribution charges, including the mode of payment. The share of the costs attributable to public interest is to be taken into account in the form of a reduction in the level of contribution. The Federal Ministry of Economics and Labour may transfer to the Regulatory Authority the power according to sentence 1 by ordinance having
the force of law, securing the arrangement on agreement between the authorities concerned when it does so.

Section 144

Telecommunications Contribution Charges

(1) Persons with obligations under section 6(1) and section 4 of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) shall pay a contribution charge to offset
costs incurred by the Regulatory Authority for measures to secure fair competition and to promote public telecommunications markets with sustainable competition and for the management, control and enforcement of rights and obligations ensuing from this Act and from ordinances issued and rights of use granted under this Act, unless such costs are otherwise covered by fees or contribution charges levied under this Act. This also includes costs incurred by exercise of the functions referred to in sentence 1 in respect of international cooperation. The
share of the costs attributable to public interest is to be taken into account in the form of a reduction in the level of contribution.

(2) The relevant costs according to subsection (1) shall be split proportionately among the separate undertakings in accordance with their revenues from activities according to section 6(1)
and levied by the Regulatory Authority as an annual contribution charge.

(3) Fees paid under the Telecommunications Licence Fees Ordinance of 28 July 1997 (Federal Law Gazette Part I page 1936) and fees taken into account under section 16(2) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) shall, insofar as they exceed the fees payable under section 16(1) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) for the grant of a licence and the fees payable under the ordinance issued by virtue of that Act for the administrative cost of the grant of a licence, count towards the contribution charge. Section 143(3) applies accordingly.

(4) The Federal Ministry of Economics and Labour shall be empowered to regulate, by ordinance having the force of law but not requiring the consent of the German Bundesrat, in

agreement with the Federal Ministry of Finance, details of the collection of contribution charges,
notably the distribution key and reference date, the minimum assessment, the splitting mechanism, including a suitable estimation procedure and a classification scheme for determining the relevant costs according to subsection (2), the obligation to provide information
on sales, including a suitable procedure allowing for flat-rate payment, as well as payment deadlines, mode of payment and the level of penalties for late payment. The ordinance may also
set out arrangements for the provisional determination of contribution charges. The Federal 94
Ministry of Economics and Labour may transfer to the Regulatory Authority the power according
to sentence 1 by ordinance having the force of law, securing the arrangement on agreement between the authorities concerned when it does so. An ordinance according to sentence 3, including its repeal, shall require the agreement of the Federal Ministry of Economics and Labour and the Federal Ministry of Finance.

Section 145

Cost of Out-of-Court Dispute Resolution Procedures

Fees and expenses are payable for out-of-court dispute resolution procedures according to section 45(3) para 6. The level of the fee payable for resolution is determined as provided for by
section 11(2) sentences 2 and 3 of the Court Costs Act. Sections 3 to 9 of the Code of Civil Procedure apply accordingly with regard to determination of the amount in dispute. Where the dispute resolution office submits a proposal for resolution, it shall rule on the costs, having regard to the findings of fact and the matter in dispute, as appears fair. The cost ruling should be
made along with the dispute resolution proposal. Each party shall bear the costs it has incurred
for participation in the procedure itself. In other respects, sections 8 to 21 of the Administrative Expenses Act apply accordingly.

Section 146

Cost of Preliminary Proceedings

Fees and expenses are payable for preliminary proceedings. A fee not exceeding the fee fixed for the contested official act is payable for the complete or partial rejection of a protest. Where a fee is not payable for the contested official act of the Regulatory Authority, the fee is determined as provided for by section 11(2) sentences 2 and 3 of the Court Costs Act; section 145 sentence 3 applies accordingly. Where a protest is withdrawn after processing has

begun but prior to its completion, the fee shall not exceed 75 percent of the protest fee. The protests office shall decide the costs according to sentences 2 and 4 as appears fair.

Section 147

Information from the Regulatory Authority

The Regulatory Authority shall publish a yearly overview of its administrative costs and the total sum of charges collected. Where required, the fees and rates of contribution charges shall

be adjusted for the future in the ordinances concerned.

95

PART 10

PENAL AND ADMINISTRATIVE FINES PROVISIONS

Section 148

Penal Provisions

(1) Any person who,

1. in contravention of section 89 sentence 1 or 2, intercepts a communication or imparts to others the content of a communication or the fact of its reception; or
2. in contravention of section 90(1) sentence 1,

a) owns, or

b) manufactures, markets, imports or otherwise introduces in the area of application of this Act

transmitting equipment as referred to there,

is liable to a term of imprisonment not exceeding two years, or to a financial penalty.

(2) Where action in the cases of subsection (1) para 2 b) arises through negligence, the offender is liable to a term of imprisonment not exceeding one year, or to a financial penalty.

Section 149

Administrative Fines Provisions

(1) An administrative offence is deemed to have been committed by any person who, intentionally or negligently,

1. in contravention of section 4, fails to provide information, to provide it correctly, to provide it completely or to provide it in timely manner;
2. in contravention of section 6(1), fails to notify the Regulatory Authority, to notify it correctly, to

notify it completely, to notify it as prescribed or to notify it in timely manner;

3. in contravention of section 17 sentence 2, passes on information;
4. contravenes an enforceable order according to

a) section 20, section 23(3) sentence 2, section 29(1) sentence 1 para 1 or subsection (2) sentence 1 or 2, section 37(3) sentence 2, also in conjunction with section 38(4) sentence 4, section 38(4) sentence 2, also in conjunction with section 39(3) sentence 1

or section 42(4) sentence 1, also in conjunction with section 18(2) sentence 2;
b) section 67(1) sentence 4 or section 109(3) sentence 3;
96
c) section 29(1) sentence 2, section 39(3) sentence 2, section 65 or section 127(2) para 1;
5. in contravention of section 22(3) sentence 1, fails to submit an agreement or to submit it in timely manner;
6. charges rates without approval as required under section 30(1) or section 39(1) sentence 1;
7. in contravention of section 38(1) sentence 1 or 3 or section 39(3) sentence 4, fails to inform the Regulatory Authority of rates or rate measures, to inform it correctly, to inform it completely or to inform it in timely manner;
8. in contravention of section 47(1), fails to provide subscriber data, to provide them correctly, to provide them completely or to provide them in timely manner;
9. in contravention of section 50(3) para 4, fails to notify the Regulatory Authority, to notify it correctly, to notify it completely or to notify it in timely manner;
10. uses a frequency without frequency assignment as required under section 55(1) sentence 1;
11. exercises German rights to orbit or frequency usage without assignment of such rights as required under section 56(1) sentence 1;
12. contravenes an enforceable condition according to section 60(2) sentence 1;
13. contravenes an ordinance according to section 66(4) sentence 1 or an enforceable order issued by virtue of such ordinance, insofar as the ordinance refers to this administrative fines provision in respect of a particular offence;
14. in contravention of section 87(1) sentence 1 or section 110(1) sentence 2 or 3, fails to inform
or notify the Regulatory Authority, to inform or notify it correctly, to inform or notify it completely or to inform or notify it in timely manner;
15. in contravention of section 90(3), advertises transmitting equipment;
16. in contravention of section 95(2) or section 96(2) sentence 1 or subsection (3) sentence 1, uses data;
17. in contravention of section 96(2) sentence 2 or section 97(3) sentence 2, fails to erase data or to erase them in timely manner;
18. in contravention of section 106(2) sentence 2, fails to erase data and documents or to erase
them in timely manner;
19. in contravention of section 108(1) sentence 1, also in conjunction with an ordinance according to section 108(2) sentence 1 para 1, fails to provide access to emergency services or to provide it as prescribed;
20. in contravention of section 108(1) sentence 2 in conjunction with an ordinance according to

section 108(2) sentence 1 para 4, fails to transmit the data or information as referred to there or to transmit them in timely manner;

97

21. in contravention of section 109(3) sentence 2 or 4, fails to submit or to resubmit a security concept or to submit or to resubmit it in timely manner;

22. in contravention of section 110(1) sentence 1 para 1 in conjunction with an ordinance according to section 110(2) para 1 a), fails to provide a technical facility or to make organisational arrangements;

23. in contravention of section 110(1) sentence 1 para 2 b), fails to nominate a body as named there or to nominate it in timely manner;

24. in contravention of section 110(1) sentence 1 para 3, fails to demonstrate compliance or to demonstrate it in timely manner;

25. in contravention of section 110(1) sentence 1 para 4, fails to allow a re-check;

26. in contravention of section 110(1) sentence 1 para 5, fails to tolerate the installation or operation of equipment referred to there or to grant access to such equipment;

27. in contravention of section 110(5) sentence 3, fails to eliminate shortcomings or to eliminate

them in timely manner;

28. in contravention of section 110(6) sentence 1, fails to make available a network termination point, to make it available as prescribed or to make it available in timely manner;

29. in contravention of section 111(1) sentence 1, also in conjunction with sentence 2, or in contravention of section 111(1) sentence 3 or 4, fails to collect data or to collect them in timely manner, fails to store data or to store them in timely manner, fails to correct data or to correct them in timely manner or fails to erase data or to erase them in timely manner;

30. in contravention of section 111(2) sentence 1, also in conjunction with sentence 2, fails to collect data or to collect them in timely manner or fails to transmit data or to transmit them in timely manner;

31. in contravention of section 112(1) sentence 4, fails to ensure that the Regulatory Authority can retrieve data from customer data files;

32. in contravention of section 112(1) sentence 6, fails to ensure that no retrievals can come to his notice;

33. in contravention of section 113(1) sentence 1 or 2, section 114(1) sentence 1 or section 127(1) sentence 1, fails to provide information, to provide it correctly, to provide it completely or to provide it in timely manner;

34. in contravention of section 113(1) sentence 2 second half-sentence, transmits data; or

35. in contravention of section 113(1) sentence 4, fails to maintain silence.

(2) Such offences may be punishable by a fine not exceeding five hundred thousand euros in the cases of an offence according to subsection (1) para 4 a), paras 6, 10, 22, 27 and 31, by a

fine not exceeding three hundred thousand euros in the cases of an offence according to subsection (1) paras 16 to 18, 26, 29 and 34, by a fine not exceeding one hundred thousand euros in the cases of an offence according to subsection (1) para 4 b), paras 12, 13, 15, 19, 21
98
and 30, by a fine not exceeding fifty thousand euros in the cases of an offence according to subsection (1) paras 5, 7, 8, 9, 11, 20, 23 and 24, and by a fine not exceeding ten thousand euros in the other cases of offences according to subsection (1). The fine should exceed the economic benefit the offender has derived from the offence. Amounts as referred to in sentence 1 which are not sufficient for this may be exceeded.

(3) Administrative authority within the meaning of section 36(1) para 1 of the Administrative Offences Act shall be the Regulatory Authority.

PART 11

TRANSITIONAL AND FINAL PROVISIONS

Section 150

Transitional Provisions

(1) Determinations of market dominance made by the Regulatory Authority prior to the entry into force of this Act and the resulting obligations shall remain in effect until such time as they are replaced by new decisions taken in accordance with Part 2. This also applies when the determinations of market dominance merely constitute part of the statement of reasons for an administrative act. Sentence 1 applies accordingly with regard to obligations set out in sections 36, 37 and 39 second alternative of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120).

(2) Undertakings which have given notification under the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) that they provide telecommunications services or
are licensees shall, without prejudice to the obligation set out in section 144(1) sentence 1, not be subject to the notification requirement according to section 6.

(3) Existing frequency assignments, number allocations and rights of way granted under section 8 of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) shall remain in effect. The same applies to rights acquired beforehand entitling the holder to use frequencies.

(4) Where frequency usage and licence rights have been granted in markets in which competitive or comparative selection procedures have been carried out, rights thus granted and
obligations thus entered into shall continue. This applies, in particular, in respect of the obligation to admit service providers, applicable at the time the mobile licences were granted.

(5) Section 21(2) para 3 applies until 30 June 2008 subject to the proviso that wholesale line rental has to be made available only in conjunction with calls.

(6) Section 48(2) para 2 applies with regard to equipment placed on the market as from 1 January 2005.
(7) Until such time as a Frequency Usage Plan according to section 54 is issued, frequencies shall be assigned in accordance with the provisions of the applicable National Table
of Frequency Allocations.
(8) Section 62(1) to (3) do not apply to rights granted under section 2(1) of the Telecommunication Installations Act as published on 3 July 1989 (Federal Law Gazette Part I 99
page 1455) or to licences granted or frequencies assigned under sections 10, 11 and 47(5) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) for the period of validity specified for such licences and frequencies.
(9) Where Deutsche Telekom AG intends not to offer universal services as specified in section 78(2) to the full extent or to offer them under less favourable conditions than those specified in this Act, it shall notify the Regulatory Authority of such intentions one year prior to their taking effect.
(10) The Telecommunications Interception Ordinance of 22 January 2002 (Federal Law Gazette Part I page 458), last amended by Article 328 of the Ordinance of 25 November 2003 (Federal Law Gazette Part I page 2304) applies in place of the ordinance according to section 110(2) until such time as this ordinance has entered into force.
(11) The technical directive issued under section 11 of the Telecommunications Interception Ordinance as amended at the time of entry into force of section 110 applies in place of the technical directive according to section 110(3) until such time as this directive has been issued.
(12) In respect of contractual relationships existing on the date of entry into force of this provision, persons with obligations under section 112(1) shall enter data they have to hand as a
result of earlier data surveys without undue delay in customer data files according to section 112(1). In respect of contracts concluded after the entry into force of section 112, data which providers have not yet been able to include in a customer data file on account of the file structure used hitherto shall be included without undue delay following adaptation of the file. The
interface specification published by the Regulatory Authority under section 90(2) and (6) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) as amended at the time of the entry into force of section 112 applies in place of the technical directive according to section 112(3) sentence 3 until such time as this directive has been issued.
(13) The admissibility of appeals against court decisions shall be decided in accordance with the provisions applicable to date if the court decision is pronounced prior to the entry into force

of this Act or served ex officio instead of pronouncement.

(14) The provisions to date are applicable to motions submitted under section 99(2) of the Code of Administrative Court Procedure prior to the entry into force of this Act.

Section 151

Amendment of Other Legal Provisions

(1) The Code of Criminal Procedure as published on 7 April 1987 (Federal Law Gazette Part I pages 1047, 1319), last amended by Article 4(22) of the Act of 5 May 2004 (Federal Law Gazette Part I page 718) shall be amended as follows–

in section 100b(3) sentence 2 for the words "section 88 of the Telecommunications Act" there shall be substituted the words "section 110 of the Telecommunications Act".

(2) The Article 10 Act of 26 June 2001 (Federal Law Gazette Part I pages 1254, 2298), last amended by Article 4(6) of the Act of 5 May 2004 (Federal Law Gazette Part I page 718) shall be amended as follows–

100

1. in section 2(1) sentence 4 for the words "section 88 of the Telecommunications Act" there shall be substituted the words "section 110 of the Telecommunications Act";

2. section 20 shall read as follows–

"Section 20

Compensation

Bodies authorised under section 1(1) shall pay compensation for services according to section 2(1), the level of which shall be determined, in respect of measures for

a) postal intercepts, in accordance with section 17a of the Reimbursement of Witnesses and Experts Act; and

b) telecommunications intercepts, in accordance with the ordinance referred to in section 110(9)."

(3) Section 17a(1) para 3 subpara (1) second and third half-sentences and subsection (6) of the Reimbursement of Witnesses and Experts Act as published on 1 October 1969 (Federal Law

Gazette Part I page 1756), last amended by Article 1(5) of the Act of 22 February 2002 (Federal

Law Gazette Part I page 981) shall expire on the date of the entry into force of the ordinance according to section 110(9).

Section 152

Entry into Force, Expiry

(1) Subject to sentence 2, this Act shall enter into force on the day following its promulgation. Section 43(a) and (b), section 96(1) para 9 a) to 9 f) in conjunction with subsection (2) sentence 1 and section 97(6) and (7) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120), last amended by Article 4(73) of the Act of 5 May 2004

(Federal
Law Gazette Part I page 718) remain applicable in the version valid until the entry into force of this Act until such time as the ordinance according to section 66(4) of this Act has been issued. In respect of section 43b(2) this applies subject to the proviso that the pricing information requirement is no longer restricted to calls from the fixed network as from 1 August 2004.
(2) The Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120), last amended by Article 4(73) of the Act of 5 May 2004 (Federal Law Gazette Part I page 718), the Television Signals Transmission Act of 14 November 1997 (Federal Law Gazette Part I page 2710), last amended by Article 222 of the Ordinance of 25 November 2003 (Federal Law Gazette Part I page 2304), the Telecommunications Rates Regulation Ordinance of 1 October 1996 (Federal Law Gazette Part I page 1492), the Network Access Ordinance of 23 October 1996 (Federal Law Gazette Part I page 1568), the Telecommunications Universal Service Ordinance of 30 January 1997 (Federal Law Gazette Part I page 141), section 4 of the Telecommunications Customer Protection Ordinance of 11 December 1997 (Federal Law Gazette Part I page 2910), last amended by the Ordinance of 20 August 2002 (Federal Law Gazette Part I page 3365), the Telecommunications Data Protection Ordinance of 18 December
2000 (Federal Law Gazette Part I page 1740), amended by Article 2 of the Act of 9 August 2003
(Federal Law Gazette Part I page 1590), the Frequency Assignment Ordinance of 26 April 2001
(Federal Law Gazette Part I page 829) and the Telecommunications Licence Fees Ordinance of
9 September 2002 (Federal Law Gazette Part l page 3542) shall expire on the day following the

promulgation of this Act.

附錄五、德國巴伐利亞邦個人資料保護法

Bayerisches Datenschutzgesetz
(BayDSG)
Vom 23. Juli 1993
Zum Ausgangs- oder Titeldokument
Fundstelle: GVBl 1993, S. 498
Stand: letzte berücksichtigte Änderung: mehrfach geänd. (G v. 20.7.2011, 307)

Der Landtag des Freistaates Bayern hat das folgende Gesetz beschlossen, das nach Anhörung des Senats hiermit bekanntgemacht wird:

Inhaltsübersicht

Erster Abschnitt
Allgemeine Bestimmungen

Art. 1
Zweck des Gesetzes
Zweck dieses Gesetzes ist es, die einzelnen davor zu schützen, daß sie bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch öffentliche Stellen in unzulässiger Weise in ihrem Persönlichkeitsrecht beeinträchtigt werden.

Art. 2
Anwendungsbereich des Gesetzes
(1) Die Vorschriften dieses Gesetzes - ausgenommen der Sechste Abschnitt - gelten für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Behörden, Gerichte und sonstige öffentliche Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts.
(2) 1 Die Vorschriften dieses Gesetzes gelten auch für Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen - ungeachtet der Beteiligung nicht-öffentlicher Stellen -
1.
eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts beteiligt sind, oder
2.
außer einer oder mehrerer der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts auch eine oder mehrere der in § 2 Abs. 1 des Bundesdatenschutzgesetzes genannten juristischen Personen des öffentlichen Rechts

oder Vereinigungen beteiligt sind, wenn sie keine öffentlichen Stellen des Bundes gemäß § 2 Abs. 3 des Bundesdatenschutzgesetzes sind.
2 Beteiligt sich eine Vereinigung des privaten Rechts, auf die dieses Gesetz nach Satz 1 Anwendung findet, an einer weiteren Vereinigung des privaten Rechts, so findet Satz 1 entsprechende Anwendung.
(3) Für personenbezogene Daten in automatisierten Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten von den Vorschriften dieses Gesetzes nur die Art. 5, 7, 17 Abs. 4, Art. 25, 29 bis 31, 32 Abs. 1 bis 3, Art. 33 und 37.
(4) Die Vorschriften dieses Gesetzes gelten nicht für die Ausübung des Begnadigungsrechts.
(5) Die Vorschriften dieses Gesetzes gelten für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird.
(6) In bezug auf Gerichte und den Obersten Rechnungshof gelten der Vierte und Fünfte Abschnitt sowie Art. 9 nur, soweit sie in Verwaltungsangelegenheiten tätig werden.
(7) Soweit besondere Rechtsvorschriften über den Datenschutz oder über Verfahren der Rechtspflege auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.
(8) Die Vorschriften dieses Gesetzes gehen denen des Bayerischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten erhoben, verarbeitet oder genutzt werden.
(9) Dieses Gesetz läßt die Verpflichtung zur Wahrung der in § 203 Abs. 1 des Strafgesetzbuchs genannten Geheimnisse unberührt.

Art. 3
Öffentliche Stellen, die am Wettbewerb teilnehmen
(1) 1 Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten für sie sowie für ihre Zusammenschlüsse und Verbände die Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts. 2 Art. 2 Abs. 7 bleibt unberührt. 3 Für die Durchführung und die Kontrolle des Datenschutzes gelten an Stelle der §§ 4d bis 4g und 38 des Bundesdatenschutzgesetzes die Art. 9 und 25 bis 33.
(2) 1 Soweit öffentlich-rechtliche Versicherungsunternehmen am Wettbewerb teilnehmen, gelten für sie die Vorschriften des Bundesdatenschutzgesetzes, die auf privatrechtliche Versicherungsunternehmen anzuwenden sind. 2 Für öffentlich-rechtliche Kreditinstitute sowie für ihre Zusammenschlüsse und Verbände

gelten die Vorschriften des Bundesdatenschutzgesetzes, die auf privatrechtliche Kreditinstitute anzuwenden sind. 3 Art. 2 Abs. 7 bleibt unberührt.
(3) Die Anstalt für Kommunale Datenverarbeitung in Bayern unterliegt den Vorschriften dieses Gesetzes auch, soweit sie am Wettbewerb teilnimmt.

Art. 4
Begriffsbestimmungen
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene).
(2) 1 Öffentliche Stellen im Sinn dieses Gesetzes sind die in Art. 2 Abs. 1 und 2 bezeichneten Stellen und Vereinigungen. 2 Öffentliche Stellen im Sinn der Art. 18 und 24 sind darüber hinaus die öffentlichen Stellen des Bundes gemäß § 2 des Bundesdatenschutzgesetzes und der anderen Länder nach § 2 des Bundesdatenschutzgesetzes und der jeweils maßgeblichen Landesdatenschutzgesetze. 3 Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter Satz 1 oder 2 fallen. 4 Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle.
(3) 1 Eine Datei ist
1.
eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei) oder
2.
jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei).
2 Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.
(4) 1 Akten sind alle sonstigen amtlichen oder dienstlichen Zwecken dienenden Unterlagen; dazu zählen auch Bild- und Tonträger. 2 Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.
(5) Erheben ist das Beschaffen von Daten über Betroffene.
(6) 1 Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. 2 Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
1.
Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,

2.
Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3.
Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an Dritte in der Weise, daß
a)
die Daten durch die speichernde Stelle an Dritte weitergegeben werden oder
b)
Dritte Daten einsehen oder abrufen, die von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehalten werden,
4.
Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5.
Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.
(7) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt, insbesondere die Weitergabe von Daten innerhalb der speichernden Stelle an Teile derselben Stelle mit anderen Aufgaben oder anderem örtlichem Zuständigkeitsbereich.
(8) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
(9) Speichernde Stelle ist jede öffentliche Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt.
(10) 1 Dritte sind alle Personen oder Stellen außerhalb der speichernden Stelle.
2 Dritte sind nicht die Betroffenen sowie diejenigen Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

Art. 5
Datengeheimnis
1 Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). 2 Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Art. 6
Erhebung, Verarbeitung oder Nutzung
personenbezogener Daten im Auftrag

(1) 1 Werden personenbezogene Daten durch andere Stellen im Auftrag erhoben, verarbeitet oder genutzt, bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. 2 Die im Zweiten Abschnitt genannten Rechte sind ihm gegenüber geltend zu machen.

(2) 1 Auftragnehmer sind unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. 2 Der Auftrag ist schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. 3 Der Auftraggeber hat sich soweit erforderlich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen.

(3) 1 Ist eine öffentliche Stelle Auftragnehmer, so gelten für sie nur die Art. 5, 7, 25, 29 bis 31, 32 Abs. 1 bis 3, Art. 33 und 37. 2 Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. 3 Ist er der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) 1 Die Absätze 1 bis 3 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen durch andere Stellen vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. 2 Ist eine schriftliche Auftragserteilung nach Absatz 2 Satz 2 nicht möglich, so ist diese unverzüglich nachzuholen.

Art. 7
Technische und organisatorische Maßnahmen

(1) 1 Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. 2 Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1.
Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene

Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2.
zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3.
die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4.
zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
5.
zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6.
zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
7.
zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8.
zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9.
zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
10.
die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Art. 8
Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten an Dritte durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.
(2) 1 Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. 2 Hierzu haben sie schriftlich festzulegen:
1.
die Aufgaben, zu deren Erfüllung personenbezogene Daten verarbeitet werden und die Rechtsgrundlage der Verarbeitung,
2.
die Datenempfänger,
3.
die Art der zu übermittelnden Daten,
4.
die nach Art. 7 erforderlichen technischen und organisatorischen Maßnahmen.
(3) 1 Die Zulässigkeit des einzelnen Abrufs beurteilt sich nach den für die Erhebung und Übermittlung geltenden Vorschriften. 2 Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. 3 Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlaß besteht. 4 [1] Die speichernde Stelle hat zu gewährleisten, daß die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. 5 [1] Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufs oder der Übermittlung des Gesamtbestands.
(4) Die Absätze 1 bis 3 gelten nicht für den Abruf aus Datenbeständen, die allen, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen.
Fußnoten
[1])
Absatz 3 Satz 4 in Kraft mit Wirkung vom 1. März 1995
[1])
Absatz 3 Satz 5 in Kraft mit Wirkung vom 1. März 1995

Zweiter Abschnitt
Schutzrechte

Art. 9
Anrufung des Landesbeauftragten für den Datenschutz

Jeder kann sich an den Landesbeauftragten für den Datenschutz mit dem Vorbringen wenden, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen in seinen Rechten verletzt worden zu sein.

Art. 10
Auskunft und Benachrichtigung
(1) 1 Die speichernde Stelle hat den Betroffenen auf Antrag Auskunft zu erteilen über
1.
die zur Person gespeicherten Daten,
2.
den Zweck und die Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung,
3.
die Herkunft der Daten und die Empfänger übermittelter Daten, soweit diese Angaben gespeichert sind,
4.
die Empfänger regelmäßiger Datenübermittlungen,
5.
im Fall des Art. 6 Abs. 1 bis 3 die Auftragnehmer,
6.
im Fall des Art. 15 Abs. 6 den strukturierten Ablauf der automatisierten Verarbeitung oder Nutzung seiner Daten und die dabei herangezogenen Entscheidungskriterien.
2 Dies gilt nicht für personenbezogene Daten, die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.
(2) Für die Auskunft werden Kosten nicht erhoben, es sei denn, daß mit der Auskunftserteilung ein besonderer Verwaltungsaufwand verbunden ist.
(3) 1 In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. 2 Sind die personenbezogenen Daten nicht in automatisierten Dateien gespeichert, so wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. 3 Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.
(4) 1 Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Behörden der Staatsanwaltschaft, an Polizeidienststellen, an Behörden der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, an Verfassungsschutzbehörden, an den Bundesnachrichtendienst,

an den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, an andere Behörden des Bundesministeriums der Verteidigung, so ist sie nur mit Zustimmung dieser Stellen zulässig. 2 Für die Versagung der Zustimmung durch Behörden des Freistaates Bayern gilt Absatz 5 entsprechend.

(5) Die Auskunftserteilung unterbleibt, soweit

1.
die Auskunft die ordnungsgemäße Erfüllung von Aufgaben der Gefahrenabwehr oder die Verfolgung von Straftaten, Ordnungswidrigkeiten oder berufsrechtlichen Vergehen gefährden würde,

2.
die Auskunft die öffentliche Sicherheit oder Ordnung, die Sicherheit des Staates, die Landesverteidigung oder ein wichtiges wirtschaftliches oder finanzielles Interesse des Freistaates Bayern, eines anderen Landes, des Bundes oder der Europäischen Union - einschließlich Währungs-, Haushalts- und Steuerangelegenheiten - gefährden würde oder

3.
personenbezogene Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen Dritter geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(6) 1 Die Ablehnung der Auskunftserteilung durch Behörden der Staatsanwaltschaft, durch Justizvollzugsanstalten und Behörden der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, bedarf keiner Begründung. 2 Die Ablehnung der Auskunftserteilung durch sonstige öffentliche Stellen bedarf keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. 3 In den Fällen der Sätze 1 und 2 ist der Betroffene darauf hinzuweisen, daß er sich an den Landesbeauftragten für den Datenschutz wenden kann.

(7) 1 Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die Staatskanzlei, die Staatsministerien, die sonstigen obersten Dienststellen des Staates oder die obersten Aufsichtsbehörden jeweils für ihren Zuständigkeitsbereich im Einzelfall feststellen, daß dadurch die Sicherheit des Freistaates Bayern, eines anderen Landes oder des Bundes gefährdet würde. 2 Die Mitteilung des Landesbeauftragten für den Datenschutz an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft

zustimmt.
(8) 1 Werden in einer Datei zur Person Betroffener Daten gespeichert, die weder von den Betroffenen mit ihrer Kenntnis erhoben noch von ihnen mitgeteilt worden sind, so hat die speichernde Stelle die Betroffenen von der Tatsache der Speicherung zu benachrichtigen und dabei die Art der Daten sowie die Zweckbestimmung und die Rechtsgrundlage der Speicherung zu nennen; Absatz 1 Satz 2 gilt entsprechend. 2 Die Benachrichtigung erfolgt zum Zeitpunkt der Speicherung oder im Fall einer beabsichtigten Übermittlung spätestens mit deren Durchführung. 3 Dienen die Daten der Erstellung einer beabsichtigten Mitteilung an Betroffene, kann die Benachrichtigung mit dieser Mitteilung verbunden werden. 4 Die Sätze 1 bis 3 gelten nicht, wenn
1.
eine Rechtsvorschrift die Speicherung der personenbezogenen Daten ausdrücklich vorsieht,
2.
die Betroffenen auf andere Weise Kenntnis von der Tatsache der Speicherung erlangt haben, oder
3.
die Benachrichtigung der Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.
5 Absatz 5 gilt entsprechend.
(9) 1 Die Absätze 1 bis 8 gelten für Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden. 2 Absatz 6 Satz 3 und Absatz 7 gelten für den Obersten Rechnungshof nur, soweit er in Verwaltungsangelegenheiten tätig wird. 3 Absatz 8 gilt nicht für Behörden der Staatsanwaltschaft, für Justizvollzugsanstalten, für Führungsaufsichtsstellen und für Stellen der Gerichts- und Bewährungshilfe.

Art. 11
Berichtigung
1 Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. 2 Wird bei personenbezogenen Daten in Akten festgestellt, daß sie unrichtig sind, oder wird ihre Richtigkeit vom Betroffenen bestritten, so ist dies in den Akten zu vermerken oder auf sonstige Weise festzuhalten.

Art. 12
Löschung, Sperrung
(1) Personenbezogene Daten in Dateien sind zu löschen, wenn
1.

ihre Speicherung unzulässig ist oder
2.
ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.
(2) Personenbezogene Daten in Dateien sind zu sperren, wenn
1.
ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt oder
2.
eine Löschung nach Absatz 1 wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.
(3) 1 Personenbezogene Daten in Akten sind zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, daß ihre Speicherung unzulässig ist. 2 Stellt die speichernde Stelle im Einzelfall fest, daß der gesamte Akt ausschließlich unzulässig gespeicherte Daten enthält, so sind die personenbezogenen Daten zu löschen.
(4) 1 Personenbezogene Daten in Akten sind ferner zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, daß ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden. 2 Stellt die speichernde Stelle im Einzelfall fest, daß der gesamte Akt zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist, sind die personenbezogenen Daten zu löschen.
(5) An die Stelle einer Löschung tritt eine Sperrung, wenn Grund zu der Annahme besteht, daß durch eine Löschung die schutzwürdigen Interessen des Betroffenen beeinträchtigt würden.
(6) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn
1.
es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich oder zur Wahrnehmung von Aufsichts- oder Kontrollbefugnissen oder zur Rechnungsprüfung erforderlich ist und
2.
die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.
(7) Daten, die wegen Unzulässigkeit der Speicherung gesperrt sind, dürfen ohne Einwilligung des Betroffenen nicht mehr übermittelt oder genutzt werden, es sei denn, daß dies zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen oder zur

Rechnungsprüfung erforderlich ist.
(8) Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, ist eine Löschung erst zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten worden sind und von diesem nicht als archivwürdig übernommen worden sind oder über die Übernahme nicht fristgerecht (Art. 6 Abs. 4 Bayerisches Archivgesetz oder auf Grund der entsprechenden Festlegungen der Träger von Archiven sonstiger öffentlicher Stellen nach Abschnitt III des Bayerischen Archivgesetzes) entschieden worden ist.

Art. 13
Benachrichtigung nach Datenübermittlung
Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen diese Daten übermittelt wurden, es sei denn, dass die Verständigung sich als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

Art. 14
Schadensersatz
(1) 1 Fügt eine öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen zum Ersatz dieses Schadens verpflichtet. 2 Die Ersatzpflicht entfällt, soweit die öffentliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.
(2) 1 Fügt eine öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist sie dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet. 2 Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen. 3 Der Anspruch ist insgesamt bis zu einem Betrag in Höhe von 125.000 Euro begrenzt. 4 Ist auf Grund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 125.000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht. 5 Sind bei einer Datei mehrere Stellen speicherungsberechtigt und sind Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(3) Mehrere Ersatzpflichtige haften als Gesamtschuldner.
(4) 1 Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, so gilt § 254 des Bürgerlichen Gesetzbuchs. 2 Auf die Verjährung finden die Vorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.
(5) Vorschriften, nach denen Ersatzpflichtige in weiterem Umfang als nach dieser Vorschrift haften oder nach denen andere für den Schaden verantwortlich sind, bleiben unberührt.
(6) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

Dritter Abschnitt
Rechtsgrundlagen der Datenerhebung, -verarbeitung und -nutzung

Art. 15
Zulässigkeit der Datenerhebung,
-verarbeitung und -nutzung
(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, wenn
1.
dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder
2.
der Betroffene eingewilligt hat.
(2) Wird eine Einwilligung eingeholt, so sind Betroffene auf den Zweck der Erhebung, Verarbeitung oder Nutzung, auf die Empfänger vorgesehener Übermittlungen sowie unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern können.
(3) 1 Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. 2 Im Bereich der wissenschaftlichen Forschung liegen solche besonderen Umstände auch dann vor, wenn der bestimmte Forschungszweck durch die Schriftform erheblich beeinträchtigt würde. 3 In diesem Fall sind der Hinweis gemäß Absatz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des wissenschaftlichen Forschungszwecks ergibt, schriftlich festzuhalten.
(4) Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.
(5) 1 Widersprechen Betroffene schriftlich einer bestimmten Erhebung, Verarbeitung oder Nutzung und ergibt eine Abwägung im Einzelfall, dass das schutzwürdige Interesse eines Betroffenen wegen seiner besonderen persönlichen Situation das

Interesse der öffentlichen Stelle an der Erhebung, Verarbeitung oder Nutzung dieser Daten überwiegt, so dürfen insoweit personenbezogene Daten nicht erhoben, verarbeitet oder genutzt werden. 2 Satz 1 gilt nicht, wenn eine Rechtsvorschrift die Erhebung, Verarbeitung oder Nutzung anordnet.

(6) 1 Entscheidungen, die für Betroffene eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung oder Nutzung zum Zweck der Bewertung einzelner Persönlichkeitsmerkmale gestützt werden. 2 Satz 1 gilt nicht, soweit

1.
eine Rechtsvorschrift dies ausdrücklich vorsieht,

2.
damit dem Begehren der Betroffenen stattgegeben wird, oder

3.
den Betroffenen die Tatsache einer Entscheidung nach Satz 1 mitgeteilt wird und ihnen Gelegenheit gegeben wird, ihren Standpunkt geltend zu machen; die öffentliche Stelle ist verpflichtet, nach Eingang der Stellungnahme ihre Entscheidung erneut zu prüfen.

(7) 1 Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben, ist über die Vorschriften dieses Abschnitts hinaus nur zulässig, wenn

1.
eine Rechtsvorschrift dies ausdrücklich vorsieht,

2.
die Betroffenen eingewilligt haben, wobei sich die Einwilligung ausdrücklich auf diese Daten beziehen muss,

3.
es zum Schutz lebenswichtiger Interessen Betroffener oder Dritter erforderlich ist, sofern die Betroffenen aus physischen oder rechtlichen Gründen außerstande sind, ihre Einwilligung zu geben,

4.
es sich um Daten handelt, die Betroffene offenkundig öffentlich gemacht haben,

5.
es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung erforderlich ist,

6.
es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder

zum Vollzug von Strafen oder Maßnahmen im Sinn des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinn des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
7.
es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,
8.
es erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts Rechnung zu tragen, oder
9.
es zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.
2 Art. 20 bleibt unberührt.
(8) 1 Die Absätze 5 bis 7 gelten für Strafgerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden. 2 Die Absätze 5 bis 7 gelten nicht für Behörden der Staatsanwaltschaft, für Justizvollzugsanstalten, für Führungsaufsichtsstellen und für Stellen der Gerichts- und Bewährungshilfe.

Art. 16
Erhebung
(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist.
(2) 1 Personenbezogene Daten, die nicht aus allgemein zugänglichen Quellen entnommen werden, sind beim Betroffenen mit seiner Kenntnis zu erheben.
2 Personenbezogene Daten dürfen bei Dritten nur erhoben werden, wenn
1.
eine Rechtsvorschrift eine solche Erhebung vorsieht oder zwingend voraussetzt,
2.
a)
die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder im Einzelfall eine solche

Erhebung erforderlich macht oder
b)
die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde oder keinen Erfolg verspricht
und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden, oder
3.
die Daten nach Art. 18 Abs. 1 oder einer anderen Rechtsvorschrift von einer öffentlichen Stelle an die erhebende Stelle übermittelt werden dürfen.
3 Werden Daten beim Betroffenen ohne seine Kenntnis erhoben, gelten die Nummern 1 und 2 Buchst. a des Satzes 2 entsprechend.
(3) 1 Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. 2 Werden sie beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. 3 Auf Verlangen ist der Betroffene über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären. 4 Bei einer Datenerhebung auf schriftlichem Weg ist die Rechtsvorschrift stets anzugeben.
(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

Art. 17
Verarbeitung und Nutzung
(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn
1.
es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und
2.
es für die Zwecke erfolgt, für die die Daten erhoben worden sind; ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.
(2) Abweichend von Absatz 1 Nr. 2 ist das Speichern, Verändern oder Nutzen personenbezogener Daten für andere Zwecke zulässig, wenn
1.
eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder die Beteiligung

von Trägern öffentlicher Belange bestimmt,
2.
der Betroffene eingewilligt hat,
3.
offensichtlich ist, daß es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, daß er in Kenntnis des anderen Zwecks seine Einwilligung hierzu verweigern würde,
4.
die Daten für den anderen Zweck auf Grund einer durch Rechtsvorschrift festgelegten Auskunfts- oder Meldepflicht beim Betroffenen erhoben werden dürfen und der Betroffene dieser Pflicht nicht nachgekommen ist,
5.
Angaben des Betroffenen überprüft werden sollen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
6.
Angaben des Betroffenen zur Erlangung von finanziellen Leistungen öffentlicher Stellen mit anderen derartigen Angaben verglichen werden sollen,
7.
es zur Entscheidung über die Verleihung von staatlichen Orden oder Ehrenzeichen oder von sonstigen staatlichen Ehrungen erforderlich ist,
8.
die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle die Daten veröffentlichen dürfte,
9.
es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit oder Ordnung oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,
10.
es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinn des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinn des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist oder
11.
es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit

unverhältnismäßigem Aufwand erreicht werden kann.
(3) 1 Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- oder Kontrollbefugnissen, der Erstellung von Geschäftsstatistiken, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen für die speichernde Stelle oder der Prüfung oder Wartung automatisierter Verfahren der Datenverarbeitung dient. 2 Das gilt auch für die Verarbeitung und Nutzung zu Ausbildungs- oder Prüfungszwecken durch die speichernde Stelle, soweit nicht offensichtlich überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.
(4) Personenbezogene Daten in automatisierten Dateien im Sinn des Art. 2 Abs. 3 sowie personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verarbeitet oder genutzt werden.
(5) 1 Sind mit personenbezogenen Daten, die nach den Absätzen 1 bis 3 durch Weitergabe innerhalb der speichernden Stelle genutzt werden dürfen, weitere personenbezogene Daten des Betroffenen oder Dritter in Akten so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Weitergabe auch dieser Daten zulässig, soweit nicht offensichtlich überwiegende schutzwürdige Interessen des Betroffenen oder Dritter entgegenstehen. 2 Eine darüber hinausgehende Nutzung oder Verarbeitung dieser Daten ist nur zulässig, soweit die Daten auch hierfür hätten weitergegeben werden dürfen.

Art. 18
Datenübermittlung an öffentliche Stellen
(1) Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden Stelle liegenden Aufgaben erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 zulässig wäre.
(2) 1 Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. 2 Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. 3 In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht. 4 Art. 8 Abs. 3 bleibt unberührt.
(3) 1 Die empfangende Stelle darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt worden sind. 2 Eine Verarbeitung oder Nutzung für andere Zwecke ist nur zulässig, wenn für diese

Zwecke eine Nutzung nach Art. 17 Abs. 2 bis 4 zulässig wäre.
(4) 1 Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder Dritter in Akten so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht offensichtlich überwiegende schutzwürdige Interessen des Betroffenen oder Dritter entgegenstehen. 2 Eine Nutzung oder Verarbeitung dieser Daten durch den Empfänger ist nur zulässig, soweit die Daten auch hierfür hätten übermittelt werden dürfen.

Art. 19
Datenübermittlung an nicht-öffentliche Stellen
(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn
1.
sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 zulassen würden oder
2.
die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.
(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.
(3) 1 In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. 2 Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt, wenn die Unterrichtung wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen nicht geboten erscheint, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Freistaates Bayern, eines anderen Landes oder des Bundes Nachteile bereiten würde.
(4) 1 Die nicht-öffentliche Stelle darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt worden sind. 2 Sie ist von der übermittelnden Stelle darauf hinzuweisen. 3 Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 auch für die anderen Zwecke zulässig wäre und die übermittelnde Stelle zugestimmt hat.

Art. 20

Datenübermittlung an öffentlich-rechtliche
Religionsgesellschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung von Art. 18 zulässig, wenn sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen sind.

Art. 21
Datenübermittlung an Stellen im Ausland

(1) Für die Übermittlung personenbezogener Daten an öffentliche Stellen innerhalb der Mitgliedstaaten der Europäischen Union oder der anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder an Organe und Einrichtungen der Europäischen Union gelten Art. 18 Abs. 1, Art. 22 und 23 sowie für die Übermittlung an nicht-öffentliche Stellen innerhalb der Mitgliedstaaten der Europäischen Union oder der anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum Art. 19 Abs. 1 und 3, soweit nicht besondere Rechtsvorschriften anzuwenden sind.

(2) 1 Für die Übermittlung personenbezogener Daten an Stellen außerhalb der Mitgliedstaaten der Europäischen Union und der anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum sowie an über- und zwischenstaatliche Stellen gelten Art. 19 Abs. 1 und 3, Art. 22 und 23 entsprechend nach Maßgabe der Sätze 2 bis 5, soweit nicht besondere Rechtsvorschriften anzuwenden sind. 2 Die Datenübermittlung ist nur zulässig, wenn das Drittland oder die über- oder zwischenstaatliche Stelle ein angemessenes Datenschutzniveau gewährleistet. 3 Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei Datenübermittlungen von Bedeutung sind; insbesondere werden die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung oder Nutzung, das Herkunfts- und das Endbestimmungsland, die in dem Drittland geltenden Rechtsvorschriften sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt. 4 Ist kein angemessenes Datenschutzniveau gewährleistet, so ist die Übermittlung nur zulässig, wenn

1.
die Betroffenen ihre Einwilligung gegeben haben,
2.
die Übermittlung für die Erfüllung eines Vertrags zwischen der übermittelnden Stelle und den Betroffenen oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung der Betroffenen getroffen worden sind, erforderlich ist,

3.
die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse Betroffener von der übermittelnden Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4.
die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
5.
die Übermittlung für die Wahrung lebenswichtiger Interessen Betroffener erforderlich ist,
6.
die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind oder
7.
die empfangende Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; diese Garantien können sich insbesondere aus Vertragsklauseln ergeben.
5 Datenübermittlungen, die nach Satz 4 Nr. 7 vorgenommen werden, sind dem Staatsministerium des Innern mitzuteilen.
(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.
(4) Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie ihm übermittelt werden.

Art. 21a
Videobeobachtung und Videoaufzeichnung (Videoüberwachung)
(1) 1 Mit Hilfe von optisch-elektronischen Einrichtungen sind die Erhebung (Videobeobachtung) und die Speicherung (Videoaufzeichnung) personenbezogener Daten zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist,
1.
um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe

aufhalten, oder
2.
um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Dienstgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen
zu schützen. 2 Es dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.
(2) Die Videoüberwachung und die erhebende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
(3) Die Daten dürfen für den Zweck verarbeitet und genutzt werden, für den sie erhoben worden sind, für einen anderen Zweck nur, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.
(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über die Tatsache der Speicherung entsprechend Art. 10 Abs. 8 zu benachrichtigen.
(5) Die Videoaufzeichnungen und daraus gefertigte Unterlagen sind spätestens drei Wochen nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.
(6) 1 Art. 26 bis 28 gelten für die Videoaufzeichnung entsprechend. 2 Öffentliche Stellen haben ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz einer Videoaufzeichnung neben den in Art. 26 Abs. 3 Satz 1 genannten Beschreibungen die räumliche Ausdehnung und Dauer der Videoaufzeichnung, die Maßnahmen nach Abs. 2 und die vorgesehenen Auswertungen mitzuteilen.

Art. 22
Zweckbindung bei personenbezogenen Daten, die
einem Berufs- oder besonderen Amtsgeheimnis unterliegen
1 Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Person oder Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der speichernden Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. 2 Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn sie von der zur Verschwiegenheit verpflichteten Person oder Stelle auch für diesen Zweck übermittelt werden dürften und die zur Verschwiegenheit verpflichtete Person oder Stelle in die Zweckänderung eingewilligt hat. 3 Die Übermittlung an eine nicht-öffentliche Stelle ist darüber hinaus nur zulässig,

wenn die zur Verschwiegenheit verpflichtete Person oder Stelle eingewilligt hat.

Art. 23
Verarbeitung und Nutzung personenbezogener Daten
durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.
(2) Die Übermittlung personenbezogener Daten an andere als öffentliche Stellen für Zwecke der wissenschaftlichen Forschung ist nur zulässig, wenn diese sich verpflichten, übermittelte Daten nicht für andere Zwecke zu verarbeiten oder zu nutzen und die Vorschriften der Absätze 3 und 4 einzuhalten.
(3) 1 Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. 2 Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. 3 Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.
(4) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn der Betroffene eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist.

Art. 24
Rechtsverordnungsermächtigung
für Datenübermittlungen

1 Die Staatsregierung kann durch Rechtsverordnung für bestimmte Sachgebiete die Voraussetzungen näher regeln, unter denen personenbezogene Daten an öffentliche Stellen und an nicht-öffentliche Stellen übermittelt werden dürfen. 2 Dabei sind die schutzwürdigen Belange der Betroffenen, berechtigte Interessen Dritter und die Belange einer wirtschaftlichen und zweckmäßigen Verwaltung miteinander abzuwägen. 3 In der Rechtsverordnung sind die für die Übermittlung bestimmten Daten, deren Empfänger und der Zweck der Übermittlung zu bezeichnen.

Vierter Abschnitt
Durchführung des Datenschutzes
bei öffentlichen Stellen

Art. 25 [1]
Sicherstellung des Datenschutzes, behördliche Datenschutzbeauftragte
(1) Die Staatskanzlei, die Staatsministerien und die sonstigen obersten Dienststellen des Staates, die Gemeinden, die Gemeindeverbände und die sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts sowie die privatrechtlichen Vereinigungen, auf die dieses Gesetz gemäß Art. 2 Abs. 2 Anwendung findet, haben für ihren Bereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.
(2) 1 Öffentliche Stellen, die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, haben einen ihrer Beschäftigten zum behördlichen Datenschutzbeauftragten zu bestellen. 2 Mehrere öffentliche Stellen können gemeinsam einen ihrer Beschäftigten bestellen; bei Staatsbehörden kann die Bestellung auch durch eine höhere Behörde erfolgen.
(3) 1 Die behördlichen Datenschutzbeauftragten sind in dieser Eigenschaft der Leitung der öffentlichen Stelle oder deren ständigen Vertretung unmittelbar zu unterstellen; bei obersten Dienstbehörden können sie auch dem Ministerialdirektor (Amtschef), in Gemeinden einem berufsmäßigen Gemeinderatsmitglied unterstellt werden. 2 Sie sind in ihrer Eigenschaft als behördliche Datenschutzbeauftragte weisungsfrei. 3 Sie können sich in Zweifelsfällen unmittelbar an den Landesbeauftragten für den Datenschutz wenden. 4 Sie dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. 5 Sie sind im erforderlichen Umfang von der Erfüllung sonstiger dienstlicher Aufgaben freizustellen. 6 Die Beschäftigten öffentlicher Stellen können sich in Angelegenheiten des Datenschutzes an ihre behördlichen Datenschutzbeauftragten wenden.
(4) 1 Die behördlichen Datenschutzbeauftragten haben die Aufgabe, auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz in der öffentlichen Stelle hinzuwirken. 2 Sie können die zur Überwachung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz erforderliche Einsicht in Dateien und Akten der öffentlichen Stelle nehmen, soweit nicht gesetzliche Regelungen entgegenstehen; sie dürfen Akten mit personenbezogenen Daten, die dem Arztgeheimnis unterliegen, Akten über die Sicherheitsüberprüfung und nicht in Dateien geführte Personalakten nur mit Einwilligung der Betroffenen einsehen. 3 Sie sind zur Verschwiegenheit über Personen verpflichtet, die ihnen in ihrer Eigenschaft als behördliche Datenschutzbeauftragte Tatsachen anvertraut haben, sowie über diese Tatsachen selbst, soweit sie nicht davon durch diese Personen befreit werden.
Fußnoten
[1])
Art. 25 in Kraft mit Wirkung vom 1. März 2001

Art. 26 [1]
Datenschutzrechtliche Freigabe
automatisierter Verfahren

(1) 1 Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf der vorherigen schriftlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle. 2 Eine datenschutzrechtliche Freigabe nach Satz 1 ist nicht erforderlich für Verfahren, welche durch den Vorstand der Anstalt für Kommunale Datenverarbeitung in Bayern bereits datenschutzrechtlich freigegeben worden sind, soweit diese Verfahren unverändert übernommen werden; das Gleiche gilt bei öffentlichen Stellen des Freistaates Bayern für Verfahren, welche durch das fachlich zuständige Staatsministerium oder die von ihm ermächtigte öffentliche Stelle für den landesweiten Einsatz datenschutzrechtlich freigegeben worden sind. 3 Für wesentliche Änderungen von Verfahren gelten die Sätze 1 und 2 entsprechend.

(2) Die datenschutzrechtliche Freigabe hat folgende Angaben zu enthalten:

1.Bezeichnung des Verfahrens,
2.Zweck und Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung,
3.Art der gespeicherten Daten,
4. Kreis der Betroffenen,
5.Art der regelmäßig zu übermittelnden Daten und deren Empfänger,
6.Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung,
7.verarbeitungs- und nutzungsberechtigte Personengruppen,
8.im Fall des Art. 6 Abs. 1 bis 3 die Auftragnehmer,
9.Empfänger vorgesehener Datenübermittlungen in Drittländer.

(3) 1 Öffentliche Stellen haben ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens eine Verfahrensbeschreibung mit den in Absatz 2 aufgeführten Angaben zur Verfügung zu stellen; zugleich ist eine allgemeine Beschreibung der Art der für das Verfahren eingesetzten Datenverarbeitungsanlagen und der technischen und organisatorischen Maßnahmen nach Art. 7 und 8 beizugeben. 2 Die behördlichen Datenschutzbeauftragten erteilen die datenschutzrechtliche Freigabe, soweit nicht schon eine datenschutzrechtliche Freigabe nach Absatz 1 Sätze 2 und 3 vorliegt. 3 Wird ihren datenschutzrechtlichen Einwendungen nicht Rechnung getragen, so legen sie die Entscheidung über die datenschutzrechtliche Freigabe den Personen vor, denen sie nach Art. 25 Abs. 3 Satz 1 unterstellt sind; bei den in Art. 15 Abs. 7 genannten Daten haben sie zuvor eine Stellungnahme des Landesbeauftragten für den Datenschutz einzuholen.

Fußnoten
[1])
Art. 26 in Kraft mit Wirkung vom 1. März 2001

Art. 27 [1]
Verfahrensverzeichnis
(1) Die behördlichen Datenschutzbeauftragten führen ein Verzeichnis der bei der öffentlichen Stelle eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden.
(2) In dem Verzeichnis sind für jedes automatisierte Verfahren die in Art. 26 Abs. 2 genannten Angaben fest zu halten.
(3) 1 Das Verfahrensverzeichnis kann von jedem kostenfrei eingesehen werden.
2 Dies gilt nicht bei Behörden der Staatsanwaltschaft, bei Justizvollzugsanstalten, bei Führungsaufsichtsstellen, bei Stellen der Gerichts- und Bewährungshilfe und bei Behörden der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern. 3 Art. 10 Abs. 5 gilt entsprechend.
Fußnoten
[1])
Art. 27 in Kraft mit Wirkung vom 1. März 2001

Art. 28
Rechtsverordnungsermächtigungen
(1) 1 Die Staatsregierung wird ermächtigt, durch Rechtsverordnung das Nähere zur Ausgestaltung der datenschutzrechtlichen Freigabe und des Verfahrensverzeichnisses zu regeln, insbesondere zum Zweck der Vereinfachung der Verfahren und zur Entlastung der öffentlichen Stellen. 2 Die Staatsregierung wird ferner ermächtigt, durch Rechtsverordnung zu bestimmen, dass
1.
für automatisierte Verfahren, die dem internen Verwaltungsablauf dienen, wie Registraturverfahren, ausschließlich der Erstellung von Texten dienende Verfahren, Kommunikationsverzeichnisse und Anschriftenverzeichnisse für die Versendung an die Betroffenen,
2.
für automatisierte Verfahren, die ausschließlich Zwecken der Datensicherung und Datenschutzkontrolle dienen, und
3.
für automatisierte Verfahren, deren einziger Zweck das Führen eines Registers ist, das

auf Grund einer Rechtsvorschrift zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht,
keine Freigabe und Aufnahme in das Verfahrensverzeichnis erforderlich sind.
(2) 1 Die Bestellung behördlicher Datenschutzbeauftragter, die datenschutzrechtliche Freigabe und die Führung eines Verfahrensverzeichnisses sind nicht erforderlich, wenn in öffentlichen Stellen ausschließlich automatisierte Verfahren eingesetzt werden, von denen unter Berücksichtigung der erhobenen, verarbeiteten oder genutzten Daten eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen unwahrscheinlich ist. 2 Die Staatsministerien regeln für ihren Geschäftsbereich und für die unter ihrer Aufsicht stehenden juristischen Personen des öffentlichen Rechts durch Rechtsverordnung, bei welchen öffentlichen Stellen die Voraussetzungen des Satzes 1 erfüllt sind. 3 In der Rechtsverordnung sind die in Art. 26 Abs. 2 genannten Angaben fest zu halten; diese Angaben sind nicht erforderlich für automatisierte Verfahren, die dem internen Verwaltungsablauf dienen, wie Registraturverfahren, ausschließlich der Erstellung von Texten dienende Verfahren, Kommunikationsverzeichnisse und Anschriftenverzeichnisse für die Versendung an die Betroffenen.

Fünfter Abschnitt
Landesbeauftragter für den Datenschutz

Art. 29
Ernennung und Rechtsstellung

(1) 1 Der Landtag wählt auf Vorschlag der Staatsregierung einen Landesbeauftragten für den Datenschutz. 2 Die Ernennung, Entlassung und Abberufung erfolgt durch den Präsidenten des Landtags. 3 Der Landesbeauftragte für den Datenschutz ist Beamter auf Zeit und wird für die Dauer von sechs Jahren berufen.4 Wiederwahl ist zulässig. 5 Vor Ablauf seiner Amtszeit kann der Landesbeauftragte für den Datenschutz auf seinen Antrag entlassen werden; ohne seine Zustimmung kann er vor Ablauf seiner Amtszeit nur mit Zweidrittelmehrheit der Mitgliederzahl des Landtags abberufen werden, wenn eine entsprechende Anwendung der Vorschriften über die Amtsenthebung von Richtern auf Lebenszeit dies rechtfertigt.
(2) 1 Der Landesbeauftragte für den Datenschutz ist in Ausübung seines Amts unabhängig und nur dem Gesetz unterworfen; er kann sich jederzeit an den Landtag wenden. 2 Er untersteht der Dienstaufsicht des Präsidenten des Landtags. 3 Der Landesbeauftragte für den Datenschutz ist oberste Dienstbehörde im Sinn des § 96 der Strafprozeßordnung und des Art. 6 Abs. 3 Satz 3 des Bayerischen Beamtengesetzes;

die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken sowie die Zeugenaussage bedürfen der Zustimmung des Präsidenten des Landtags.
(3) 1 Der Landesbeauftragte für den Datenschutz bedient sich einer Geschäftsstelle, die beim Landtag eingerichtet wird; Verwaltungsangelegenheiten der Geschäftsstelle werden vom Landtagsamt wahrgenommen, soweit sie nicht der Zuständigkeit des Landesbeauftragten für den Datenschutz unterliegen. 2 Die Stellen sind im Einvernehmen mit dem Landesbeauftragten für den Datenschutz zu besetzen. 3 Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit dem Landesbeauftragten für den Datenschutz versetzt, abgeordnet oder umgesetzt werden. 4 Der Landesbeauftragte für den Datenschutz ist Dienstvorgesetzter dieser Mitarbeiter. 5 Sie sind in ihrer Tätigkeit nach diesem Gesetz nur an seine Weisungen gebunden und unterstehen ausschließlich seiner Dienstaufsicht.
(4) Die Personal- und Sachmittel der Geschäftsstelle werden im Einzelplan des Landtags gesondert ausgewiesen.

Art. 30
Aufgaben
(1) Der Landesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz.
(2) 1 Die Kontrolle durch den Landesbeauftragten für den Datenschutz erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung. 2 Akten über die Sicherheitsprüfung unterliegen seiner Kontrolle nicht, wenn Betroffene der Kontrolle der auf sie bezogenen Daten widersprochen haben. 3 Unbeschadet des Kontrollrechts des Landesbeauftragten für den Datenschutz unterrichtet die speichernde Stelle die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht. 4 Der Widerspruch ist schriftlich gegenüber der speichernden Stelle zu erklären.
(3) Die Kontrolle durch den Landesbeauftragten für den Datenschutz erstreckt sich nicht auf personenbezogene Daten, die der Kontrolle durch die Kommission nach Art. 2 des Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz unterliegen, es sei denn, die Kommission ersucht den Landesbeauftragten für den Datenschutz, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen und in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.
(4) 1 Die Kontrolle durch den Landesbeauftragten für den Datenschutz über die Erhebung personenbezogener Daten durch Strafverfolgungsbehörden bei der

Verfolgung von Straftaten ist erst nach Abschluß des Strafverfahrens zulässig. 2 Sie erstreckt sich nicht auf eine Datenerhebung, die gerichtlich überprüft wurde. 3 Die Sätze 1 und 2 gelten für die Strafvollstreckung entsprechend.
(5) 1 Der Landesbeauftragte für den Datenschutz erstattet dem Landtag und der Staatsregierung alle zwei Jahre einen Bericht über seine Tätigkeit. 2 Er gibt dabei auch einen Überblick über die technischen und organisatorischen Maßnahmen nach Art. 7 und regt Verbesserungen des Datenschutzes an. 3 Der Bericht ist in der Datenschutzkommission vorzuberaten.
(6) Der Landtag oder die Staatsregierung können den Landesbeauftragten für den Datenschutz ersuchen, bestimmte Vorgänge aus seinem Aufgabenbereich zu überprüfen.
(7) Der Landesbeauftragte für den Datenschutz und das Landesamt für Datenschutzaufsicht tauschen regelmäßig die in Erfüllung ihrer Aufgaben gewonnenen Erfahrungen aus und unterstützen sich gegenseitig bei ihrer Aufgabenwahrnehmung.

Art. 31 [1]
Beanstandungen
(1) 1 Der Landesbeauftragte für den Datenschutz beanstandet festgestellte Verstöße gegen dieses Gesetz oder andere Vorschriften über den Datenschutz und fordert ihre Behebung in angemessener Frist. 2 Der Landesbeauftragte für den Datenschutz verständigt von der Beanstandung die nach Art. 25 Abs. 1 für die Sicherstellung des Datenschutzes verantwortliche Stelle. 3 Bei juristischen Personen des öffentlichen Rechts, die der Aufsicht des Freistaates Bayern unterstehen, verständigt er darüber hinaus auch die Aufsichtsbehörde.
(2) 1 Wird die Beanstandung nicht behoben, so fordert der Landesbeauftragte für den Datenschutz von der für die Sicherstellung des Datenschutzes nach Art. 25 Abs. 1 verantwortlichen Stelle binnen angemessener Frist geeignete Maßnahmen. 2 Absatz 1 Satz 3 gilt entsprechend. 3 Hat dies nach Ablauf dieser Frist keinen Erfolg, verständigt er den Landtag und die Staatsregierung.
(3) Der Landesbeauftragte für den Datenschutz kann von einer Beanstandung absehen, insbesondere wenn es sich um unerhebliche oder inzwischen behobene Mängel handelt.
Fußnoten
[1])
Art. 31 in Kraft mit Wirkung vom 1. März 2001

Art. 32

Unterstützung durch die öffentlichen Stellen
(1) 1 Der Landesbeauftragte für den Datenschutz ist von allen öffentlichen Stellen in der Erfüllung seiner Aufgaben zu unterstützen. 2 Ihm sind alle zur Erfüllung seiner Aufgaben notwendigen Auskünfte zu geben und auf Anforderung alle Unterlagen über die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Einsicht vorzulegen. 3 Er hat ungehinderten Zutritt zu allen Diensträumen, in denen öffentliche Stellen Daten erheben, verarbeiten oder nutzen.
(2) 1 Für
1.
Einrichtungen der Rechtspflege, soweit sie strafverfolgend, strafvollstreckend oder strafvollziehend tätig werden,
2.
Behörden, soweit sie Steuern verwalten oder strafverfolgend oder in Bußgeldverfahren tätig werden und
3.
Polizei und Verfassungsschutzbehörden
gilt Absatz 1 nur gegenüber dem Landesbeauftragten für den Datenschutz selbst und gegenüber den von ihm schriftlich besonders damit Beauftragten. 2 Die Sätze 2 und 3 des Absatzes 1 gelten für diese Stellen nicht, soweit das jeweils zuständige Staatsministerium im Einzelfall feststellt, daß die Auskunft oder Einsicht die Sicherheit des Freistaates Bayern, eines anderen Landes oder des Bundes gefährden würde.
(3) Die Staatskanzlei und die Staatsministerien unterrichten den Landesbeauftragten für den Datenschutz rechtzeitig über Entwürfe von Rechts- und Verwaltungsvorschriften des Freistaates Bayern sowie über Planungen bedeutender Automationsvorhaben, sofern sie die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betreffen.
(4) Die öffentlichen Stellen sind verpflichtet, die nach Art. 27 zu führenden Verfahrensverzeichnisse dem Landesbeauftragten für den Datenschutz auf Anforderung zuzuleiten.

Art. 33
Datenschutzkommission
(1) 1 Beim Landtag wird eine Datenschutzkommission gebildet. 2 Sie besteht aus zehn Mitgliedern. 3 Der Landtag bestellt sechs Mitglieder aus seiner Mitte nach Maßgabe der Stärke seiner Fraktionen; dabei wird das Verfahren nach Sainte-Laguë/Schepers angewandt. 4 Für Fraktionen, die hiernach nicht zum Zuge kommen, kann der Landtag jeweils ein weiteres Mitglied bestellen, auch wenn sich

dadurch die Zahl der Mitglieder nach Satz 2 erhöht. 5 Ferner bestellt der Landtag jeweils ein weiteres Mitglied auf Vorschlag
1.
der Staatsregierung,
2.
der kommunalen Spitzenverbände,
3.
des Staatsministeriums für Arbeit und Sozialordnung, Familie und Frauen aus dem Bereich der gesetzlichen Sozialversicherungsträger und
4.
des Verbands freier Berufe e. V. in Bayern.
6 Für jedes Mitglied der Datenschutzkommission wird zugleich ein stellvertretendes Mitglied bestellt.
(2) Die Mitglieder der Datenschutzkommission werden für fünf Jahre, die Mitglieder des Landtags für die Wahldauer des Landtags bestellt; sie sind in ihrer Tätigkeit an Aufträge und Weisungen nicht gebunden.
(3) 1 Die Datenschutzkommission unterstützt den Landesbeauftragten für den Datenschutz in seiner Arbeit. 2 Sie gibt sich eine Geschäftsordnung.
(4) 1 Die Datenschutzkommission tritt auf Antrag jedes ihrer Mitglieder oder des Landesbeauftragten für den Datenschutz zusammen. 2 Den Vorsitz führt ein Mitglied des Landtags.
(5) 1 Der Landesbeauftragte für den Datenschutz nimmt an allen Sitzungen teil. 2 Er verständigt die Datenschutzkommission von Beanstandungen nach Art. 31 Abs. 1. 3 Vor Maßnahmen nach Art. 31 Abs. 2 ist der Datenschutzkommission Gelegenheit zur Stellungnahme zu geben.
(6) 1 Die Mitglieder der Datenschutzkommission haben, auch nach ihrem Ausscheiden, über die ihnen bei ihrer Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. 2 Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.
(7) Die Mitglieder der Datenschutzkommission erhalten vom Landesbeauftragten für den Datenschutz Reisekostenvergütung in entsprechender Anwendung der Bestimmungen des Bayerischen Reisekostengesetzes.

Sechster Abschnitt
Aufsichtsbehörde für den Datenschutz bei nicht-öffentlichen Stellen

Art. 34

Landesamt für Datenschutzaufsicht

(1) Zuständige Aufsichtsbehörde gemäß § 38 Abs. 6 des Bundesdatenschutzgesetzes für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich des Dritten Abschnitts des Bundesdatenschutzgesetzes ist das Landesamt für Datenschutzaufsicht.

(2) Sitz des Landesamts für Datenschutzaufsicht ist Ansbach.

Art. 35

Unabhängigkeit der Aufsichtsbehörde

(1) 1 Der Präsident des Landesamts für Datenschutzaufsicht ist Beamter auf Zeit und wird durch die Staatsregierung für die Dauer von fünf Jahren ernannt. 2 Die Wiederernennung ist zulässig. 3 Zum Präsidenten des Landesamts für Datenschutzaufsicht kann nur ernannt werden, wer die Befähigung zum Richteramt besitzt und über die erforderliche Verwaltungserfahrung verfügt. 4 Wird ein Beamter oder ein Richter auf Lebenszeit von der Staatsregierung zum Präsidenten des Landesamts für Datenschutzaufsicht ernannt, gilt er für die Dauer der Amtszeit als ohne Bezüge beurlaubt. 5 Der Präsident des Landesamts für Datenschutzaufsicht kann ohne seine Zustimmung vor Ablauf der Amtszeit nur entlassen werden, wenn eine entsprechende Anwendung der Vorschriften über die Amtsenthebung von Richtern auf Lebenszeit dies rechtfertigt.

(2) 1 Der Präsident des Landesamts für Datenschutzaufsicht ist in Ausübung des Amts unabhängig und nur dem Gesetz unterworfen. 2 Für die Ausübung der Dienstaufsicht gegenüber dem Präsidenten des Landesamts für Datenschutzaufsicht gelten die für den Präsidenten des Obersten Rechnungshofs anzuwendenden Vorschriften entsprechend. 3 Das Landesamt für Datenschutzaufsicht ist oberste Dienstbehörde im Sinn des § 96 der Strafprozessordnung und des Art. 6 Abs. 3 Satz 3 des Bayerischen Beamtengesetzes.

(3) 1 Die Haushaltsmittel des Landesamts für Datenschutzaufsicht werden im Einzelplan des Staatsministeriums des Innern gesondert ausgewiesen. 2 Die Erhebung von Kosten (Gebühren und Auslagen) durch das Landesamt für Datenschutzaufsicht bestimmt sich nach dem Kostengesetz.

Art. 36

(aufgehoben)

Siebter Abschnitt

Ordnungswidrigkeiten, Strafvorschrift, Schlußvorschriften

Art. 37
Ordnungswidrigkeiten, Strafvorschrift
(1) Mit Geldbuße bis zu dreißigtausend Euro kann belegt werden, wer unbefugt von diesem Gesetz oder von nach Art. 2 Abs. 7 diesem Gesetz vorgehenden Rechtsvorschriften geschützte personenbezogene Daten, die nicht offenkundig sind,
1.
speichert, verändert oder übermittelt,
2.
zum Abruf mittels automatisierten Verfahrens bereithält oder
3.
abruft oder sich oder einem anderen aus Dateien verschafft.
(2) Ferner kann mit Geldbuße bis zu dreißigtausend Euro belegt werden, wer
1.
die Übermittlung von durch dieses Gesetz oder durch nach Art. 2 Abs. 7 diesem Gesetz vorgehenden Rechtsvorschriften geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,
2.
entgegen Art. 19 Abs. 4 Satz 1, Art. 22 Satz 1 oder Art. 23 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt oder
3.
entgegen Art. 23 Abs. 3 Satz 3 die in Art. 23 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.
(3) 1 Wer eine der in den Absätzen 1 und 2 bezeichneten Handlungen gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. 2 Die Tat wird nur auf Antrag verfolgt. 3 Antragsberechtigt sind die Betroffenen, die speichernde öffentliche Stelle und der Landesbeauftragte für den Datenschutz.

Art. 38
Änderung von Gesetzen
(1) Art. 3 des Bayerischen Statistikgesetzes (BayStatG) vom 10. August 1990 (GVBl S. 270, BayRS 290-1-I) erhält folgende Fassung:
" Art. 3
Anwendbarkeit des Bayerischen
Datenschutzgesetzes
(1) Werden für eine Statistik, die von einer öffentlichen Stelle durchgeführt wird, Einzelangaben verarbeitet, so gelten von den Vorschriften des Bayerischen

Datenschutzgesetzes nur die Art. 7 bis 9, 25, 29 bis 31, 32 Abs. 1 bis 3 und Art. 33.
(2) Für die Durchführung von Geschäftsstatistiken findet das Bayerische Datenschutzgesetz Anwendung, soweit nichts anderes bestimmt ist.
(3) Einzelangaben dürfen an das Landesamt und an Statistikstellen für die Durchführung von Geschäftsstatistiken weitergegeben und von dort - auch in aufbereiteter Form - rückübermittelt werden.".
(2) 1 Das Gesetz zur Ausführung des Staatsvertrags über Bildschirmtext (Bildschirmtext-Staatsvertrag) - AG BtxStV - vom 4. August 1983 (GVBl S. 542, BayRS 2252-2-S), zuletzt geändert durch Gesetz vom 19. Februar 1993 (GVBl S. 59), wird wie folgt geändert:
1.
Art. 1 Abs. 3 Satz 2 erhält folgende Fassung:
"2 Art. 30, 31, 32 Abs. 1 bis 3 und Art. 33 des Bayerischen Datenschutzgesetzes (BayDSG) finden Anwendung.".
2.
In Art. 4 Abs. 2 werden die Worte "Art. 32 des Bayerischen Datenschutzgesetzes" durch "Art. 34 BayDSG" ersetzt.
2 Die Staatskanzlei wird ermächtigt, das Gesetz mit neuer Artikelfolge neu bekanntzumachen und Unstimmigkeiten des Wortlauts zu beseitigen.
(3) 1 Das Gesetz über die Errichtung und die Aufgaben einer Anstalt des öffentlichen Rechts "Der Bayerische Rundfunk" (Bayerisches Rundfunkgesetz) - BayRG - (BayRS 2251-1-K), zuletzt geändert durch Gesetz vom 23. Juli 1993 (GVBl S. 529), wird wie folgt geändert:
1.
In Art. 19c Abs. 1 werden die Worte "Art. 14 und 15" durch die Worte "Art. 5 bis 8" ersetzt.
2.
Art. 19d Abs. 1 wird wie folgt geändert:
a)
In Satz 1 wird "Art. 26 Abs. 1" durch "Art. 25" ersetzt.
b)
Satz 3 erhält folgende Fassung:
"3 Art. 9 und 29 bis 33 BayDSG finden keine Anwendung.".
2 Das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst wird ermächtigt, das Gesetz mit neuer Artikelfolge neu bekanntzumachen und Unstimmigkeiten des Wortlauts zu beseitigen.
(4) 1 Das Gesetz über die Entwicklung, Förderung und Veranstaltung privater Rundfunkangebote und anderer Mediendienste in Bayern (Bayerisches Mediengesetz

- BayMG) vom 30. November 1992 (GVBl S. 584, BayRS 2251-4-K) wird wie folgt geändert:

1.

Art. 20 wird wie folgt geändert:

a)

In Absatz 3 Satz 5 werden die Worte "Art. 14 und 15" durch die Worte "Art. 5 bis 8" ersetzt.

b)

Absatz 4 Satz 4 erhält folgende Fassung:

"4 Art. 9 und 29 bis 33 BayDSG finden keine Anwendung.".

2.

In Art. 35 Abs. 4 Satz 1 werden die Worte "Art. 26 bis 33" durch die Worte "Art. 25 bis 35" ersetzt.

2 Das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst wird ermächtigt, das Gesetz mit neuer Artikelfolge neu bekanntzumachen und Unstimmigkeiten des Wortlauts zu beseitigen.

(5) Das Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz - PAG) in der Fassung der Bekanntmachung vom 14.September 1990 (GVBl S. 397, BayRS 2012-1-1-I), geändert durch Art. 6 Abs. 5 des Gesetzes vom 27. Dezember 1991 (GVBl S. 496), wird wie folgt geändert:

1.

Art. 46 Abs. 2 wird aufgehoben. Die bisherigen Absätze 3 und 4 werden Absätze 2 und 3.

2.

Art. 47 Abs. 1 Satz 4 erhält folgende Fassung:

"4 Art. 26 und 27 des Bayerischen Datenschutzgesetzes finden keine Anwendung.".

(6) In Art. 10 des Bayerischen Verfassungsschutzgesetzes (BayVSG) vom 24.August 1990 (GVBl S. 323, BayRS 12-1-I) werden die Worte "Art. 8 bis 12, 16 bis 18, 20 und 26 Abs. 2" durch die Worte "Art. 10 bis 13, 15 bis 23 und 26 bis 28" ersetzt.

(7) Die Anlage - Bayerische Besoldungsordnungen - des Bayerischen Besoldungsgesetzes - BayBesG - (BayRS 2032-1-1-F), zuletzt geändert durch Gesetz vom 29. Juli 1991 (GVBl S. 231), wird wie folgt geändert:

In Besoldungsgruppe B 6 werden vor den Worten "Landesbeauftragter für den Datenschutz" die Worte "Ministerialdirigent - als" eingefügt.

Art. 39

Inkrafttreten, Außerkrafttreten,

Übergangsbestimmungen

(1) 1 Dieses Gesetz tritt am 1. März 1994 in Kraft. 2 Gleichzeitig tritt das Bayerische Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bayerisches Datenschutzgesetz - BayDSG) vom 28. April 1978 (BayRS 204-1-I), zuletzt geändert durch Art. 24 des Gesetzes vom 24. August 1990 (GVBl S. 323), außer Kraft. 3 Abweichend von Satz 2 tritt Art. 7 des Bayerischen Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 28. April 1978 am 1. August 1993 außer Kraft. 4 Abweichend von Satz 1 treten Art. 8 Abs. 3 Sätze 4 und 5 erst am 1. März 1995 in Kraft.
(2) Die Verordnung über das Datenschutzregister (Datenschutzregisterverordnung - DSRegV) vom 23. November 1978 (BayRS 204-1-1-I) tritt am 1. August 1993 außer Kraft.
(3) Die Berufung des Landesbeauftragten für den Datenschutz erfolgt nach den Bestimmungen des Art. 29 Abs. 1 erstmalig zum 1. April 1994.
(4) 1 Verfahren, die bei Inkrafttreten dieses Gesetzes bereits datenschutzrechtlich freigegeben worden sind, müssen nicht erneut nach Art. 26 dieses Gesetzes datenschutzrechtlich freigegeben werden. 2 Die Anlagen- und Verfahrensverzeichnisse nach Art. 27 sind bis zum 1. März 1995 einzurichten.
München, den 23. Juli 1993
Der Bayerische Ministerpräsident
Dr. Edmund Stoiber