Thematic Legal Study on assessment of data protection measures and relevant institutions

Report on Germany

Mechtild Lauth, LL.M.

February 2009

Contents Structure

Abbreviations:

Bundesdatenschutzgesetz (BDSG) - Federal Data Protection Law (FDPL)

Landesdatenschutzgesetz (LDSG) – Data Protection Law (DPL)

Introduction

[1]. The data protection system in Germany can be characterized as being highly fragmented. The fragmentation of the data protection system is threefold: firstly, data protection regulations are spread over general laws on data protection and a series of special provisions in other laws both at the federal and at the *Länder* level. Secondly, due to the federal structure of Germany, data protection authorities exist at the federal level as well as at the level of the 16 German *Länder*. Thirdly, the responsibility for monitoring of the application of data protection legislation is distributed between supervisory authorities for the public sector on the one hand and the non-public sector on the other hand. There is one data protection authority at the federal level with the specific competence to supervise the public sector at the federal level in addition to at least one data protection authority in each of the 16 German *Länder*, also having the competence to supervise the public sector in the respective territory, and in many cases also the non-public sector. In a number of *Länder* there are additional authorities responsible only for the supervision of the non-public sector. A comprehensive review of the German data protection system, i.e. data protection measures and institutions, is therefore difficult to provide in the context of the given research project. The report aims at highlighting the relevant practice at both the federal as well as the *Länder* level, however, considering the limitation both in terms of time as well as the scope of this research it is not possible to elaborate on the individual practice of each *Land* or authority individually. The report, in so far as possible and practicable, makes reference to what appears to be the dominant practice, without wanting to raise the impression of absolute completeness. As appropriate and as required, the report makes reference to tables listing the relevant institutions and their competencies, which are annexed to this report (Annex 3, 4, 5 and 6).

[2]. During the preparation of this report, communication was had with a number of Commissioners for Data Protection or their staff both at federal and at *Länder* level, who provided valuable information and insight into their work. Many made very helpful contributions and suggestions relating to issues to be highlighted in the context of this research.

Executive Summary

[3]. ***Constitutional standards for data protection.*** In the absence of a specific data protection provision in the German *Grundgesetz* (GG) [Basic Law, Constitution], the constitutional standards of data protection were developed through the jurisprudence of the *Bundesverfassungsgericht* (BVerfG) [Federal Constitutional Court]. As early as 1969, the Constitutional Court laid down the basic foundations in the area of data protection. In 1983 the Court developed a specific fundamental right to informational self-determination based on article 2 para 1 and the right to human dignity of article 1 para 1 of the Constitution in its landmark decision on the *Volkszählungsgesetz* (VolkszählungsG) [Law on the General Census], a position it confirmed in a couple of later decisions relating to computerised profile searches, eavesdropping and data retention, amongst others. It also recently acknowledged a "fundamental right to confidentiality and integrity of information technology systems" in addition to the already existing right to informational self-determination in the context of a constitutional claim against the secret infiltration of technical information ("online searches").

[4]. ***Data protection legislation.*** The *Bundesdatenschutzgesetz* (BDSchG) [Federal Data Protection Law, FDPL] entered into force in 1977. Data protection laws have also been adopted at the level of all *Länder*. A considerable number of sector-specific laws contain data protection rules which precede the FDPL and the data protection legislation of the *Länder*. The legal environment thus is highly fragmented. The FDPL, also transposing EC directive 95/46/EC, covers both the public sector at the federal level and the private sector. It regulates a number of data protection principles, technical and organisational measures, special categories of sensitive data, the transfer of data and the legal basis for data processing, rights of the data subject and sanctions. The law foresees a two-prong control-system consisting of a mandatory self-control through data protection officials on the one hand and external control by the Federal Commissioner for Data Protection on the other hand.

[5]. ***Relevant Institutions.*** *Beauftragte für Datenschutz* [Commissioners for Data Protection] are established at the federal and at the *Länder* level with the mandate to independently control the implementation and application of data protection legislation at the federal level and at the level of the *Länder* respectively. The control of private companies at the level of the *Länder* is in some *Länder* the

responsibility of the Commissioners for Data Protection and in others the responsibility of the *Aufsichtsbehörden* [supervisory authorities]. The Commissioners for Data Protection regularly submit activity reports to the federal or *Länder* Parliament, issue opinions and investigate occurrences at the request of Parliament or the Government, make recommendations on the improvement of data protection and advice on data protection issues. Most Commissioners for Data Protection are also responsible for the implementation of the relevant *Informationsfreiheitsgesetze* (IFGs) [Laws on Freedom of Information]. The staffing and the budgets of the Commissioners for Data Protection of the *Länder* vary considerably according to the difference in the ambit of their respective role. It has been a regular point of criticism that some of the Commissioners for Data Protection have not been equipped corresponding to the increasing demands as a result of the growing competence for the area of freedom of information as well as the private sector that were recently placed upon them. Annexes 3-6 list the mandates and competencies of the relevant institutions.

[6]. ***Effectiveness of the data protection system.*** The effectiveness of the data protection system has been the subject of fierce and extensive debates in recent years. Main issues under discussion are the excessive collection, abuse and illegal trade of personal data of employees and customers by private companies, the voluntary disclosure of personal data via internet and the extension of surveillance competencies of law enforcement authorities and intelligence services in the context of the fight against terrorism. Specific and efficient protection rules are lacking in a number of areas, such as for the protection of employees and for the health sector, amongst others. The Federal Commissioner for Data Protection together with other Commissioners in the context of the Data Protection Conference, amongst others, have repeatedly requested the adoption of relevant legislation ('Arbeitnehmer-Datenschutzgesetz'), especially in the light of a number of recent data protection scandals in the employment sphere. In the field of anti-terrorism legislation heated debates and demonstrations took place about new surveillance competencies of law enforcement authorities and intelligence services in new Anti-terrorism-legislation.

[7]. ***Transposition of Article 28 of Directive 95/46/EC.*** The Commissioners for Data Protection have a very strong consultation role, and they should be associated with all matters affecting their area of responsibility already at an early stage. They can be consulted during the various phases of the legislative process. The Commissioners can be requested by the respective Parliament or Government to issue expert opinions in the process of the preparation of regulation or the adoption of measures and can also pro-actively

make recommendations concerning the improvement of data protection. The activity reports of the Commissioners for Data Protection which they are obliged by law to prepare annually or bi-annually also fulfil an important advisory and also awareness raising function. A detailed list outlining the competences of the Commissioners for Data Protection within the various jurisdictions, including their involvement in the legislative process can be found in Annex 4 of this report. The Commissioners are also empowered to conduct investigative examinations of their own and control compliance with the Data Protection Laws in all fields of their competence. Public bodies of the Federation are obliged to support the Commissioners and his staff in the performance of their duties. Similar regulations exist in relation to the private sphere. The Commissioners can issue formal complaints against state bodies infringing upon the respective Data Protection Law. In relation to the private sector, the supervisory authority may instruct that technical and organization measures are taken to rectify irregularities detected.

The Federal Commissioner as well as the *Länder* Commissioners and the authorities for the non-public sector all issue various forms of decisions and opinions, many of which are publicly available. The opinions of the Working Party under article 29 of Directive 95/46/EC are widely used and referred to in the work of the Data Protection authorities. The Commissioners also have the right to initiate proceedings leading to criminal prosecution.

[8]. ***Guarantees of independence.*** The lack of independence as a result of the subjection of the *Länder* Commissioners for Data Protection to the supervision of the authority of different state bodies is the subject of proceedings currently pending before the European Court of Justice (ECJ). Concerns are also expressed in relation to the complete independence of the Commissioners for Data Protection responsible for the control of the public sector. It is questionable whether the data protection authorities can act in 'complete independence' as required by Directive 95/46/EC as they are all, in one way or the other, subject to some form of state supervision.

[9]. ***Detection of data protection violations.*** Data protection violations are detected both through independent monitoring activities of the Commissioners as well as by affected individuals. However, very often the affected individuals are not even informed about the violation of their rights. In addition, there is often a problem in relation to sensitive information provided by individuals as there is no effective legislation in force for the protection of the so-called "whistleblowers".

[10]. ***Registration of data processing operations*.** Non-public bodies have a duty to notify automated data processing operations prior to their implementation to the supervisory authority or the competent Commissioner for Data Protection; public bodies of the Federation have to announce them to the Federal Commissioner for Data Protection in accordance with the procedure laid down in the FDPL. Relevant amendments of the Federal Data Protection Law entered into force in 2001 also introducing a couple of exceptions from the notification duty so that the duty has become an exception rather than the rule. Stricter rules apply to the control to be carried out prior to the commencement of the processing (prior checking) in case the processing involves sensitive data. However, with the possibility to appoint data protection officials within the relevant institutions, the previously established practice regarding data protection registers was substantially amended.

[11]. ***Appointment of data protection officers*.** All public bodies at the federal level and all non-public bodies which process personal data in an automated way are obliged to appoint a data protection officer in written form. Very often private companies also use the possibility to appoint external data protection officers who either support an internal officer in the discharge of his or her duties or who provide relevant data protection services independently. No clear regulation exists, however, regarding the education and training for data protection officers. Also, data protection officers in private companies have a rather weak position and do not enjoy the same status and protection as, for example, the Works Councils. The appointment of a data protection officer in public *Länder* bodies by law has either been envisaged or prescribed by law.

[12]. ***Sanctions, compensations and enforcement.*** In most *Länder* jurisdictions and at the Federal level an infringement upon certain data protection provisions may be considered an *Ordnungswidrigkeit* [administrative offence] or a criminal offence depending on the intention of the offender. Some differences exist in the diverse *Länder* Data Protection Laws regarding the exact elaboration of the elements of the offences laid down therein. In relation to administrative offences, the level of fines imposed for the commission of an administrative offence are usually determined by the severity of the infringement and can range from 25,000 € to 250,000 € in the different jurisdictions. Compensation can be awarded at either the federal or the *Länder* level depending on the violated norms and whether the offender was a private party or a state agency. However, the compensation system has a couple of gaps as, for example in the case of data protection violations committed in the private sphere, it is difficult for the individuals concerned to pursue their claims mainly because of the burden of proof resting upon them.

Enforcement of legislation often depends on the personal initiative of data subjects, which is often highlighted as one of the main problems in the context of efficient data protection. Legal advice can, by and large, only be provided by admitted attorneys and support during legal proceedings, if they are commenced at all, is regulated in accordance with the general principles of legal aid. The Commissioners for Data Protection are not sufficiently staffed to engage in all cases that would be appropriate to be supported and secondly (and maybe more importantly), they cannot substitute themselves for admitted attorneys as the right to provide legal advice is basically limited in accordance with the *Rechtsberatungsgesetz* [Law on Legal Advice].

[13]. ***Possible improvements of deficiencies*.** In general, the whole body of data protection legislation has to be simplified, while at the same time some currently under-regulated areas should become subject of legislation. A stricter application of the relevant criminal legislation would also help to rectify a number of problems. In that context, training of the relevant officials within all spheres of government as well as within the private sphere in data protection issues should have a positive impact. Legal amendments should also go hand in hand with the strengthening of the supervisory authorities, otherwise even severe violations of data protection regulations might remain without redress. In addition, the right to take legal action ('Klagerechte') of associations ('Verbraucherverbände') has to be extended to also include data protection issues.

[14]. ***Good practice.*** Examples of good practice include the continuous development of the right to informational self-determination by the Constitutional Court in the last decades which has had a significant impact on the codification of data protection legislation as well as on the relevant data protection practice. The practice of a data protection audit as well as a data protection seal of quality ('Datenschutzgütesiegel) in the *Land* Schleswig-Holstein, the adoption of which has been under discussion for years at the federal level should also be noted here. The *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (ULD) [Independent Centre for Data Protection Schleswig Holstein] also runs extensive training programs in the form of a data protection academy established in the early 1990ies. The appointment of data protection officers both within private and public institutions as an exception to the notification duty under article 18 para 2 of the EC Directive 95/46/EC has also been pointed out as a good practice.

1. Overview

A. Constitutional standards for data protection

A.1. The right to informational self-determination as enshrined in article 2 para 1 in conjunction with article 1 para 1 of the Constitution and related fundamental rights

[15]. There is no specific provision in the German *Grundgesetz* (GG) [Basic Law, Constitution] on data protection.[1] The constitutional standards of data protection were, however, developed through relevant jurisprudence of the *Bundesverfassungsgericht* (BVerfG) [Federal Constitutional Court]. Already in 1969, the Constitutional Court laid down the basic foundations in the area of data protection in a decision relating to (the extent of compilation of) official statistics.[2] According to the Court's decision dealing with various aspects of a micro census carried out, the right to personal freedom enshrined in article 2 para 1 in conjunction with the right to human dignity enshrined in article 1 para 1 of the Constitution protect an untouchable and inviolable sphere of private life which must not be infringed upon by the public authorities. The Court held that it is incompatible with the right to human dignity if the state forcibly registers and indexes the human being, even if the collection of statistics is carried out anonymously.[3]

---

[1] Many of the Länder constitutions, contrary to the federal Constitution, do provide for a specific data protection provision, see article 33 of the Constitution of the Land Berlin, article 11 Constitution of Brandenburg, article 12 para 3 1st sentence of the Constitution of Bremen, article 6 para of the Constitution of Mecklenburg-Vorpommern, article 4 para 2 of the Constitution of Nordrhein-Westfalen, article 4 a of the Constitution of Rheinland-Pfalz; article 2 2nd sentence of the Constitution of Saarland, article 34 of the Constitution of Sachsen, article 6 para 1 of the Constitution of Sachsen-Anhalt; article 6 para 2 of the Constitution of Thüringen; the constitutions of Baden-Württemberg, Hamburg, Hessen and Schleswig-Holstein do no contain a provision on data protection. The constitution of Schleswig-Holstein, however, makes indirect reference to data protection by limiting the right of members of parliament to request information from the government. On the debate as to whether a specific right to data protection should be included in the federal Constitution see below under para 3.

[2] Germany/Bundesverfassungsgericht/Judgment of 16 July 1969 case no.: 1 BvL 19/63 '*Mikrozensusurteil'* [Judgment on the Micro Census] BVerfGE 27, 1 (6).

[3] Germany/Bundesverfassungsgericht/Judgment of 16 July 1969 case no.: 1 BvL 19/63 '*Mikrozensusurteil*' [Judgment on the Micro Census] BVerfGE 27, 1 (6).

[16]. The Constitutional Court went further to develop a specific fundamental right to informational self-determination in its landmark decision in the case concerning the *Volkszählungsgesetz* (VolkszählungsG) [Law on the General Census] in December 1983. The Court, in response to the dangers associated with modern information technology, developed the fundamental right to informational self-determination based on the right to freedom of personal development in article 2 para 1 and the right to human dignity of article 1 para 1 of the Constitution[4], which guarantees the right of the individual to decide on the disclosure and the use of his or her personal data. At the same time the Court stressed that the right to informational self-determination is an essential condition for the functioning of a democratic society based on the citizens' competence to interact and to communicate.[5]

[17]. Thus, the Constitutional Court developed a fundamental right not only protecting against infringements of the private sphere through the processing of personal data of a special private or intimate character, but also stressed that "trivial data" do not exist in the context of automated processing, since even seemingly unimportant information potentially allows to draw conclusions about the individual, his life and personality if the information is linked with other data[6]. According to the Court it is the context of the use or processing of data that is decisive in the end. The restriction of the right to informational self-determination is only allowed if (1) the restriction is necessary for a predominant public interest, (2) the conditions for restriction are in accordance with a clear law enabling the individual concerned to foresee its effects, and (3) if the restriction is proportionate to the aim pursued. Overall surveillance and registration of the individual as well as the creation of comprehensive profiles of a person are absolutely forbidden[7]. State authorities have to take into account the potential danger for fundamental rights arising from "additive" surveillance measures. The legislature is obliged to evaluate new technical developments and, where necessary to correct existing legislation in order to avoid disproportionate or overall

---

[4] Germany/Bundesverfassungsgericht/Judgment of 15 December 1983 ('*Volkszählungsurteil')* [Judgement on the Census], BVerfGE 65, 1.

[5] Germany/Bundesverfassungsgericht/Judgment of 15 December 1983 ('*Volkszählungsurteil*') [Judgement on the Census], BVerfGE 65, 1 (43).

[6] Germany/Bundesverfassungsgericht/Judgment of 15 December 1983 ('*Volkszählungsurteil*') [Judgement on the Census], BVerfGE 65, 1 (45).

[7] Germany/Bundesverfassungsgericht/Judgment of 16 July 1969 case no.: 1 BvL 19/63 '*Mikrozensusurteil*' [Judgment on the Micro Census] BVerfGE 27, 1 (6); Judgment of 15 December 1983 '*Volkszählungsurteil'* [Judgement on the Census], BVerfGE 65, 1, (42, 48, 53); Judgement of 3 March 2004 case no.: 2 BvH 1/04'*Akustische Wohnraumüberwachung'* [Judgement on electronic eavesdropping in private homes], BVerfGE 109, 275 (323).

surveillance[8]. The legislature must also respect the principles of 'data economy' ('Datensparsamkeit')[9] and 'purpose limitation' ('Zweckbindung'). Moreover, and it is required to regulate procedural and organizational safeguards[10], such as the right to be informed or the need for a decision on a restricting measure to be taken by a judge.

[18]. Despite some initial reluctance to fully accept the right to informational self-determination as developed by the Constitutional Court expressed occasionally and especially in the (immediate) aftermath of the delivery of the decision[11], the existence of this fundamental right can be said to be fully acknowledged ever since then. Moreover, the decision is often referred to as a milestone[12] or even praised as the 'magna charta of data protection'[13].

[19]. The Constitutional Court confirmed its position and further elaborated upon the right to informational self-determination in a couple of later decisions.[14] For example, the judgment relating to computerised profile searches ('Rasterfahndung') of 2004 was an important judgment concerning security policy. In computerized profile searches selected data kept by different public and private bodies are compared by computers to the characteristics identified after a process of profiling of typical trouble-makers or terrorists. The characteristics identified, such as sex, age, religion, country of birth, date of birth or the field of study may then be related to the personality or to the behaviour of a person. The Constitutional Court held that such computerized profile searches, if carried out with a preventive purpose, are only compatible with the right to informational self-determination in case of a concrete danger for high ranking protected

---

[8] Germany/Bundesverfassungsgericht/Judgment of 12 April 2005 case no.: 2 BvR 581/01 *'GPS'*, http://www.bverfg.de/entscheidungen/rs20050412_2bvr058101.html (10.02.09). Concerning human rights-oriented evaluation of security legislation see R. Weinzierl, *'Die Evaluierung von Sicherheitsgesetzen'* [Evaluation of Security Legislation], Berlin, German Institute for Human Rights 2006, http://www.institut-fuer-menschenrechte.de/sl.php?id=159 (03.02.09).

[9] According to the principle of data economy only those data may be collected that are absolutely necessary to reach the aim pursued.

[10] Germany/Bundesverfassungsgericht/Judgment of 15 December 1983 '*Volkszählungsurteil'* [Judgement on the Census], BVerfGE 65, 1, (44, 49).

[11] For example, the other (2nd) senate of the Constitutional Court did not take over the concept immediately. See also S. Simitis *Kommentar zum Bundesdatenschutzgesetz* 5th edition, Baden-Baden 2003, § 1, p. 112.

[12] http://www.saechsdsb.de/ueberblick-alle-themen/350-25-jahre-volkszaehlungsurteil (01.02.09).

[13] See President of the Federal Constitutional Court, Hans-Jürgen Papier, in a speech given at a celebration on the occasion of 25 years of the judgment on the general census ('Volkszählungsurteil') on 15 December 2008, referring to his previous colleague Wolfgang Hoffmann-Riem, http://www.sueddeutsche.de/computer/895/451606/text/ (01.02.09).

[14] On the development of the Constitutional Court's jurisprudence relating to data protection and specifically the right to informational self determination see H.-H. Trute in: A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, pp. 171ss.

legal interests ('Rechtsgüter'), such as the danger for the existence or the safety of the state or in case of a danger for life or freedom of a person. Thus, a computerized profile search cannot be justified with a general threat of terrorism after 9/11 or with tensions in external relations.[15] The judgement on computerized profile searches was one of the judgements in which the Constitutional Court underlined the close connection between the right to informational self-determination and other fundamental rights like the right to privacy of correspondence, posts and telecommunications (Art. 10 of the Basic Law), the right to inviolability of the home (Art. 13 of the Basic Law) and the prohibition of discrimination based on origin or religion (art. 3 para 3 of the Basic Law).[16]

[20]. In its landmark decision on the legitimacy of eavesdropping ('Großer Lauschangriff') the Constitutional Court held that given the special protection that the home enjoys for the development of the individual personality, electronic eavesdropping in private homes may only be ordered in case there is, prior to the application of the measure, a concrete indication that the observation does not apply to statements that can be considered to belong to the core area of private life ('Lebensgestaltung').[17]

[21]. Recently, regulations relating to eavesdropping, surveillance of telecommunications, the automatic scanning of registration plates and the retention of data, amongst others, have infringed upon the right to informational self-determination and the right to privacy[18] and in many cases, the Constitutional Court issued relevant decisions. Since the Constitutional Court repeatedly held data retention, except for statistical purposes, to be unconstitutional[19] and since in its (interim) decision of 11 March 2008 the Constitutional Court declared data retention as regulated by the *Gesetz zur Vorratsdatenspeicherung* [Law on the Retention of Data], transposing EC directive 2006/24/EC

---

[15] Germany/Bundesverfassungsgericht/Decision of 4 April 2006, case no.: 1 BvR 518/02, http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html (01.02.09).

[16] Germany/Bundesverfassungsgericht/Decision of 4 April 2006, case no.: 1 BvR 518/02, http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html (01.02.09), paras 104, 105.

[17] Germany/Bundesverfassungsgericht/Judgment of 3rd March 2004, case no.: 1 BvR 2378/98 and 1 BvR 1084/99, http://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html (01.02.09).

[18] See below and also the Berlin Declaration of the 75th Conference of the Commissioners for Data Protection of the Federation and of the Länder on 3rd and 4th April 2008, http://www.lfd.m-v.de/dschutz/beschlue/entsch75.html#nr3 (25.01.09).

[19] See e. g. Germany/Bundesverfassungsgericht/Judgment of 15 December 1983 '*Volkszählungsurteil'* [Judgement on the Census], BVerfGE 65, 1, (47) and Germany/Bundesverfassungsgericht/Decision of 4 April 2006, case no.: 1 BvR 518/02, http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html (01.02.09), para. 105.

partly unconstitutional[20], the final judgement of the Court is expected with some tension.

A.2. The fundamental right to "confidentiality and integrity of information technology systems"

[22]. The Constitutional Court, dealing with a constitutional claim against the possibility of secret infiltration of technical information ("online searches"), developed another new fundamental right, yet again in the light of new technological developments.[21] The Court held that the general right to personal freedom as enshrined in article 2 para 1 in conjunction with article 1 para 1 of the Constitution also implies "the fundamental right to confidentiality and integrity of information technology systems" ('Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme') in addition to the already existing right to informational self-determination.[22]

A.3. Data protection in the Constitutions of the 16 *Länder*

[23]. In reaction to the experience of surveillance in the socialist German Democratic Republic (GDR) the constitutions of all six new *Länder* situated on the territory of the former GDR contain a right to data protection or a right to informational self-determination. The same is true for four of the Constitutions of the old *Länder*[23].

---

[20] Pending a final decision, the Court declared the law unconstitutional in so far as it allows the forwarding of data in cases against persons against whom a reasonable suspicion of having committed a crime does not exist. The retention of data as such, however, has thus far not been declared unconstitutional. http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html (25.01.09).

[21] Germany/Bundesverfassungsgericht/Judgment of 28 February 2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html?Suchbegriff=online (01.02.09).

[22] Germany/Bundesverfassungsgericht/Judgment of 28 February 2008. Another recent decision finding a violation of the fundamental right to informational self-determination relates to the automatic scanning of registration numbers, declaring the relevant law unconstitutional, http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html (25.01.09); in its (interim) decision of 11 March 2008 the Constitutional Court also decided on the question of retention of data as regulated by the *Gesetz zur Vorratsdatenspeicherung* [Law on the Retention of Data], transposing EC directive 2006/24/EC of 15th March 2006 into domestic law. Pending a final decision of the Court, the Court declared the law unconstitutional in so far as it allows the forwarding of data in cases against persons against whom a reasonable suspicion of having committed a crime does not exist. The retention of data as such, however, has thus far not been declared unconstitutional, http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html (25.01.09).

[23] See above footnote 1 and the overview of the NGO *Humanistische Union* http://www.humanistische-union.de/themen/datenschutz/grundrecht/ (10.02.09).

B. International standards

[24]. The European Convention of Human Rights enjoys the status of a simple federal law and is directly applicable in Germany. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 was ratified by Germany in June 1985 and entered into force in October the same year; the additional protocol regarding supervisory authorities and transborder data flows was ratified and entered into force in Germany in July 2004. [24]

[25]. The Convention on Human Rights and Biomedicine of 1997 has not been signed by Germany. Direct reference, for example, by courts, to relevant international guidelines, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 or the United Nations General Assembly Guidelines for the Regulation of Computerized Personal Data Files of December 1990 is possible, but not the rule, given that article 25 of the Constitution only makes "the general rules of international law" an integral part of federal law. However, such guidelines as well as for example the ILO Code of Practice on the protection of workers' personal data of 1997 can be considered persuasive regulations in that the relevant companies can bring their practice in line with the regulations.

C. Overview of data protection legislation

[26]. The first *Datenschutzgesetz* (DSG) [data protection law] was adopted in 1970 by the Land Hessen with the other *Länder* following suit in the coming years[25]. The *Bundesdatenschutzgesetz* (BDSchG) [Federal Data Protection Law, FDPL] entered into force in 1977 and was amended several times[26].

---

[24] The Government, with reference to paragraph 67, sub-paragraph 5, of the Explanatory Report to the Convention, made an interpretative declaration in relation to article 12 para 2 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 according to which "[it] starts from the assumption that Article 12, paragraph 2, leaves a Party at liberty to lay down, in its domestic data protection law, provisions which do not permit, in particular cases, the transfer of personal data, in consideration of the interests of the data subject that warrant protection". See also S. Simitis *Kommentar zum Bundesdatenschutzgesetz* 5th edition, Baden-Baden 2003, Einleitung, p. 70.

[25] The next DPL after the one in Hessen entered into force in Rheinland-Pfalz in 1974, the last one in Hamburg in 1981, see S. Simitis *Kommentar zum Bundesdatenschutzgesetz*, 5th edition, Baden-Baden 2003, pp. 2-3.

[26] See the Bundesdatenschutzgesetz as of November 2006 with English translation http://www.bfdi.bund.de/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-

[27]. The data protection legislation was adopted on the basis of the constitutional standards described above. After the above described landmark decisions of the Constitutional Court a new federal data protection law entered into force in 1990, the main changes being that it was not only directed towards the prevention of abuse (of data), but that it also pursued the aim of protecting the individual from infringements of his or her right to freedom of personality. It was also extended to cover the data processing phases of collection and use of data as well as the improvement of the system of internal and external control.[27] Further amendments to the federal data protection law entered into force in 2001 and, already prior to that, also of the data protection laws of the *Länder* in the context of the transposition of Directive 95/46/EC. A considerable number of sector-specific laws contain data protection rules which precede the *Bundesdatenschutzgesetz* and the data protection legislation of the *Länder*. Such sector-specific rules can for example be found in the *Auländerzentralregistergesetz* [Law on a Central Register for Foreign Nationals], in laws on the different Secret Services the *Bundesnachrichtendienstgesetz* (BND-Gesetz) [Law on the Federal Intelligence Agency] and *the Bundesverfassungsschutzgesetz* [Law on the Protection of the Constitution] , in the *Sozialgesetzbuch* (SGB) [Social Code] and in the *Telekommunikationsgesetz* [Law on Telecommunications], amongst others. The legal environment thus is highly fragmented[28].

[28]. The purpose of the general data protection laws at the federal level and the level of the *Länder* is to protect individuals from violations of their right to privacy through the processing of data related to them and to provide them with recourse to a supervisory body having investigative and intervention powers. The laws provide for the legal basis to act ('Ermächtigungsgrundlagen') in cases involving data protection issues on the one hand, also regulating the way in which data can be collected in the given cases. Thus, they constitute both protective and enabling legislation. The following overview focuses on the Federal Data Protection Law.

[29]. The scope of the Federal Data Protection Law, also transposing EC directive 95/46/EC, covers both the public sector at the federal level

---

FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf. (10.02.09)

[27] A. Roßnagel in: A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 9.

[28] For an overview of special legislation see the Federal Commissioner for Data protection and Freedom of Information, http://www.bfdi.bund.de/cln_027/nn_531520/DE/GesetzeUndRechtsprechung/Spezialgesetze/Spezialgesetze__node.html__nnn=true (10.02.09)

and the private sector. It regulates a number of data protection principles, technical and organisational measures, special categories of sensitive data, the transfer of data and the legal basis for data processing, rights of the data subject and sanctions. The law foresees a two-prong control-system consisting of a mandatory self-control through data protection officials on the one hand and external control by the Federal Commissioner for Data Protection on the other hand.

[30]. The collection, processing and use of personal data is only admissible on the basis of a legal provision or if the data subject has given his consent, article 4 para 1 FDPL ('principle of permission or consent') and if it is carried out for specified, explicit and legitimate purposes and necessary for the fulfilment of a legal duty of the processing body ('principle of necessity'). The law also incorporates data protection principles as developed by the German Constitutional Court like the principle of 'data prevention ('Datenvermeidung') and 'data economy' ('Datensparsamkeit') and the principle of proportionality[29]. In addition, it announces the adoption of a *Bundesdatenschutzauditgesetz* (BDSAuditG) [Law on data protection audits], amongst others.

D. Relevant Institutions

D.1. Beauftragte für Datenschutz [Commissioners for Data Protection]

[31]. The federal and the *Länder* data protection laws as well as some *Länder* constitutions[30] provide for the establishment of offices of *Datenschutzbeauftragte* [Commissioners for Data Protection] with the mandate, amongst others, to independently control the implementation and application of data protection legislation at the federal level and at the level of the *Länder*. Annexes 3-6 list the mandates and competencies of the relevant institutions.

[32]. The office of the Federal Commissioner for Data Protection was established in January 1978 with the mandate to control the application of relevant data protection legislation within the public authorities of the *Bund* [Federation] as well as within telecommunication and postal companies. The Federal Commissioner

[29] See for example Art. 3a and 13 ff. of the Federal Data Protection Law.

[30] Art. 33a Constitution of Bayern, art. 47 Constitution of Berlin, art. 74 Constitution of Brandenburg, art. 37 Constitution of Mecklenburg-Vorpommern, art. 62 Constitution of Niedersachsen, art. 77a Constitution of Nordrhein-Westfalen, art. 57 Constitution of Sachsen, art. 69 Constitution of Thüringen.

is not responsible for the control of data protection within the private business sphere, except for private companies with absolute majority-shareholding of the Federation and telecommunication services[31].

[33]. The control of other private companies at the level of the *Länder* is often not the responsibility of the Commissioners for Data Protection, but of the *Aufsichtsbehörden* [supervisory authorities] of the *Länder*, very often of the ministries of interior of the respective *Land*. In many *Länder*, the control over the private sphere is, however, also vested in the Commissioners for Data Protection of the relevant *Land*, which are also (similar to the Federal Commissioner) responsible for the control of data protection within the administration of the respective *Land* and the municipalities on their territory.[32]

[34]. It needs to be pointed out that most Commissioners for Data Protection are also responsible for the implementation of the relevant *Informationsfreiheitsgesetze* (IFGs) [Laws on Freedom of Information] which was adopted at the federal level in 2006 and at the level of a number of *Länder* in recent years respectively, with the exception of six[33], and which transferred the power to control the implementation of the laws to the relevant Commissioners for Data Protection. Therefore, the official title of most of the Commissioners for Data Protection is in fact "Commissioner for the Protection of Data and Freedom of Information"[34]. Even though the implementation of the laws on freedom of information is not the focus of this research, it needs to be factored in in the given context as freedom of information is seen to be closely linked to data protection and as the new laws add considerable responsibilities to the Data Protection Authorities whose resources had already been stretched before.[35]

---

[31] Art. 115 para 4 Law on Telecommunications.

[32] Responsibility of the Commissioners for Data Protection is given in Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen, Schleswig-Holstein. For an overview of the distribution of responsibility regarding the control of the private sphere see Annex 3.

[33] Baden-Württemberg, Bayern, Hessen, Niedersachsen, Rheinland-Pfalz, Sachsen.

[34] For example, the *Bundesbeauftragter für Datenschutz und Informationsfreiheit* [Federal Commissioner for Data Protection and Freedom of Information], http://www.bfdi.bund.de/cln_027/nn_533554/EN/Home/homepage__node.html__nnn=true (28.01.09), the *Berliner Beauftragter für Datenschutz und Informationsfreiheit* [Commissioner for Data Protection and Freedom of Information Berlin] http://www.datenschutz-berlin.de/ (28.01.09), or for example, in the case of Brandenburg, *the Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg* [State Commissioner for Data Protection and Access to Information] http://www.lda.brandenburg.de/sixcms/detail.php?template=start_e_lda&id=97044 (28.01.09).

[35] See, for example, activity report of the Federal Commissioner for Data Protection for the period 2005 and 2006, published on 24 April 2007, p. 156,

D.2. Parlamentarisches Kontrollgremium (PKGr) [Supervisory Committee of Parliament] *and G 10 – Kommission* [Commission on Article 10 of the Constitution]

[35]. In relation to the activities of the intelligence services, especially in relation to potential infringements of data protection rights, the *Parlamentarische Kontrollgremium* (PKGr) [Supervisory Committee of Parliament][36] and the so called *G 10 – Kommission* [Commission on Article 10 of the Constitution][37] have certain control competencies.

[36]. The Supervisory Committee of Parliament is competent to control the intelligence services of the Federation and supervises the *Bundesnachrichtendienst* (BND) [German Federal Intelligence Service], the *Militärischen Abschirmdienst* (MAD) [Military Counter-Intelligence Service] and the *Bundesamt für Verfassungsschutz* (BfV) [Federal Office for the Protection of the Constitution]. In accordance with the *Kontrollgremiumgesetz* (PKGrG) [Law on the Parliamentarian Control of the Intelligence Service Activities of the Federation] the government is obliged to comprehensively inform the Supervisory Committee about the general activities of the intelligence services and about proceedings of special importance. The Committee can also request reports from the government. The Committee, in turn, is obliged to regularly inform the *Bundestag* [1st Chamber of Parliament] about its control activities. In that regard it also submits reports to the Parliament.[38]

[37]. The Supervisory Committee also appoints the members of the so called *G 10 – Kommission* [Commission on Article 10 of the Constitution][39][40] and participates in the annual consultation of the intelligence services' economic plans. The Commission on Article 10 is an independent body not subject to any instructions and decides ex officio or on the basis of complaints about the necessity and admissibility of all limiting measures of the intelligence services carried out in the area of privacy of letters, posts, and

---

http://www.bfdi.bund.de/cln_027/nn_531940/SharedDocs/Publikationen/Taetigkeitsberichte/21-Taetigkeitsbericht-2005-2006,templateId=raw,property=publicationFile.pdf/21-Taetigkeitsbericht-2005-2006.pdf (28.01.09), For more details see below Chapter 2.

[36] http://www.bundestag.de/parlament/gremien/kontrollgremien/parlkon/index.html (01.02.09).

[37] http://www.bundestag.de/parlament/gremien/kontrollgremien/g10/index.html (01.02.09).

[38] See most recent report submitted to Parliament covering the period 1st January to 31st December 2007, BT Drs 16/11559 and 16/11560.

[39] http://www.bundestag.de/parlament/gremien/kontrollgremien/g10/index.html (01.02.09).

[40] For the conformity of the law on Article 10 with the European Convention on Human Rights see European Court of Human Rights, Admissibility decision of 10 January 2000, appl. No. 54934/00 (*Weber and Saravia versus Germany).*

telecommunications. The control of the Commission does not only extend to the ministerial order of surveillance activities, but to the whole process of collection, processing and use of personal data obtained by the intelligence services including the decision on the information of the persons concerned. In accordance with article 24 para 2 of the FDPL the Federal Commissioner for Data Protection is not competent for the control of personal data that are subject to the control by the Commission on Article 10 of the Constitution. The G-10 Commission may give the Federal Commissioner for Data protection the right to deliver an opinion concerning data protection issues (art. 15 para 5 4th sentence *G-10-Gesetz)* [law on Art. 10].

[38]. The external control of information requests by intelligence services not involving the secrecy of letters, post and telecommunications falls within the competence of the Federal Commissioner for Data Protection.

E. Other relevant instruments

E.1.Datenschutzkommissionen [Data Protection Commissions]

[39]. Some *Länder* constitutions provide for the establishment of a *Datenschutzkommission* [Data Protection Commission] either within parliament or composed of members of parliament of the respective *Land*.[41] It is the responsibility of the Data Protection Commissions to support the work of the Commissioner for Data Protection.[42]

E.2. Datenschutzkonferenz [The Data Protection Conference]

[40]. The federal and the *Länder* Commissioners for Data Protection together form the so called *Datenschutzkonferenz* [Data Protection Conference]. The meetings of the Data Protection Conference usually take place twice a year and are aimed at reaching a common position on a specific issue, in addition to discussing general matters. During each meeting the conference takes a number of decisions directed at various institutions and actors, highlighting deficiencies in data protection in general or in relation to specific issues, for example in the context of draft legislation, amongst others.[43]

---

[41] See, for example, art. 33 DPL Bayern, art. 26 DPL Rheinland-Pfalz.
[42] Art. 33 para 3 DPL Bayern.
[43] http://www.bfdi.bund.de/nn_1207020/DE/Entschlie_C3_9Fungen/DSBundLaender/DSBundLaender__node.html__nnn=true (25.01.09).

E.3. Düsseldorfer Kreis [Düsseldorf Circle]

[41]. The counter-part of the Data Protection Conference for the non-public sector is the so called *Düsseldorfer Kreis* [Düsseldorf Circle], which is the conference of the supreme data protection supervisory authorities for the non-public sphere ('Oberste Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich'). Similarly to the Data Protection Conference, the Düsseldorf Circle meets regularly and points out problematic issues.[44]

E.4. Data protection officers in private and public bodies

[42]. The involvement of data protection officers within public administrations as well as within private companies is discussed further below. Trade Unions and Work Councils can also play an important role particularly within the under-regulated area of data protection in the employment sphere.

F. National Debate regarding effectiveness of the data protection system

F.1. General

[43]. Data protection legislation as well as the effectiveness of the data protection system in general has been the subject of fierce and extensive debates in recent years. There seems to be a general understanding that data protection as a whole is a subject requiring increased attention in the future. The main issues under discussion are the excessive collection, abuse and illegal trade of personal data of employees and customers by private companies, the problem of many persons, especially juveniles tending to disclose personal data via internet voluntarily and the extension of surveillance competencies of law enforcement authorities and intelligence services in the context of the fight against terrorism. The discussion as a whole, intensified by reports on some data protection scandals and mishaps in private[45] and

---

[44] Recently, for example, on the need to amend the Federal Data Protection Law in the area of trading addresses, marketing and data protection audit, see Resolution of 13/14 November 2008, http://www.bfdi.bund.de/cln_007/nn_1207036/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DuesseldorferKreis/141108Adresshandel,templateId=raw,property=publicationFile.pdf/141108Adresshandel.pdf (25.01.09).

[45] http://satundkabel.magnus.de/buntes/artikel/hintergrund-datenschutz-die-groessten-pannen-der-letzten-monate.html (01.02.09).

public[46] bodies, also reanimated a discussion on the reform of data protection legislation in general[47].

[44]. The main general points of discussion and criticism are:

- the high degree of fragmentation of the legal environment and its impact on the rights of the data subject[48],
- the lack of a preventive concept of 'self data protection' ('Selbstdatenschutz') to be implemented especially through simplification of the law and awareness-raising measures[49] (see below),
- the lack of positive incentives for good data protections standards (discussion on *Datenschutzaudit*, see further below),
- the lack of full implementation of existing criminal law sanctions partly because of insufficient knowledge of relevant data protection legislation within prosecution offices and courts,
- the ineffectiveness of criminal sanctions against illegal trade with personal data[50],
- the relatively weak position of data protection officers
- the partly insufficient independence of data protection authorities[51] (see for further below),
- the insufficiency of staffing and budgets of data protection authorities (see further below),

---

[46] http://www.heise.de/tp/r4/artikel/28/28579/1.html (25.01.09), http://www.dorstenerzeitung.de/nachrichten/politik/blickpunkt/art302,350317 (25.01.09), http://www.tagesschau.de/inland/datenschutz110.html (25.01.09).

[47] For an overview see *Datenschutz im Informationszeitalter* [Data Protection in the Information Era], Blickpunkt Bundestag Spezial, October 2008, pp. 13-16, http://www.bundestag.de/blickpunkt/pdf/BB_0804_spezial.pdf (23.01.09) and A. Roßnagel/A. Pfitzmann/H. Garstka, *Modernisierung des Datenschutzrechts* [Modernisation of Data Protection Law], Gutachten im Auftrag des Bundesministeriums des Innern [Expert Opinion provided at the Request of the Federal Ministry of the Interior], 2001, http://www.computerundrecht.de/media/gutachten.pdf (01.02.09).

[48] See http://www.dernewsticker.de/news.php?id=72407; A. Roßnagel/A. Pfitzmann/H. Garstka, *Modernisierung des Datenschutzrechts* [Modernisation of Data Protection Law], Gutachten im Auftrag des Bundesministeriums des Innern [Expert Opinion provided at the Request of the Federal Ministry of the Interior], 2001, http://www.computerundrecht.de/media/gutachten.pdf (01.02.09).

[49] For more details see A. Roßnagel/A. Pfitzmann/H. Garstka, Expert Opinion, pp. 14, 40.

[50] http://www.sueddeutsche.de/politik/907/306864/text/; http://www.kanzlei-prof-schweizer.de/bibliothek/content/schweizer-theilmann_datenschutz.html (25.01.09).

[51] See e. g. the interview with the Federal Commissioner for Data Protection and Freedom of Information Peter Schaar in *Datenschutz im Informationszeitalter* [Data Protection in the Information Era], Blickpunkt Bundestag Spezial, October 2008, 10 http://www.bundestag.de/blickpunkt/pdf/BB_0804_spezial.pdf (23.01.09).

- a more and more sector-specific approach especially problematic in the context of an increased linkage between data stored in public and non-public bodies at national, European and international level,
- increasing storage of data by law enforcement authorities and intelligence services as well as mandatory data retention by private bodies for law enforcement purposes.

F.2. Special proposals, legislative processes and discussions

[45]. Among the data protection areas for which more specific and efficient protection rules are demanded are data protection of employees, *Arbeitnehmer-Datenschutzgesetz* [Law on Data Protection in Employment][52], data protection issues in the health sector ("the transparent patient" – gläserner Patient[53]), data protection in the social sector, data protection in the use of RFID (Radio Frequency Identification) in the private sector and data protection in the use of geo data.

[46]. A couple of legislative proposals brought forward by the Government are under discussion as well as initiatives of a couple of political parties and the *Bundesrat* [Second Chamber of Parliament]. One draft concerns amendments to the Federal Data Protection Law and the possible adoption of a *Bundesdatenschutzauditgesetz* (BDSAuditG) [Law on Data Protection Audit][54]. Already in 2001 a general regulation for a data protection audit was included in amendments to the Federal Data Protection Law (article 9a), but an implementing law has not been adopted. According to the new draft, suppliers of data processing systems and programmes and bodies processing data shall in future have their data protection concepts and their technical facilities examined and evaluated by independent and approved auditors. A public body or publicly authorized body shall issue a certificate which can be used by the companies or authorities for marketing purposes in the following two years. The Federal

---

[52] See Decision of the 73rd Data Protection Conference, 8-9 March 2007, http://www.bfdi.bund.de/cln_007/nn_533554/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBundLaender/73DSK-Beschaeftigtendatenschutz,templateId=raw,property=publicationFile.pdf/73DSK-Beschaeftigtendatenschutz.pdf (01.02.09).

[53] http://www.bfdi.bund.de/cln_007/nn_531516/DE/Schwerpunkte/ElektronischeGesundheitskarte/eGK__node.html__nnn=true (25.01.09).

[54] Draft Law on Amendments to the Data Protection Law adopted by the government on 10 December 2008, http://dip21.bundestag.de/dip21/btd/16/105/1610529.pdf (02.02.09), http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2008/12/Weitere__Informationen,templateId=raw,property=publicationFile.pdf/Weitere_Informationen.pdf (02.02.09).

Commissioner shall keep a public register of all data protection seals of quality ('Datenschutzgütesiegel'), which should be accessible via internet.[55]

[47]. Other pending draft laws include a law on the scoring for the assessment of the credit-worthiness of consumers, which shall regulate which data may be used and transferred during the proceedings[56], a law regulating the access to digital geo data[57], and the above mentioned *Arbeitnehmer-Datenschutzgesetz* [Law on Data Protection in Employment] aiming at more legal certainty for employees and companies and expanding the competences of and protection for the data protection officer within companies. In the light of the recent scandals involving serious violations of data protection rights in a number of companies it is also being considered whether the data protection officers should be *obliged* to inform the official data protection bodies in certain cases. [58]

[48]. The Federal Commissioner for Data Protection recently initiated a (public) debate on a "charter of digital data protection and of freedom of information" in the light of the increasing collection, linking and assessment of information, not only aiming at pointing out the responsibilities of public institutions and business corporations, but also of each individual for the contents of information published about them.[59]

[49]. In the field of anti-terrorism legislation[60] heated debates and demonstrations took place about new surveillance competencies of law enforcement authorities and intelligence services in new Anti-terrorism-legislation in 2002 and 2007, about the installation of a common data base of the police at federal and *Länder* level as well as of intelligence services in 2007, and about the law on data retention implementing the respective directive 2006/24/EC. Recently, an amendment to the *Gesetz über das Bundeskriminalamt* (BKAG) [Law on the Federal Criminal Police Office] was adopted after lengthy discussions in the Parliament. The new law allows online-searches and computerized profile searches by the Federal Criminal

---

[55] It is interesting to note that the Land Schleswig-Holstein has applied a similar procedure of data protection audit and seal of quality registration for a number of years already, see https://www.datenschutzzentrum.de/faq/audit.htm (23.01.09) and https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm (23.01.09)

[56] BT Drs 16/683, http://dip.bundestag.de/btd/16/006/1600683.pdf (02.02.09).

[57] BT Drs 16/10530, http://dip21.bundestag.de/dip21/btd/16/105/1610530.pdf (02.02.09).

[58] http://www.bundestag.de/aktuell/hib/2006/2006_196/01.html (02.02.09).

[59] http://www.bfdi.bund.de/cln_027/nn_533554/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM__32__08__ChartaDigitalerDatenschutz.html (02.02.09).

[60] http://www.bfdi.bund.de/nn_579908/DE/Schwerpunkte/Terrorismusbekaempfung/Terrorismusbekaempfung__node.html__nnn=true (01.02.09).

Police Office. The Federal Office for Administration (subject to supervision of the Federal Ministry of the Interior), according to the government, is intended to become a "knot of communication" ('Kommunikationsknoten')[61] linking not only the federal with the *Länder* level but also the national level with EU information systems like the Schengen Information System (SIS II) and the Visa Information System (VIS). Complaints are pending before the Constitutional Court concerning the law on the Federal Police[62] and concerning the law on data retention[63]. A spying scandal in the Deutsche Telekom AG, Europe's biggest telecommunication company in 2008 was used as a new argument against Europe-wide retention of telecommunication data[64]. Data protection in the EU's third pillar has also been discussed.[65]

[50]. Finally, there has been an extensive debate as to whether the right to data protection should be included in the federal constitution. Despite the fact that the right to privacy and data protection, particularly in the form of informational self-determination has been acknowledged as a fundamental right on the basis of the case law of the Constitutional Court[66], the inclusion of a specific right is often demanded in order to highlight the importance of this fundamental right, amongst others. Arguments in favour of the inclusion of the right to data protection in the constitution focus on the wording of the Constitution, i.e. that the (fundamental) right to informational self-determination may be acknowledged by the Constitutional Court and in practice, but, that this right is still not specifically mentioned in the constitution. It is however considered desirable that citizens can identify their fundamental rights contained in the constitution in the constitution itself. The inclusion of the right to data protection in the constitution would provide for more legal certainty and clarity and would

---

[61] See proposal of the Govenment for the law transposing the EU directives in the field of immigration and asylum, BT-Drs. 16/5065, pp. 192, 193.

[62] http://hpd.de/node/6228 (01.02.09).

[63] See the interim decision of the Constitutional Court http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html (25.01.09). For relvant case law of the German Constitutional Court see above.

[64] See www.vorratsdatenspeicherung.de and http://www.heise.de/newsticker/Telekomgate-Datenschuetzer-fordert-Aussetzung-der-Vorratsdatenspeicherung--/meldung/108835 (09.02.09).

[65] See http://www.heise.de/newsticker/Nationale-Sicherheit-vs-Datenschutz-fuer-Sicherheitsbehoerden--/meldung/97664 and Recommendations of the German Institute for Human Rights for Germany's EU presidency http://files.institut-fuer-menschenrechte.de/437/DIMR_Empfehlungen_EU_Ratspraesidentschaft_2006.pdf (10.02.09).

[66] See above Chapter 1, par 2.

consequently increase the confidence of the citizen in the constitution.[67]

2. Data Protection Authority

A. Type, Structure, Legal Basis and Powers of the Data Protection Authorities

[51]. The German data protection authority at federal level is the Federal Commissioner for Data Protection and Freedom of Information[68]. He is responsible for the control of compliance with the provisions of the Federal Data Protection Law[69] by the federal public authorities of the state and the public authorities of the *Länder* in so far as they implement federal law. The federal public authorities subject to his control are, amongst others, the federal ministries, the armed forces, the federal police as well as the customs authorities. The Commissioner does not have any power over the judiciary except in so far as they are active in administrative matters.[70]Additionally since 2006 the Federal Commissioner for Data Protection and Freedom of Information also observes the compliance with the Freedom of Information Act[71], which entitles everyone to have access to information of federal authorities and other bodies of the state in so far as they carry out federal administrative tasks.

---

[67] See the report on an expert speech and a political panel discussion on the topic http://files.institut-fuer-menschenrechte.de/437/Bericht_Datenschutz_ins_Grundgesetz.pdf. The arguments against the inclusion of the right to data protection in the constitution mainly relate to a potential abuse of the constitutional text and that such a procedure would only constitute symbolic politics. Since the pronouncement of the "census judgment" in 1983 the fundamental right to data protection has had an enormous effect without being subject of express textual codification. The inclusion of findings of constitutional jurisprudence in the constitution could water down the Constitution's content and put into question the core constitutional content derived from the rule of law. Sufficient protection of the rights to free personal development, privacy and personal data is already guaranteed through article 1 para and article 2 para 1 of the Constitution. See amongst others the Federal Minister of Justice B. Zypries *'Verfassungsänderung kein Gewinn für Datenschutz'*, speech given at the Friedrich Ebert foundation on 1st July 2008, http://www.bmj.de/enid/4a860ebb36f9c6c5b6fccb888226b76a,6e5534706d635f6964092d0935323631093a095f7472636964092d0935323933/Reden/Brigitte_Zypries_zc.html (02.02.09).

[68] http://www.bfdi.bund.de/cln_007/nn_670410/EN/Home/homepage__node.html__nnn=true (25.01.09).

[69] http://www.bfdi.bund.de/cln_007/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf (16.12.08).

[70] Article 21 2nd sentence FDPL.

[71] http://www.bfdi.bund.de/cln_027/nn_672734/IFG/Gesetze/IFG/TextIFG,templateId=raw,property=publicationFile.pdf/TextIFG.pdf (16.12.08).

[52]. The Federal Commissioner for Data Protection and Freedom of Information is elected by the *Bundestag* [Parliament] for a term of five years and may be re-elected once.[72] Currently the Federal Commissioner for Data Protection and Freedom of Information disposes of a staff of in total 69 employees and is allocated an annual budget of about 4,511,000 €.

[53]. It is the duty of the Federal Commissioner for Data Protection to control the compliance by the public bodies of the Federation with the provisions of the FDPL and of other data protection provisions, article 24 para 1 FDPL. He has the power to control compliance with data protection legislation and to lodge complaints in cases of infringements and to decide on individual appeals. He submits an activity report to the Parliament every two years, issues opinions and investigates occurrences at the request of Parliament, the Government or the Petitions Committee, makes recommendations on the improvement of data protection and advises on data protection issues.

[54]. Public bodies of the Federation are obliged to support the Commissioner in the discharge of his duties, article 24 para 4 FDPL. In that context the Commissioner is entitled to request information as well as to have access to all files, especially saved data which are relevant for his control activities. He can also enter the facilities of the public bodies at any time.

[55]. The purpose of the Data Protection Law is to protect individuals from violations of their right to personal freedom through the processing of data related to them and to provide them with recourse to a supervisory body having investigative and intervention powers. Additionally since 2006 the Federal Commissioner for Data Protection and Freedom of Information also observes compliance with the *Informationsfreiheitsgesetz* (IFG) [Freedom of Information Act][73], which entitles everyone to have access to information of federal authorities and other bodies of the state in so far as they carry out federal administrative tasks.

[56]. In accordance with article 22 para 4 FDPL the Federal Commissioner for Data Protection is independent in the discharge of his duties and is only subject to law. According to article 22 para 5 of the FDPL the office of the Federal Commissioner for Data Protection and Freedom

---

[72] article 22 I, III BDSG. The current Federal Commissioner for Data Protection, Peter Schaar, was recently re-elected for a second term, see http://www.heise.de/newsticker/Peter-Schaar-als-Bundesdatenschutzbeauftragter-im-Amt-bestaetigt--/meldung/119467 (25.01.09).

[73] http://www.bfdi.bund.de/cln_007/nn_672734/IFG/Gesetze/IFG/TextIFG,templateId=raw,property=publicationFile.pdf/TextIFG.pdf (16.12.08).

of Information is established as an independent body with the Federal Ministry of the Interior. As an independent body he is not part of the ministry. He is also not an institution subordinate to the Ministry of Interior.

[57]. Nevertheless he is subject to the *Dienstaufsicht* [administrative/hierarchical supervision] of the Federal Minister of the Interior as well as to the *Rechtsaufsicht* [legal supervision] of the Federal Government.

[58]. The Federal Commissioner reports on his activities to the *Bundestag* [Parliament] every other year.[74] In accordance with article 21 FDPL, everyone is entitled to address the Federal Commissioner if he/she is of the opinion that his/her rights were violated during the collection, processing or use of personal data by public authorities of the state. The Federal Commissioner is also empowered to conduct examinations of his own and can issue formal complaints against state bodies infringing upon the Federal Data Protection Law.[75] Moreover, the Federal Commissioner for Data Protection can be requested to issue expert opinions by the *Bundestag* [Parliament] or the Federal Government and pro-actively make recommendations concerning the improvement of data protection.[76]

[59]. The data protection system at federal level is complemented by the control of compliance with data protection regulations at the *Länder* level, which is entrusted to the 16 Commissioners for Data Protection established in each of the *Länder*.[77] These Commissioners for Data Protection are mandated to protect individuals from violations of their right to personal freedom through the processing of data by *Länder* public authorities based upon *Länder* regulations and administration thereof as well as by the municipalities and other bodies performing state functions. The Commissioners at *Länder* level also do not have any power over the judiciary except in so far as they are active in administrative matters.[78]

[60]. The details are regulated by the respective data protection laws of the *Länder*. In addition about half[79] of the Commissioners for Data Protection of the *Länder* have also been put in charge of the

---

[74] Art. 26 para 1 FDPL.
[75] Art. 24 and 25 FDPL.
[76] Art. 26 para 2 and 3 FDPL.
[77] For a complete list of the Länder Commissioners for Data Protection see: http://www.bfdi.bund.de/cln_007/nn_671936/EN/AdressesAndLinks/Landesdatenschutzbeauftragte/Landesdatenschutzbeauftragte__node.html__nnn=true (16.12.08).
[78] See, for example, art. 21 FDPL.
[79] Berlin, Brandenburg, Bremen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Saarland, Sachsen-Anhalt and Schleswig-Holstein.

observation of compliance with the particular *Länder* freedom of information laws by the *Länder* authorities and municipalities and are thus termed Commissioner for Data Protection and Freedom of Information,[80] while in the other *Länder* this task has been assigned to a special freedom of information supervision body.

[61]. Moreover, it is important to note that the supervision of data protection compliance in the private sector has been entirely transferred into *Länder* jurisdiction pursuant to Art. 38 para 6 FDPL, which gives the respective *Länder* governments the competence to designate the supervisory authorities responsible for the implementation of data protection within the area of data processing by private bodies and public-law enterprises participating in competition.[81] The *Länder* have done so, in parts by law in the respective *Länder* data protection laws[82], partly by way of administrative order[83]. A total of nine *Länder* chose to assign the supervision of the private sector to their respective Commissioner for Data Protection, too,[84] while seven *Länder* entrusted the task either directly to the Ministry of the Interior of their *Land*[85] or to regional

---

[80] The German terminology varies between *Landesbeauftragter für Datenschutz und Informationsfreiheit* and *Landesbeauftragter für Datenschutz und das Recht auf Akteneinsicht.*

[81] S. Simitis *Kommentar zum Bundesdatenschutzgesetz*, 5th edition, 2003 Baden-Baden, article 38 para 6 notes 43-46.

[82] Art. 33 para 1 DPL Berlin, art. 33 a DPL Mecklenburg-Vorpommern, art. 22 para 6 DPL Niedersachsen, art. 22 para 6 DPL Nordrhein-Westfalen, art. 24 para 1 DPL Rheinland-Pfalz, art. 30 a DPL Sachsen, art. 38 DPL Schleswig-Holstein.

[83] Baden-Württemberg: Verordnung der Landesregierung über die zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich (Datenschutzzuständigkeitsverordnung - DSZuVO) [Decree of the Government on the Competent Supervisory Authority over Data Protection in the non-public Sphere] of 1st Januar 1978, http://www.landesrecht-bw.de/jportal/portal/t/gyj/page/bsbawueprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=jlr-DSZustVBWpP1&doc.part=X&doc.price=0.0#focuspoint (02.02.09), Bayern: Datenschutzverordnung (DSchV) [Data Protection Decree] of 1st March 1994, http://www.datenschutz-bayern.de/recht/DSchV.htm (02.02.09), Brandenburg: http://www.landesrecht.brandenburg.de/sixcms/detail.php?gsid=land_bb_bravors_01.c.14214.de (02.02.09), Hessen: http://www.hessenrecht.hessen.de/gesetze/300_Organisation/300-39-ZustVO-BDSG/ZustVO-BDSG.htm (02.02.09), Saarland: http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/gesamt/DSZustV_SL.htm#DSZustV_SL_rahmen (02.02.09). Executive orders also regulate the establishment and mandate of the Supervisory Authorities in Bremen, Hamburg, Sachsen-Anhalt and Thüringen (not available in electronic form).

[84] Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen, Schleswig-Holstein.

[85] *Landesinnenministerium Baden-Württemberg*, http://www.innenministerium.baden-wuerttemberg.de/de/Datenschutz/83821.html (02.02.09), *Landesinnenministerium Brandenburg*, http://www.mi.brandenburg.de/sixcms/list.php?page=mi_datenschutz (02.02.09), *Landesinnenministerium Saarland*, http://www.saarland.de/3841.htm (02.02.09).

administrative bodies[86], which are under the ultimate legal and material supervision of the respective Ministry of the Interior.[87]

[62]. The staffing and the budgets of the Commissioners for Data Protection of the *Länder* thus vary according to the difference in the ambit of their respective role and have also to be regarded in relation to the population size as well as the economic activity of the particular *Land*. Yet in general the staff numbers reach from 12 to 45 and the budgets may range between 640,700 € and 2,989,700 € per year.[88] Also, in both of these exemplary *Länder* at the extreme ends of the existing range funding has been decreased in comparison to the previous year.[89]

[63]. All of the Commissioners for Data Protection possess powers similar to those of the Federal Commissioner for Data Protection. Namely they are entitled to receive individual complaints and to conduct examinations into the legality of activities relevant to data protection of their own. They can also issue formal complaints against state bodies infringing upon the respective *Länder* data protection laws. Furthermore, they are all empowered to issue expert opinions upon request by their respective Government, Parliament and some also provide for requests made by other parliamentary organs or bodies. Additionally, the Commissioners for Data Protection can recommend improvements concerning data protection on their own initiative, too. Differing from the ambit of the powers allocated to the Federal Commissioner for Data Protection and going further than these, some *Länder* data protection laws contain a mandatory duty to consult the respective Commissioner for Data Protection in the process of law

---

[86]Bayern: *Regierung Mittelfranken,* http://www.regierung.mittelfranken.bayern.de/aufg_abt/abt1/abt1dsa60.htm (02.02.09), Hessen: *Regierungspräsidium Darmstadt,* http://www.rp-darmstadt.hessen.de/irj/RPDA_Internet?cid=79a2a5eee51f280592670fc88767ac32 (02.02.09), Sachsen-Anhalt: *Landesverwaltungsamt,* http://www.sachsen-anhalt.de/LPSA/index.php?id=14760 (02.02.09), Thüringen: *Landesverwaltungsamt,* http://www.thueringen.de/de/tlvwa/inneres/hoheit/datenschutz/ *(02.02.09).*

[87]For a complete list see: http://www.bfdi.bund.de/cln_007/nn_674018/EN/AdressesAndLinks/AufsichtsbehoerdenNichtOeffentlich/AufsBehoerdFuerDenNichtOeffBereich__node.html__nnn=true (16.12.2008).

[88] Bayern: 1,597,300 € per year, staff number of 24; Berlin: 2,4 Million € per year, staff number of 31; Brandenburg: 1,077,700 € per year, staff number of 16; Nordrhein-Westfalen: 2,989,700 € per year, staff number of 45; Rheinland-Pfalz: 1,159,700 € per year, staff number of 13 2/3 (11 full and 4 part time); Saarland: 640,700 € per year, staff number of 12; Sachsen: 1,27 Million € for a two year period, staff number of 23; Schleswig Holstein: 1,8 Million € per year, staff number of 39 (25 permanent employees and 14 project related with third party funding); Thüringen: 1,781,600 € for a two year period, staff number of 14.

[89] In Nordrhein-Westfalen the budget went from 3,238,900 € and a staff of 48 in 2008 to 2,989,700 € and staff of 45 in 2009; in Saarland the budget went from 681,100 € in 2007 to 640,700 € in 2008, while the staff number of 12 remained the same.

and regulation making[90] or require the compulsory notification of the Commissioner for Data Protection in such legislative or executive procedures which are relevant to data protection issues.[91]

B. Transposition of Article 28 of Directive 95/46/EC

B.1. Consultation in the preparation of regulation or the adoption of administrative measures (article 28 para 2 of Directive 95/46/EC)

[64]. In accordance with article 28 para 2 of Directive 95/46/EC each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. The wording 'shall provide' indicates that Member States are obliged to ascertain the consultation of the supervisory authorities. According to Rules 21 para 1, 45 para 3 and 62 para 2 of the *Gemeinsame Geschäftsordnung der Bundesministerien* (GGO) [Joint Rules of Procedure of the Federal Ministries] of December 2006, the Federal Commissioner for Data Protection has to be associated with all matters ('Vorhaben') affecting his area of responsibility already at an early stage. The rules of procedure repeat this obligation with regard to his association during the process of drafting legislative proposals and regulations by the government.[92] While the respective Joint Rules of Procedure of the *Länder* ministries also regulate the involvement of the Commissioners for Data Protection, they do not all make reference to their

---

[90] Art. 31 para 3 2nd sentence DPL Baden-Württemberg, art. 23 para 5 DPL Brandenburg, art. 21 para 5 DPL Hessen, art. 33 para 2 4th sentence DPL Mecklenburg-Vorpommern, art. 22 para 1 4th sentence DPL Niedesachsen, art 23 para 8 DPL Rheinland-Pfalz, art. 26 DPL Sachsen.

[91] Art. 27 para 2 no 2 DPL Bremen, art. 22 para 3 2nd sentence DPL Nordrhein-Westfalen.

[92] Rule 21 of the Joint Rules of Procedure of the Federal Ministries provides as follows: "Cooperation with the Commissioners of the Government and the Federal Commissioners.
(1) The Commissioners of Government and the Federal Commissioners (Annex 3 of the Joint Rules of Procedure) shall be involved in all matters affecting their area of responsibility at an early stage.
(2)…"
Rule 45 (3) of the Joint Rules of Procedure of the Federal Ministries (contained in the relevant Chapter 6 –Legislation, provides an identical provision for the legislative procedure. Annex 3 to the Rules 21 and 45 specifically lists the Federal Commissioner for Data Protection and the other Federal Commissioners and Commissioners of Government. http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2007/GGO,templateId=raw,property=publicationFile.pdf/GGO.pdf (22.01.09).

involvement "at an early stage".[93] Seven *Länder* data protection laws explicitly prescribe a mandatory duty of consultation of the respective Commissioner for Data Protection in the process of law and regulation making.[94] Also two more *Länder* data protection laws require at least the compulsory notification of the Commissioner for Data Protection in such legislative or executive procedures which are relevant to data protection issues,[95] and in one *Land* the Commissioner for Data Protection needs to be heard with regard to activities in certain areas which are considered specifically data protection sensitive subject matters[96].

[65]. An explicit legal obligation to consult the Commissioners for Data Protection when drawing up administrative decisions and regulations is missing at the federal level and in some of the Länder.[97] In order to guarantee meaningful influence of the supervisory authorities before the end of main political debates, consultation at an early stage should always be guaranteed explicitly. A corresponding legal obligation is therefore desirable.

[66]. In addition to the above mentioned obligations to consult the Commissioners, the Federal Commissioner for Data Protection can be requested to issue expert opinions by the *Bundestag* [Parliament] or the Federal Government in the process of the preparation of regulation or the adoption of measures and he can always pro-actively make recommendations concerning the improvement of data protection in general or as regards legislative projects.[98] This is also within the competence of all the *Länder* Commissioners for Data Protection with the exception of the *Land* Bayern. The Commissioners are empowered to issue expert opinions upon request by the Government and Parliament of the respective *Land* and some laws also provide for requests made by other parliamentary organs or

---

[93] See, for example, Rule 40 of the Joint Rules of Procedure of the Ministries of the Government of Sachsen, http://www.landtag.sachsen-anhalt.de/fileadmin/downloads/GO-Ministerien_01.pdf (02.02.09).

[94] Art. 31 para 3 2nd sentence DPL Baden-Württemberg, art 23 para 5 DPL Brandenburg, art. 21 para 5 DPL Hessen, art. 33 para 2 4th sentence DPL Mecklenburg-Vorpommern, art. 22 para 1 4th sentence DPL Niedersachsen, art. 23 para 8 DPL Rheinland-Pfalz, art. 26 DPL Sachsen.

[95] Art. 27 para 2 no 2 DPL Bremen, art. 22 para 3 2nd sentence DPL Nordrhein-Westfalen.

[96] This is the case in Schleswig-Holstein, see art. 5 para 3 DPL Sachsen (concerning data protection security measures of the *Landes* Government) and art. 16 para 3 DPL Sachsen (concerning data transmission to foreign jurisdictions).

[97] See also the recommendation of A. Roßnagel/A. Pfitzmann/H. Garstka, *Modernisierung des Datenschutzrechts* [Modernisation of Data Protection Law], Gutachten im Auftrag des Bundesministeriums des Innern [Expert Opinion provided at the Request of the Federal Ministry of the Interior], 2001, p. 20, http://www.computerundrecht.de/media/gutachten.pdf (01.02.09).

[98] Art. 26 para 2 and 3 FDPL.

bodies.[99] Additionally the *Länder* Commissioners for Data Protection can recommend improvements concerning data protection on their own initiative, too.[100]

B.2. Investigative powers (article 28 para 3 1st indent)

[67]. The Federal Commissioner is empowered to conduct investigative examinations of his own and control compliance with the Federal Data Protection Law in all fields of his competence.[101]

[68]. According to article 24 para 4 of the FDPL public bodies of the Federation shall be obliged to support the Federal Commissioner and his staff in the performance of their duties. They shall be provided with information in response to their questions and shall be given the opportunity to inspect all documents, especially stored data and data processing programs connected with the monitoring duty of the authority. They shall also have access to the premises at any time. All *Länder* Commissioners for Data Protection possess similar powers to the Federal Commissioner for Data Protection, namely to conduct examinations into the legality of activities relevant to data protection of their own in their areas of supervision.[102]

[69]. Similar regulations also exist in relation to the private sphere. According to article 38 of the FDPL the bodies subject to monitoring shall provide the supervisory authority with the required information. A person obliged to provide information may refuse to do so in case he has a right to refuse to give evidence and if there is a danger of criminal prosecution or of proceedings under the *Ordnungswidrigkeitengesetz* (OWiG) [Law on Administrative Offences]. The persons appointed to carry out the monitoring shall be authorized to enter the property and premises of the body and may inspect business documents, especially the list of automated processing procedures subject to obligatory notification[103] as well as stored personal data and data processing programs.

---

[99] See art. 31 para 2 DPL Baden-Württemberg, art. 32 para 1 DPL Bremen, art. 22 para 4 DPL Nordrhein-Westfalen, art. 24 para 5 DPL Rheinland-Pfalz, art. 30 para 3 DPL Sachsen, art. 39 para 4 1st sentence DPL Schleswig-Holstein, art. 40 para 4 DPL Thüringen.
[100] See art. 31 para 3 1st sentence DPL Baden-Württemberg, art. 27 para 1 DPL Bremen, art. 22 para 1 DPL Nordrhein-Westfalen, art. 24 para 3 and 4 DPL Rheinland-Pfalz, art. 30 para 4 DPL Sachsen, art. 39 para 3 DPL Schleswig-Holstein, art. 40 para 7 DPL Thüringen.
[101] Art. 24 FDPL.
[102] See art. 28 para 1 DPL Baden-Württemberg, art. 27 para 1 DPL Bremen, art. 22 para 1 DPL Nordrhein-Westfalen, art. 24 para 1 DPL Rheinland-Pfalz, art. 27 para 1 DPL Sachsen, art. 39 para 1 DPL Schleswig-Holstein, art. 37 para 1 DPL Thüringen.
[103] Art. 19 Directive 95/46/EC, article 4 e FDPL.

[70]. Furthermore, the Federal and the *Länder* Commissioners for Data Protection are entitled to receive and scrutinise complaints of individuals claiming to have been violated in their rights to data protection.[104]

B.3. Effective Powers of Intervention (article 28 para 3 2nd indent)

[71]. The Federal Commissioner for Data Protection as well as the *Länder* Commissioners for Data Protection can issue formal complaints against state bodies infringing upon the respective Data Protection Law.[105] The supervisory authority of the public body in question is informed about the complaint, which does not oblige the public body to correct the reprimanded action or to omit the action in future. However, the state body is obliged to submit a statement at the time determined by law or by the (data protection) supervisory authority. In case the infringement or the deficiency is not rectified, the supervisory authority can make recommendations, contact Parliament or report on the matter in the activity report.[106] While the data protection law does not explicitly regulate whether the data subjects concerned have to be informed of the infringement and/or deficiency, literature on the topic presumes the existence of a duty to ex officio inform the data subjects.[107] Also, the Data Protection Commissioner cannot bring the violations of data protection law by state bodies before administrative courts. Such a possibility is one of the recommendations of an expert opinion on the modernization of data protection law prepared at the request of the Federal Ministry of the Interior.[108]

[72]. In relation to the private sector, the supervisory authority may instruct that technical and organization measures are taken to rectify irregularities detected, article 38 para 5 FDPL. In case of grave irregularities the supervisory authority may prohibit the application of

---

[104] See art. 21 FDPL, art. 27 DPL Berlin, art. 26 DPL Mecklenburg-Vorpommern, art. 19 para 1 DPL Niedersachsen, art. 25 para 1 DPL Nordrhein-Westfalen, art. 29 para 1 DPL Rheinland-Pfalz, art. 24 para 1 DPL Sachsen, art. 40 DPL Schleswig-Holstein.

[105] See art. 25 FDPL, art. 26 para 1 DPL Berlin, art. 32 DPL Mecklenburg-Vorpommern, art. 23 para 1 2nd sentence DPL Niedersachsen, art. 24 para 1 DPL Nordrhein-Westfalen, art. 25 para 1 DPL Rheinland-Pfalz, art. 29 DPL Sachsen, art. 42 para 2 DPL Schleswig-Holstein.

[106] S. Simitis *Kommentar zum Bundesdatenschutzgesetz* (5th edition, Baden-Baden, 2003), article 25, notes 11-15.

[107] S. Simitis *Kommentar zum Bundesdatenschutzgesetz* (5th edition, Baden-Baden, 2003), article 28, notes 16-17.

[108] A. Roßnagel/A. Pfitzmann/H. Garstka, *Modernisierung des Datenschutzrechts* [Modernisation of Data Protection Law], Gutachten im Auftrag des Bundesministeriums des Innern [Expert Opinion provided at the Request of the Federal Ministry of the Interior], 2001, p. 20, http://www.computerundrecht.de/media/gutachten.pdf (01.02.09)

particular procedures if the irregularities, in contravention of the instruction and despite the imposition of a fine, are not rectified within a reasonable period. The supervisory authority may demand the dismissal of the institution's data protection official if he does not possess the specialised knowledge and does not demonstrate the reliability required for the performance of his or her duties. The supervisory authority does not have the right to give instructions other than those relating to technical and organizational measures. Further powers of the supervisory authority and the power to order the blocking, erasure or destruction of data have been recommended by experts.[109]

B.4. Power to engage in legal proceedings or to bring violations to the attention of judicial authorities

[73]. In relation to criminal offences laid down in the different *Länder* data protection laws a distinction needs to be made between *Antragsdelikte*, the prosection of which is dependent on the lodging of a complaint by the victim or alternatively the initiation of the prosecution by a competent public authority on the one hand and *Offizialdelikte* which can be prosecuted without such a special requirement. The latter is the case in most of the *Länder* jurisdictions, while six *Länder* pertain to the former system, at the same time enabling the respective Commissioner for Data Protection to initiate the prosecution.[110] Yet all this refers only to the initiation of prosecution based upon violations of the *Länder* data protection laws in the public sector.[111]

[74]. As regards the prosecution of violations committed in the non-public sector and the public sector at federal level article 44 para 2 FDPL establishes a general right of all supervisory authorities installed by the *Länder* Governments to initiate proceedings leading to criminal prosecution in accordance with article 38 para 6 FDPL.[112]

---

[109] S. Simitis *Kommentar zum Bundesdatenschutzgesetz* (5th edition, Baden-Baden, 2003), article 38 note 39 and A. Roßnagel/A. Pfitzmann/H. Garstka, *Modernisierung des Datenschutzrechts* [Modernisation of Data Protection Law], Gutachten im Auftrag des Bundesministeriums des Innern [Expert Opinion provided at the Request of the Federal Ministry of the Interior], 2001, p. 20, http://www.computerundrecht.de/media/gutachten.pdf (01.02.09).

[110] Art. 37 para 3 2nd sentence DPL Bayern, art. 32 para 3 1st sentence DPL Berlin, art. 38 para 3 2nd sentence DPL Brandenburg, art. 42 para 4 DPL Mecklenburg-Vorpommern, art. 22 para 8 DPL Sachsen-Anhalt, art. 42 para 4 DPL Thüringen.

[111] S. Simitis *Kommentar zum Bundesdatenschutzgesetz* (5th edition, Baden-Baden, 2003), article 44 para 2, note 17.

[112] S. Simitis *Kommentar zum Bundesdatenschutzgesetz* (5th edition, Baden-Baden, 2003), article 44 para 2, notes 13-15.

[75]. In any case, the subject of protection is the individual's constitutional right to informational self-determination based on article 2 para 1 in conjunction with article 1 para 1 of the Constitution also in the context of criminal prosecution. Therefore, the additional option to initiate proceedings is only supplementary and intended to be beneficial to the promotion of the individual's right to data protection as derived from the Constitution. This is one of the reasons why the victim is usually consulted by the competent Commissioner for Data Protection and criminal prosecution is not pursued without the victim's consent, even though, for example, the Data Protection Law of the *Land* Berlin in its article 32 para 3 3rd sentence specifically stipulates that criminal proceedings can be initiated also against the express will of the victim. However, in practice the reluctance to bring criminal complaints against the volition of the individual concerned accounts for the relatively small number of criminal proceedings in the field of data protection.

B.5. Sufficient powers sufficient for effective data protection

[76]. There is not much debate as to whether the commissioners for data protection should be given more powers by law, the question is rather whether they are sufficiently staffed and resourced to ensure effective data protection. Also, the question is discussed in the context of the extent of independence of the Commissioners for Data Protection.

B.6. Limitations of the data protection authorities' remit

[77]. The main limitations of the Federal Commissioner for Data Protection are those relating to the judiciary as well as those relating to the intelligence services. An exception to the general control competencies of the Federal Commissioner for Data Protection exists in relation to the limitation of the secrecy of letters, post and telecommunications through the activities of the intelligence services. Regarding the activities of the intelligence services, especially in relation to potential infringements of data protection rights, the *Parlamentarische Kontrollgremium* (PKGr) [Supervisory Committee of Parliament][113] and the so called *G 10 – Kommission* [Commission on Article 10 of the Constitution][114] have certain control competencies. In accordance with article 24 para 2 of the FDPL the Federal Commissioner for Data Protection is not competent for the control of personal data that are subject to the control by the

[113] http://www.bundestag.de/parlament/gremien/kontrollgremien/parlkon/index.html (01.02.09).
[114] http://www.bundestag.de/parlament/gremien/kontrollgremien/g10/index.html (01.02.09).

Commission on Article 10 of the Constitution. The G-10 Commission may give the Federal Commissioner for Data protection the right to deliver an opinion concerning data protection issues (art. 15 para 5 4th sentence *G-10-Gesetz)* [law on Art. 10].

[78]. In relation to the control of the federal courts, the competence of the Federal Commissioner for Data Protection is limited to matters of administration of justice. With a view to the independence of judges enshrined in article 97 of the Constitution, the judicial activity of the federal courts is exempted from the control of the Commissioner for Data Protection.

B.7. Allocated resources and effective use of powers

[79]. In accordance with article 22 para 5 3rd sentence of the FDPL, the Federal Commissioner for Data Protection has to be equipped with the personnel and other resources required for the fulfilment of his duties. The equipment has to be separately listed in the budget of the federal ministry of interior. Similar provisions exist in the data protection laws of the *Länder*.[115]

[80]. However, it has been a regular point of criticism that some of the Commissioners for Data Protection have not been equipped corresponding to the increasing demands as a result of the growing competence for the area of freedom of information as well as the private sector that were recently placed upon them.[116]

[81]. The budgets of Commissioners for Data Protection vary significantly and it is difficult to clearly assess the budgetary situation for each of their offices, especially since also other aspects have to be taken into consideration here, such as the population size of the particular *Land* or the level of business activities carried out on a territory of a specific *Land* (see above).

[82]. In general, the *Bundes* as well as the *Länder* Commissioners for Data Protection have often expressed their view that, by and large, they are in the position to carry out their tasks prescribed by law with the existing resources. However, reservations are usually made in relation

---

[115] See, for example art 26 para 4 DPL Baden-Württemberg, art. 29 para 4 DPL Bayern, art. 31 DPL Hessen.

[116] http://www.humanistische-union.de/publikationen/mitteilungen/hefte/nummer/nummer_detail/back/mitteilungen-201/article/freiheit-braucht-endlich-datenschutz-mit-kontrolle/ (25.01.09), http://www.heise.de/newsticker/Peter-Schaar-als-Bundesdatenschutzbeauftragter-im-Amt-bestaetigt--/meldung/119467 (25.01.09).

to (1) the control of the non-public sphere, for which resources are usually not sufficient[117], (2) the capacity of the Commissioners for data protection to proactively engage in control activities ('anlassunabhängige Kontrolle') rather than mainly reacting to complaints brought to their attention by individuals and (3) the huge additional burden that the supervision over the Law on freedom of information placed on them without increasing the required (corresponding) resources. However, it does not seem that the concerns go as far as to question the independence and/or the effectiveness of the data protection authorities as a whole as a result of the stretched resources.

B.8. Guarantees of independence

[83]. The lack of independence as a result of the subjection of the *Länder* Commissioners for Data Protection to the supervision of the authority of different state bodies is the subject of proceedings currently pending before the European Court of Justice (ECJ). An action (Case C-518/07) was brought by the Commission of the European Communities (EC Commission) on the 22nd November of 2007 against the Federal Republic of Germany seeking to establish that Germany has failed to fulfil its obligations under the second sentence of Article 28 para 1 of Directive 95/46/EC, by making the supervisory authorities responsible for the monitoring of data processing within the private sector in the *Länder* subject to state supervision and thereby incorrectly transposing the requirement of 'complete independence' of the data protection supervisory authorities.[118]

[84]. According to the European Commission's view the wording of article 28 para 1 clearly requires the supervisory authority to act "in complete independence in exercising the functions entrusted to them", which implies not only that there should not be any form of dependence on any party, but also that there should not be any dependence in any other respect. The rules of the Member States must

---

[117] See interview with the Federal Commissioner for Data Protection, Blickpunkt Bundestag Spezial, p. 12: „the data protection culture even within a number of bigger companies is not as advanced as we would expect. More control is needed which requires an increase of the funds for the supervisory authorities",
http://www.bundestag.de/blickpunkt/pdf/BB_0804_spezial.pdf (02.02.09).

[118] http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&newform=newform&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&alldocrec=alldocrec&docj=docj&docor=docor&docop=docop&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoj=docnoj&docnoor=docnoor&typeord=ALL&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&numaff=&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=C%E2%80%91518%2F07&resmax=100&Submit=Submit (16.12.2008).

therefore preclude external influence on the decisions of the supervisory authorities and on the implementation thereof. The concept of relative independence as described in the below and advocated by the Government of Germany, cannot be brought into conformity with the unambiguous, comprehensive wording of the directive. In addition, the second sentence of Article 28 para 1 of Directive 95/46/EC would be meaningless if the supervisory authorities operate in dependency from other institutions. It thus appears to be incompatible with the second sentence of Article 28 para 1 of Directive 95/46/EC to subject the supervisory authorities responsible for the monitoring of data processing in the private sector to technical, legal or administrative supervision by the State, as is the case in all 16 *Länder* of the Federal Republic of Germany to varying degrees, thus constituting a failure to fulfil the obligation to ensure the 'complete independence' of the supervisory authorities. Irrespective of the differences between legal [*Rechtsaufsicht*], technical [*Fachaufsicht*] and administrative [*Dienstaufsicht*] supervision, all these types of supervision constitute an infringement of the independence required by the directive.[119]

[85]. From a teleological point of view, the Community legislature regarded complete independence necessary so that the functions of the supervisory authority could be carried out effectively. The requirement of 'complete independence' of the supervisory authorities of the Member States also fits in systematically with the Community acquis existing in the area of data protection law. In addition, Article 8 of the Charter of Fundamental Rights of the European Union requires that compliance with the rules on the protection of personal data must be 'subject to control by an independent authority'.[120]

[86]. While only the supervisory authorities for the private sector at the level of the *Länder* are subject of the European Commission`s action, the Commission's arguments are valid also for the Federal Commissioner for Data Protection who is subject to legal and administrative supervision. The limited independence of the Commissioners for Data Protection including the Federal Commissioner has been criticized and discussed by experts[121], politicians[122] and NGOs[123].

---

[119] See the German version of the submission of the action for confirmation of the terminology: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:037:0008:0009:DE:PDF (16.12.2008).

[120] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:037:0008:0009:EN:PDF (16.12.2008).

[121] Roßnagel/A. Pfitzmann/H. Garstka, *Modernisierung des Datenschutzrechts* [Modernisation of Data Protection Law], Gutachten im Auftrag des Bundesministeriums des Innern [Expert Opinion provided at the Request of the Federal Ministry of the Interior], 2001, p. 19, 20 http://www.computerundrecht.de/media/gutachten.pdf (01.02.09); S. Simitis, *Kommentar zum*

[87]. In the German administrative system the legal supervision [*Rechtsaufsicht*] is characterized by the fact that the supervisory body may only review the legality of the act in question in a formal manner in order to assess whether the responsible state body has acted in conformity with the pertinent legal requirements and if required can order to remedy the situation. Therefore, this kind of supervision exclusively scrutinizes the procedural lawfulness and not the material/substantive appropriateness of the case at hand. It is also intended to give the citizen an additional recourse before having to resort to a judicial settlement of the dispute and at the same time to give the administration the chance to remedy its own mistakes by way of reassessment through the next higher administrative body.[124]

[88]. In contrast thereto the technical supervision [*Fachaufsicht*] extends far further and allows for a complete review of the legal correctness as well as the perceived substantive aptness of the decision reached by the lower administrative level. Thus the supervisory body possesses the power to order the lower level administrative body to take a decision in its favour and to act in accordance with what is materially preferred by the superior administrative entity. This denotes the very core of the hierarchical structure of administration as employed within the executive branch and therefore it is contrary to autonomy and independence.[125]

[89]. In turn, the administrative supervision [*Dienstaufsicht*] relates to merely organisational legal aspects of the interior structure of the entity in question and to personnel matters, specifically questions of the legal status of its employees, their salary status, promotion or degradation and other disciplinary measures. The supervisory body could thus interfere with the recruitment of personnel and influence decisions via an attitude of anticipatory obedience on the side of the

---

Bundesdatenschutzgesetz, 5th ed., Baden-Baden 2003, art. 22 FDPL notes 19, 26. See with respect to the validity of the European Commission´s arguments for the Fedeal level also the interview with the Federal Commissioner for Data Protection Peter Schaar See interview with the Federal Commissioner for Data Protection in: Datenschutz im Informationszeitalter [Data Protection in the Information Era], Blickpunkt Bundestag Spezial, October 2008, p. 10, http://www.bundestag.de/blickpunkt/pdf/BB_0804_spezial.pdf.

[122] See for example www.tauss.de/index.php?nr=15249&menu=1 and http://www.stokar.de/presse/76596.html.

[123] http://www.daten-speicherung.de/index.php/wie-unabhaengig-sind-staatliche-datenschutz aufsichtsbehoerden/.

[124] R. Schmidt *Allgemeines Verwaltungsrecht* (12th edition, Hamburg 2008), p. 440..

[125] R. Schmidt *Allgemeines Verwaltungsrecht* (12th edition, Hamburg 2008), p. 440.

employees who want to be promoted and act in conformity with their superiors for this very reason.[126]

[90]. The initial appeal of the EC Commission against Germany was pronounced in 2005 upon an individual's complaint of the year 2003.[127] In the meantime some amendments entered into force concerning the concretely relevant *Länder* data protection laws, which has led to a more differentiated overall picture. The administrative supervision of the Commissioners for Data Protection has been put in place for both their public and their private sector supervisory function and is largely exercised by the President of the Parliament, but also by the Ministry of the Interior,[128] the Government[129] or even the *Ministerpräsident*[130] [Prime Minister] of the respective *Land*. About half of the *Länder* Data Protection Laws tend to limit the ambit of the administrative supervision to some degree and install certain material and/or procedural safeguards to provide for more independence than is usually the case within the administrative hierarchy. In three *Länder* the pertinent provisions even explicitly prescribe that the exercise of the administrative supervision is contingent upon the preservation of the independence of the respective Commissioner for Data Protection,[131] which is the same legislative technique used to ensure the independence of judges when subjecting them to administrative supervision. Also in seven *Länder* jurisdictions specific limits are imposed on the concrete implementation of the administrative supervision.[132]

[91]. Across the board the exercise of the legal and technical supervision powers, where existent, has been designated to either the Government or the Ministry of the Interior. However, three mainly similar factions have to be distinguished according to the effects of supervisory instruments they are subjected to within the diverse group of *Länder* supervisory authorities for the non-public sector.

---

[126] http://www.daten-speicherung.de/data/Kommission_2005-07-05.pdf (16.12.2008).
[127] http://www.daten-speicherung.de/data/Kommission_2005-07-05.pdf (16.12.2008), http://www.daten-speicherung.de/data/Kommission_2006-12-14.pdf (16.12.2008).
[128] Art. 26 para 3 1st sentence DPL Baden-Württemberg, art. 21 para 3 3rd sentence DPL Nordrhein-Westfalen.
[129] Art. 25 DPL Bremen, art. 22 para 1 3rd sentence DPL Hamburg, art. 21 para 2 2nd sentence DPL Niedersachsen.
[130] Art. 35 para 5 1st sentence DPL Schleswig-Holstein.
[131] Art. 26 para 3 3rd sentence DPL Baden-Württemberg, art. 25 para 3 2nd sentence DPL Saarland, art. 25 para 4 2nd sentence DPL Sachsen.
[132] Art. 22 para 4 4th-8th sentence DPL Brandenburg, art. 32 para 2 2nd sentence and art. 21 para 4 4th sentence DPL Hessen, art. 29 para 6 2nd sentence DPL Mecklenburg-Vorpommern, art. 21 para 2 2nd sentence DPL Niedersachsen, art. 21 para 3 3rd sentence DPL Nordrhein-Westfalen, art. 21 para 1 2nd sentence DPL Sachsen-Anhalt, art. 26 para 2-6 DPL Thüringen.

[92]. The first group are those *Länder* which entrusted the task either directly to the Ministry of the Interior of their *Land*[133] or to regional administrative bodies[134]. In these jurisdictions the private sector supervisory authorities are integrated into the ordinary system of the administrative branch of the executive and are therefore automatically subject to the most comprehensive extent of supervision, that is legal, technical and administrative. In particular this mode of operation for the supervision of the private sector has also been criticised by the Federal Commissioner for Data Protection[135] in the 21st activity report[136] and the 70th Conference of the Commissioners for Data Protection of the *Bund* and the *Länder*[137].

[93]. Among those jurisdictions which assigned the supervision of the non-public sector to their *Länder* Commissioners for Data Protection there are two *Länder* which in their *Länder* Data Protection Laws explicitly subjected them to the same extensive degree of supervision as an ordinary administrative body, that is to say legal, technical and administrative as well.[138]

[94]. The last grouping also consists of those *Länder* which appointed their Commissioners for Data Protection as the supervisory authority for the private sector but in contrast to the previous group precisely regulated the scope of the supervision in such a way as to exclusively allow for legal supervision, thus forestalling any technical supervision which would amount to the possibility of influencing the material work of the data protection supervisory authorities in the non-public sector.[139]

[95]. One of the main arguments brought forward by the Government in the context of the infringement proceedings is that the model of complete independence is not known within the institutional system. Moreover,

---

[133] *Landesinnenministerium* Baden-Württemberg, *Landesinnenministerium* Brandenburg, *Landesinnenministerium* Saarland.

[134] Bayern: *Regierung* Mittelfranken; Hessen: *Regierungspräsidium* Darmstadt; Sachsen-Anhalt: *Landesverwaltungsamt*; Thüringen: *Landesverwaltungsamt*.

[135] http://www.bfdi.bund.de/cln_007/nn_533554/SharedDocs/Publikationen/PM30-05-01,templateId=raw,property=publicationFile.pdf/PM30-05-01.pdf (08.01.2009).

[136] 21st report on the activities of the Federal Commissioner for Data Protection for the years 2005-2006, pp. 17-18: http://www.bfdi.bund.de/cln_007/nn_531940/SharedDocs/Publikationen/-Taetigkeitsberichte/21-Taetigkeitsbericht-2005-2006,templateId=raw-,property=publicationFile.pdf/21-Taetigkeitsbericht-2005-2006.pdf (08.01.2009).

[137] http://www.bfdi.bund.de/cln_007/nn_533554/DE/Oeffentlichkeitsarbeit/-Entschliessungssammlung/DSBundLaender/70DSKUnabhaengigeDatenschutzkontrolleInDeutschlandGewaehrleisten,templateId=raw,property=publicationFile.pdf/70DSK-UnabhaengigeDatenschutzkontrolleInDeutschlandGewaehrleisten.pdf (08.01.2009).

[138] Art. 22 para 6 DPL Niedersachsen, art. 22 para 6 DPL Nordrhein-Westfalen.

[139] Art. 33 para 1 DPL Berlin, art. 33a DPL Mecklenburg-Vorpommern, art. 24 para 1 DPL Rheinland-Pfalz, art. 30a DPL Sachsen, art. 38 DPL Schleswig-Holstein.

complete independence would in fact constitute a violation of the principle of democracy. The principle of democracy as enshrined in article 6 para 1 of the EU Treaty, in article 20 para 2 of the Constitution and article 28 para 1 of the Constitution as well as the principle of parliamentary responsibility in fact require the subjection of officials to instructions of the competent minister who, in turn, is subject to parliamentary control.[140] The Data Protection Directive, in the opinion of the government, does not require institutional, but only functional and material independence of the supervisory authorities.

[96]. By way of conclusion the German supervisory regime would need to be regarded as inadequately ensuring the independence of its Commissioners for Data Protection in more than just the reprimanded regard, but in its entirety. As has been detailed above, not only are the *Länder* Commissioners for Data Protection supervised in different degrees in respect of their activities in the non-public sector but also their work in the public sector is subject to administrative supervision. Moreover, in the sphere of data protection as regards public activities the Federal Commissioner for Data Protection is subjected to legal and administrative supervision as well.[141] Thus, if a strict approach were to be consistently applied, the whole German data protection system in all of its aspects would have to be deemed inadequate in so far as the complete independence of the Data Protection Commissioners is concerned. The offices of the commissioners should be totally dissolved from their respective administrative connection in order for the system to be compliant with Directive 95/46/EC. Some actors also mention as potential comparative model a couple of institutions that are in fact completely independent, such as the *Bundesbank* [Federal Bank][142], the *Bundesprüfstelle für jugendgefährdende Schriften* [Federal Department for Media Harmful to Young Persons][143] as well as the *Kommission für Jugendmedienschutz* [Commission for Media Harmful to Young Persons][144][145] which would counteract the argument broad forward by

---

[140] Letter of the German Government to the European Commission of 13 February 2007, referenced in a statement of the Minister of Interior of the Parliament of Baden-Württemberg on 'Data Protection in accordance with European Standards' of 3 August 2007, Ds. 14/1636, http://www3.landtag-bw.de/WP14/Drucksachen/1000/14_1636_D.PDF (02.02.09).

[141] Pursuant to article 22 para 4 FDPL the Federal Commissioner for Data Protection and Freedom of Information is independent in the exercise of his duties and subject only to the law. Nevertheless he is subject to the *Rechtsaufsicht* [legal supervision] of the Federal Government. According to article 22 para 5 FDPL the office of the Federal Commissioner for Data Protection and Freedom of Information is established with the Federal Ministry of the Interior and is subject to the *Dienstaufsicht* [administrative supervision] of the Federal Minister of the Interior.

[142] http://www.bundesbank.de/index.en.php (25.01.09).

[143] http://www.bundespruefstelle.de/bmfsfj/generator/bpjm/information-in-english.html (25.01.09).

[144] http://www.kjm-online.de/public/kjm/ (02.02.09).

the government that the model of complete independence is not known within the German system.

B.9. Powers to become active at own initiative

[97]. In accordance with the Federal Data Protection Law as well as with the Data Protection Laws of the *Länder*, the Commissioners for Data Protection can become active on their own initiative in various situations. However, it seems that the extent to which actions are in fact taken proactively in practice is very determined by the human and financial resources that the authorities are equipped with. While many Commissioners for Data Protection seem to be able to go beyond the scope of only dealing with matters that they are approached with by individuals, others do not seem to have this possibility at all.

B.10. Monitoring role

[98]. The mandates of the Commissioners for Data Protection also imply strong monitoring roles. As described above, the Commissioners for Data Protection have the responsibility to control the application of the relevant data protection legislation in the institutions and organisations within their competence. In support of the mandate of the Commissioners, the relevant laws regulate the obligation on the side of the authorities/institutions under the jurisdiction of the Commissioner for Data Protection to cooperate with the Commissioners and their staff by providing responses to questions raised by the Commissioners, by allowing the Commissioners to inspect files and to access their offices.[146]

---

[145] See expert opinion provided by the Commissioner for Data Protection of Berlin at an expert hearing before the Committee for Interior of the Parliament of the Land Sachsen of 14 September 2006, Protocol in accordance with article 36 of the Rules of Procedure of the Parliament of Sachsen, PD 3.4 Apr 4/6-21 A, p. 11.

[146] Art. 24 para 4 FDPL, art. 29 DPL Baden-Württemberg, art. 32 DPL Bayern, art. 28 para 1 DPL Berlin, art. 26 para 1 DPL Brandenburg, art. 27 para 2 DPL Bremen, art. 23 para 5 DPL Hamburg, art. 24 paras 3 and 4 DPL Hessen regulate the duty to cooperate with the Commissioner for Data Protection in a rather general way („The Commissioner for Data Protection of Hesse cooperates with authorities and other competent bodies responsible for the control and compliance with data protection regulations of the Federation and the Länder. For the purposes of cooperation, the Commissioner may demand information from the authorities responsible for the non-public bodies in accordance with the Federal Data Protection Law."), art. 31 DPL Mecklenburg-Vorpommern, art. 22 para 4 DPL Niedersachsen, art. 22 para 2 DPL Nordrhein-Westfalen, art. 28 para 1 DPL Rheiland-Pfalz, art. 28 para 1 DPL Saarland, art. 28 para 1 DPL Sachsen, art. 23 para 1 DPL Sachsen-Anhalt, art. 41 para 1 DPL Schleswig-Holstein, art. 28 para 1 DPL Thüringen. Some laws even make explicit reference to duties to keep official or professional secrets ('Berufs- oder Amtsgeheimnisse'), not releasing the official or professional from the duty to cooperate with the Commissioner, for example art. 28 para 2 DPL Berlin, art. 26 para 3 DPL Brandenburg, 23 para 5 3rd sentence DPL Hamburg.

[99]. The Commissioner informs the controlled authority about the result of the control. At the same time he can make recommendations for the improvement of data protection, particularly regarding the remedy of detected flaws in the processing or use of personal data. He may also inform the data subject affected by the infringements.

[100]. In addition, the Commissioners have the competence to react to data protection *violations* by way of interceptions ('Beanstandungen'). All data protection laws[147] provide for the possibility of the Commissioner to issue interceptions to the responsible supervisory authority in case a data protection violation or other flaws in the context of the processing or use of personal data are detected within an institution under their jurisdiction. In addition, the Commissioners can request opinions from the authority concerned within a time limit determined by them. The opinion shall also include a description of measures taken in response to the interception of the Commissioner for Data Protection. In case the control is carried out by the Federal Data Protection Commissioner, corporations, institutions and foundations under public law ('Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts') shall send a copy of their opinion for the Commissioner for Data Protection also to the competent supervisory authority.[148]

[101]. In their activity reports the Commissioners for Data Protection mention cases where data protection violations or flaws were identified and how the relevant institutions reacted following the involvement of the Commissioners for Data Protection. Thus, the reporting performed by the Commissioners also has a very strong monitoring function.

[102]. However, reports from relevant officials often indicate that it is very difficult to clearly demonstrate the effects of the monitoring activities. In any event, the proceedings in that context can be very effective, and very often flaws are remedied as a result of the communication with the Commissioner without involving the formal procedure of interceptions.

---

[147] Art. 25 Federal Data Protection Law, art. 30 DPL Baden-Württemberg, art. 31 para 1 DPL Bayern, art. 26 para 1 DPL Berlin, art. 25 DPL Brandenburg, art. 29 para 1 DPL Bremen, art. 25 DPL Hamburg, art. 27 para 1 DPL Hessen, art. 32 DPL Mecklenburg-Vorpommern, art. 23 para 1 DPL Niedersachsen, art. 24 para 1 DPL Nordrhein-Westfalen, art. 25 para 1 DPL Rheinland-Pfalz, art. 27 para 1 DPL Saarland, art. 29 DPL Sachsen, art. 24 para 1 DPL Sachsen-Anhalt, art. 42 para 2 DPL Schleswig-Holstein, art. 39 para 1 DPL Thüringen.

[148] Art. 25 para 3 FDPL. Similar regulations exist in the data protection laws of the Länder, for example, art. 31, 32 DPL Bayern.

[103]. Data protection violations are detected both through independent monitoring and control activities of the Commissioners as well as by affected individuals. However, very often the affected individuals are not even informed about the violation of their rights. Therefore, the introduction of a duty to inform the data subjects in cases of (unintentional) violations of data protection rights would strengthen the enforcement of data protection legislation.[149]

[104]. In addition, there is often a problem in relation to sensitive information provided by individuals as there is no effective legislation in force for the protection of the so-called "whistleblowers". It appears that many of the recent data protection scandals, such as the secret video surveillance of employees of the supermarket chain Lidl[150] or the spying of telephone data within Telekom[151], were only brought to light because employees revealed internal proceedings of the company in (potential) violation of relevant employment legislation.[152] Employees expose themselves to substantial risks through revealing violations of law committed by their employers. The law does not clearly regulate how to deal with the conflict between the public interest in the disclosure of deficiencies in companies and administrations on the one side and the duties of the employee towards the employer as regulated in civil and employment law on the other side. The Constitutional Court, in a decision of July 2001, held that the citizens' duty to give statements in criminal proceedings before the Prosecutor's Office must not, in principle, lead to any disadvantage for the employee in the area of civil law.[153] The *Bundesarbeitsgericht* (BAG) [Federal Labour Court] developed further guidelines on the basis of the Constitutional Court's decision and held that the employee cannot be expected to seek clarification within the company if he finds out about serious criminal offences committed by the employer and if the employee himself exposes

---

[149] See interview with the Federal Commissioner for Data Protection in: Datenschutz im Informationszeitalter [Data Protection in the Information Era], Blickpunkt Bundestag Spezial, October 2008, p. 12, http://www.bundestag.de/blickpunkt/pdf/BB_0804_spezial.pdf, http://www.stokar.de/bundestag/antraege/197009.html (02.02.09), https://www.datenschutzzentrum.de/bdsg-novellierung/20080924-uld-aenderungsbedarf-bdsg.pdf (02.02.09).

[150] See http://www.rp-online.de/public/article/wirtschaft/news/548074/Innenministerium-leitet-Ermittlungen-ein.html (22.01.09).

[151] See http://www.heise.de/newsticker/Telekom-droht-Geldbusse-bis-zu-einer-Million-Euro--/meldung/108981 (22.01.09).

[152] A. Bugg, D. Beier, Whistleblower - Hinweisgeber mit Zivilcourage, Wissenschaftliche Dienste des Deutschen Bundestages no. 06/09 (21 January 2009), http://www.bundestag.de/wissen/analysen/2009/whistleblower.pdf (22.01.09).

[153] Germany/Bundesverfassungsgericht/Decision of 2 July 2001, case no.: 1 BvR 2049/00, para II.1. b) cc) bbb), http://www.lexrex.de/rechtsprechung/entscheidungen/searchresults/286.html (26.01.09).

himself to criminal prosecution if he does not report the offence.[154] The new *Beamtenstatusgesetz* [Law on the Status of Civil Servants][155], which is expected to enter into force shortly, now includes a provision which annuls the duty to remain silent under civil service law. In the area of employment, the draft *Arbeitsvertragsgesetz* [Law on the Employment Contract][156] includes a similar provision, however, for various reasons the law is not likely to be adopted in the near future.[157]

[105]. The extent to which the Commissioners for Data Protection can in fact operate in a proactive way very much depends on their budgetary and human resources situation.[158]

B.11. Availability of decisions

[106]. The Federal Commissioner as well as the *Länder* Commissioners and the authorities for the non-public sector all issue various forms of decisions and opinions. These include formal opinions delivered at various stages of the legislative process or the joint decision ('Entschließungen') taken by the Data Protection Conference or the Düsseldorf Circle (see above). These decisions are all available on the homepage of the Federal Data Protection Officer as well as on the homepages of most *Länder* Commissioners. In addition, they are distributed to the relevant actors. The activity reports of the Commissioners for Data Protection are made public in the same way (details see below).

[107]. In relation to the involvement of the Commissioners for Data Protection in the legislative proceedings, it depends on whether the opinion was provided as an opinion during the drafting processes within in the government or as an opinion for expert hearings of the

---

[154] Germany/Bundesarbeitsgericht, Judgement of 3rd July 2003, case no.: 2 AZR 235/ 02, http://lexetius.com/2003,3463 (26.01.09).

[155] http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Common/Anlagen/Gesetze/Beamtenstatusgesetz,templateId=raw,property=publicationFile.pdf/Beamtenstatusgesetz.pdf (26.01.09).

[156] http://www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F0A-72F79883/bst/Diskussionsentwurf_August2006.pdf (22.01.09)

[157] A. Bugg, D. Beier, Whistleblower-Hinweisgeber mit Zivilcourage, Wissenschaftliche Dienste des Deutschen Bundestages no. 06/09 (21 January 2009), http://www.bundestag.de/wissen/analysen/2009/whistleblower.pdf (26.01.09). The protection of whistleblowers was recently the subject of a public hearing where consideration was given to include a relevant provision in article 612 a of the Civil Code, http://www.bundestag.de/aktuell/archiv/2008/20612996_kw23_ernaehrung/index.html (26.01.09).

[158] http://www.bfdi.bund.de/cln_007/nn_531002/sid_41D4163A1A85BAA275285EB8D9936E54/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM__35__08__BMIGesetzesentwurf.html.

relevant committees of Parliament. The former opinions are not accessible. Concerning the latter opinions for the Parliament there is no legal obligation to grant access to expert opinions. However, in practice those opinions are usually easy to obtain through the services of the relevant parliament. In cases where opinions are not made public, the Commissioners can decide to issue press statements and/or other public decisions on a given matter.

B.12. Opinions of the Working Party established under Article 29 of Directive 95/46/EC

[108]. Consideration of opinions of the Working Party under article 29 of Directive 95/46/EC by the data protection authority appears to be the constant practice. The opinions are widely used and referred to in the work of the Data Protection authorities[159], which is also due to the fact that translated copies of the opinions are made available on the homepage of the Federal Commissioner for Data Protection and Freedom of Information and of a couple of other data protection authorities.[160]

[109]. The opinions of the Article 29 Working Group usually represent a source of inspiration and very often the position of the Working Group is directly taken up and used to support the position of the data protection commissioners in their advisory and other activities.

[110]. For example, the Federal Commissioner for Data Protection usually reiterates the relevant recommendations of the article 29 group in his own activity reports[161], recently very strongly for example in the context of Binding Corporate Rules ('unternehmensinterne Regeln')[162] and lists all opinions of the article 29 group delivered during his reporting period at the end of the activity report.

[111]. However, the opinions are not considered binding and the extent to which the various opinions in fact impact on the work of the

---

[159] See, for example, the last activity report of the Federal Commissioner for Data Protection covering the years 2005 and 2006, pp. 31-33, http://www.bfdi.bund.de/cln_007/nn_531940/SharedDocs/Publikationen/Taetigkeitsberichte/21-Taetigkeitsbericht-2005-2006,templateId=raw,property=publicationFile.pdf/21-Taetigkeitsbericht-2005-2006.pdf (02.02.09).

[160] http://www.bfdi.bund.de/cln_007/nn_532072/DE/EuropaUndInternationales/Art29Gruppe/Artikel/DatenschutzgruppeArt29EG.html (02.02.09).

[161] For example in the last activity report covering the years 2005 and 2006, pp. 33, 34, 35, 54, 109, 110.

[162] Activity report of the Federal Commissioner for Data Protection covering the years 2005 and 2006, p. 35.

individual Data Protection Commissioners depends on the subject matter at hands.

B.13. Advisory role and consultation during the legislative process

[112]. A general competence of the Commissioners for Data Protection to provide advice to the relevant institutions is included in most data protection laws. Many laws make a general reference to the term advice ('Beratung').[163] For example, in accordance with article 24 DPL Berlin the Commissioner for Data Protection controls the requirements of this law and of other data protection provisions within authorities and other public bodies. To that end he can issue recommendations for the improvement of data protection and in particular, can advise the senate and individual members of the senate in data protection matters. Article 23 para 2 DPL Brandenburg as well as other *Länder* laws provide for similar responsibilities. There is, however, no duty to generally consult or to seek the advice from the Commissioner for Data Protection on the side of the authorities or a duty of the Commissioner for Data Protection to provide advice.

[113]. In addition, a number of other competences of the Commissioners are clearly advisory activities, such as the competence to issue position papers ('Stellungnahmen') expert opinions ('Gutachten') and recommendations ('Empfehlungen') at the request of the competent *Länder* governments or parliaments.

[114]. The activity reports of the Commissioners for Data Protection which they are obliged by law to prepare annually or bi-annually also fulfil an important advisory function.[164] These reports do not only highlight the main areas of (past) activity of the commissioners, but also anticipate important upcoming data protection issues.[165] In many cases, they reiterate the advice and recommendations made by the commissioners during the reporting period. In that context it is also important to note that the reports of the Commissioners for Data

[163] Art. 26 para 3 FDPL, art. 31 para 3 DPL Baden-Württemberg, art. 24 para 1 DPL Berlin, art. 23 para 2 DPL Brandenburg, art. 27 DPL Bremen, art. 23 para 2 DPL Hamburg, art. 24 para 1 DPL Hessen, art. 33 para 2 DPL Mecklenburg-Vorpommern, art. 22 para 1 DPL Niedersachsen, art. 22 para 1 DPL Nordrhein-Westfalen, art. 24 para 4 DPL Rheinland-Pfalz, art. 26 para 2 DPL Saarland, art. 30 para 4 DPL Sachsen, art. 22 para 4 DPL Sachsen-Anhalt, art. 39 para 3 DPL Schleswig-Holstein, art. 40 para 3 DPL Thüringen. The DPL Bayern does not explicitly speak of the competence of the Commissioner to give advice.

[164] For a list of activity reports submitted by the relevant authorities see http://www.rewi.hu-berlin.de/jura/etc/lwk/DOK/Datenschutz-TBe.pdf (03.02.09).

[165] H. Heil in: A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 773.

Protection are presented to the respective parliaments by way of formal procedure, i.e. during an official briefing ('Unterrichtung'). The parliaments and/or the relevant committees within parliament, on the basis of the annual or bi-annual activity reports of the commissioners, then issue decisions and in this way also take a position on essential legal and policy issues in the area of data protection.[166] In many cases parliament takes up the Commissioners' recommendations by way of decisions and request the government to take the required action (for example, to start a legislative procedure or to take a certain position in the context of international cooperation with third countries). However, it seems that these parliamentary decisions are often taken with a considerable delay.[167]

[115]. The activity reports of the Commissioners for Data Protection and of the supervisory authorities for data protection have proved to be an effective instrument for the implementation and improvement of data protection and have significantly contributed to its development. They demonstrated that prohibition and ordering competences (which the Federal Data Protection Commissioner does not have) are not the essential criteria for the effectiveness of a data protection control institution, and that results can also be achieved in other ways, namely through publication of control results. Since the means of information, education and constructive criticism are characteristic for the work of the Federal Commissioner for Data Protection, he is occasionally described as a "persuasive authority".[168]

[116]. During the legislative procedure the Commissioners can be consulted at various phases and can be given the opportunity to provide detailed opinions on relevant laws. A distinction though has to be made

---

[166] See in relation to the federal level „Beschlussempfehlung und Bericht des Innenausschusses zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz, Tätigkeitsbericht 2003 und 2004 des Bundesbeauftragten für den Datenschutz" [Recommendation for a decision and report of the Committe for the Interior on the official briefing by the Federal Commisssioner for Data Protection, activity report 2003 and 2004 of the Federal Commissioner for Data Protection], BT-Drs 16/4882 of 28 March 2007, http://www.bfdi.bund.de/cln_027/nn_531940/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/TaetigkeitsberichteDesBFD.html (20.01.09), and for example Bremen, „Stellungnahme des Senats zum 30. Jahresbericht des Landesbeauftragten für Datenschutz", Mitteilung des Senats vom 19. August 2008 [Statement of the senate on the 30th annual report of the Commissioner for Data Protection], Drs. 17/509, http://www.datenschutz-bremen.de/pdf/stellungnahme_30.pdf (22.01.09), in relation to Baden-Württemberg http://www.landtag-bw.de/wp13/drucksachen/2000/13_2640_d.pdf. (03.02.09).

[167] For example, the respective decision taken in relation to the 20th activity report of the Federal Commissioner for Data Protection covering the period 2003 and 2004 was only taken on 29 March 2007, http://www.bfdi.bund.de/cln_007/nn_531940/SharedDocs/Publikationen/BT-Drs16__4882.html (02.02.09).

[168] H. Heil in: A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 774, U. Damann in S. Simitis, *Kommentar zum Bundesdatenschutzgesetz*, 5th ed., Baden-Baden 2003, art. 24 note 3.

between the preparatory phase of a piece of legislation, i.e. the phase when the law is being prepared within the competent ministry of government and before the draft is officially introduced into the legislative process, the so called "officer draft" ('Referentenentwurf') and the phase when the draft is pending in parliament.

[117]. The Commissioners for Data Protection are often already consulted during this first phase of a draft law even though there is no legal requirement to consult them at that phase, with the exception of rules 21 para 1 and 45 para 3 of the *Gemeinsame Geschäftsordnung der Bundesministerien* (GGO) [Joint Rules of Procedure of the Federal Ministries] of December 2006, according to which the Federal Commissioners, including the Federal Commissioner for Data Protection, have to be consulted in all matters/projects ('Vorhaben') affecting their area of responsibility already at an early stage.[169] While the respective Joint Rules of Procedure of the *Länder* ministries also regulate the involvement of the Commissioners for Data Protection, they do not all make reference to their involvement "at an early stage".[170]

[118]. Therefore, the involvement of the Commissioners takes place to varying degrees, ranging from extensive involvement to sometimes exclusion in situations where it would be appropriate for the Commissioners to be involved.[171] It is also possible that given the general fragmentation of data protection legislation and also the stretched resources within most if not all offices of the Commissioners for Data Protection, which does not enable the commissioners and their staff to always proactively find out about planned or pending legislation, relevant information about draft laws is often provided only when the law has been introduced into the parliamentary process already, when it usually becomes more difficult

---

[169] Rule 21 of the Joint Rules of Procedure of the Federal Ministries provides as follows: "Cooperation with the Commissioners of the Government and the Federal Commissioners.
(1) The Commissioners of Government and the Federal Commissioners (Annex 3 of the Joint Rules of Procedure) shall be involved in all matters affecting their area of responsibility at an early stage.
(2)…"
Rule 45 (3) of the Joint Rules of Procedure of the Federal Ministries (contained in the relevant Chapter 6 –Legislation, provides an identical provision for the legislative procedure. Annex 3 to the Rules 21 and 45 specifically lists the Federal Commissioner for Data Protection and the other Federal Commissioners and Commissioners of Government. http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2007/GGO,templateId=raw,property=publicationFile.pdf/GGO.pdf (22.01.09).

[170] See, for example, Rule 40 of the Joint Rules of Procedure of the Ministries of the Government of Sachsen, http://www.landtag.sachsen-anhalt.de/fileadmin/downloads/GO-Ministerien_01.pdf (02.02.09).

[171] In some cases relevant provisions infringing upon data protection rights are hidden somewhere in legislation so that it can be difficult for the Commissioner to identify the relevant points.

for the Commissioner to influence the shape and content of a given law.

[119]. In general it is difficult to assess the impact of the advice provided by the commissioners since information on advisory activities during the preparatory drafting phase is not easy to obtain and since the contacts of the Commissioners with the relevant actors within government are usually not displayed in public. However, it seems that at this phase the involvement and impact of the Commissioner's advice can be most effective. Many commissioners report that they have good cooperation with their relevant counterparts in the ministries.

[120]. The Commissioners for Data Protection are also frequently involved once legislation is pending in parliament. During this phase, the Commissioners for Data Protection are often appointed as experts who provide opinions during the hearings of the relevant committees of parliament.[172] However, an obligation to be consulted is not expressly regulated in all Data Protection Laws.[173] Only the data protection laws of Baden-Württemberg, Brandenburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Rheinland-Pfalz and of Sachsen expressly provide for the involvement of the Commissioner for Data Protection in legislative proceedings[174], with the data protection laws of Sachsen, Mecklenburg-Vorpommern and Niedersachsen even stipulating an obligation to hear the Commissioner for Data Protection on drafts of regulations and administrative directives if they affect the right to informational self-determination.[175] In the absence of a clear legal obligation, the Commissioners for Data Protection are often "only" invited as experts by way of nomination by a certain political group. A detailed list outlining the competences of the Commissioners for Data Protection within the various jurisdictions, including their involvement in the legislative process can be found in Annex 4 of this report.

---

[172] In accordance with Rule 70 para 1 of the Rules of Procedure of the Bundestag (first chamber of Parliament), a committee can organize public hearings of experts, stakeholders (Interessenvertreter) and other persons on a subject of consultation, and in case the matter is referred to the committee the committee is obliged to hear experts if one quarter of its members so requests.

[173] The laws that do not clearly regulate an obligation to involve the Commissioner for Data Protection are the Federal Data Protection Law as well as the data protection laws of Bayern, Berlin, Bremen, Hamburrg, Nordrhein-Westfalen, Saarland, Sachsen-Anhalt, Schleswig-Holstein, Thüringen.

[174] Art. 31 para 3 2nd sentence DPL Baden-Württemberg, art. 23 para 5 DPL Brandenburg, art. 21 para 5 DPL Hessen, art. 33 para 2 4th sentence DPL Mecklenburg-Vorpommern, art. 22 para 1 4th sentence DPL Niedersachsen, art. 23 para 8 DPL Rheinland-Pfalz, art. 26 DPL Sachsen.

[175] Art. 33 para 2 4th sentence DPL Mecklenburg-Vorpommern, art. 22 para 1 4th sentence DPL Niedersachsen, art. 26 DPL Sachsen.

[121]. By way of example, the Federal Commissioner as well as a couple of *Länder* Commissioners for Data Protection were recently included in the list of experts for a hearing on the adoption of a law on a data protection audit[176]. In the case of amendments to the data protection law of, for example, Sachsen, a couple of Commissioners from other *Länder* were heard as experts.[177]

B.14. Awareness raising role of the data protection authorities

[122]. The Federal Commissioner for Data Protection, in accordance with article 26 para 1 1st sentence, "informs Parliament and the public about essential developments in data protection" and thus his responsibility for awareness raising is already built into law.

[123]. In general, awareness raising activities are probably the most important and at the same time most effective activities carried out by the commissioners for data protection. Data protection has become an important topic of discussion in the media as well as in the political debates.

[124]. Awareness raising is mainly performed through the preparation and distribution of the activity reports. The law does not provide for details in relation to the content of the activity report, but in any event, the activity report is more than a simple record of activities by the Commissioner for Data Protection who, most importantly, uses the report to present both to Parliament and to the public the most important results of his activity, to point out specific problems in the area of data protection, to present his further considerations on relevant matters and to initiate public debates.[178] The activity reports are distributed widely (not only to the respective Parliaments, but also to administrations, institutions for vocational training and associations, amongst others) and thus have a very important multiplier function.[179]

[125]. All Commissioners for Data Protection have comprehensive homepages with extensive information on their mandates and

[176] http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung05/Stellungnahmen/index.html (02.02.09).

[177] See expert opinions provided by the Commissioner for Data Protection of Berlin and others at an expert hearing before the Committee for Interior of the Parliament of the Land Sachsen of 14 September 2006, Protocol in accordance with article 36 of the Rules of Procedure of the Parliament of Sachsen, PD 3.4 Apr 4/6-21 A.

[178] H. Heil in: Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 774.

[179] H. Heil in: Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 774.

activities and they distribute brochures and other information material to the public.

[126]. Awareness raising by the Commissioners for Data Protection is performed through work with the media and also the organization of expert events. In many cases the Commissioners initiate and/or actively participate in public debates, conferences and workshops on data protection topics.[180]

3. Compliance

A. Registration of data processing operations and duties of requesting approval of sensitive data processing operations

[127]. In accordance with article 4 d of the Federal Data Protection law and the relevant provisions of the *Länder* Data Protection Laws, non-public bodies have a duty to notify ('Meldepflicht') automated data processing operations prior to their implementation to the supervisory authority or the competent Commissioner for Data Protection; public bodies of the Federation have to announce them to the Federal Commissioner for Data Protection in accordance with the procedure laid down in article 4 e of the FDPL. Relevant amendments of the Federal Data Protection Law entered into force in 2001 also introducing a couple of exceptions from the notification duty so that the duty has become an exception rather than the rule.[181] For example, the notification duty does not apply to bodies that process data for others within the framework of an assignment. Also, the notification duty does not apply in case the responsible body has appointed a data protection officer ('Beauftragten für den Datenschutz') in accordance with article 4 d para 2 FDPL.[182] This provision constitutes an exception from the general notification duty in accordance with article 18 para 2 of Directive 95/46 EC.[183]

---

[180] http://www.bfdi.bund.de/cln_007/nn_533554/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/redenInterview__node.html__nnn=true (02.02.09).

[181] See, 2nd activity report of the Ministry for the Interior of the Land Baden-Württemberg covering the period 1st July 2001 until 1st July 2003, pp. 6-7, http://www.landtag-bw.de/wp13/drucksachen/2000/13_2200_d.pdf (02.02.09); R. Hillenbrand-Beck in: A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, pp. 831-833.

[182] See, amongst others, information provided by the Commissioners for Data Protection or supervisory authorities on the notification duty, *Landesverwaltungsamt* Thüringen, http://www.thueringen.de/de/tlvwa/inneres/hoheit/datenschutz/register/content.html. (02.02.09), https://www.datenschutzzentrum.de/download/merkmeld.pdf (02.02.09).

[183] On the history of article 18 para 2 of the EC Directive 95/46/EC and the involvement of German authorities see R. Hillenbrand-Beck in: A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, pp. 831-833.

[128]. Obligatory registration shall further not apply if the controller collects, processes or uses personal data for its own purposes, provided that a maximum of nine employees are involved in the collection, processing or use of personal data and either consent has been obtained from the data subject or the collection, processing or use serves the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject.[184]

[129]. Para 5 of article 4 d FDPL goes further in that it requires a control to be carried out prior to the commencement of the processing (prior checking) in case the automated processing involves special risks for the rights and freedoms of the persons concerned, particularly if special categories of personal data (meaning information on a person's racial and ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life, i.e. sensitive data, article 3 para 9 FDPL) are being processed or if the processing of personal data is intended to appraise the data subject's personality, including his abilities, performance or conduct.

[130]. The notification duty and the corresponding duty to keep a register have been subject to regulation on the basis of article 18 para 2 of Directive 46/95 EC in Germany. With the possibility to appoint the relevant data protection officials within the respective institutions[185], the relevant previously established practice regarding data protection registers was substantially amended.[186]

B. Appointment of data protection officers

[131]. In accordance with article 4 f para 1 FDPL all public bodies at the federal level and all non-public bodies which process personal data in

---

[184] Art. 4 d para 3 FDPL.

[185] See below, para 16 on administrative and internal data protection officers.

[186] See, for example the relevant information on the data protection registers in Baden-Württemberg: Until the entry into force of the amendments to the FDPL in May 2001 1.369 data processing bodies subject to the notification duty were registered. After the implementation of the new legislation only 72 bodies with in total 74 automated processing activities are registered, 2nd activity report of the Ministry for the Interior of the Land Baden-Württemberg covering the period 1st July 2001 until 1st July 2003, p. 7, http://www.landtag-bw.de/wp13/drucksachen/2000/13_2200_d.pdf (02.02.09). See also, the 20th activity report of the Commissioner for Data Protection of Rheinland-Pfalz for the period 1st October 2003 to 30 September 2005 which discusses the matter of data protection registers required in accordance with article 27 of the DPL Rheinland-Pfalz, mentioning, by way of background, the registration of 3200 processing activities for the year 1986 which had increased to 9200 in the year 2005, p. 92, http://www.datenschutz.rlp.de/downloads/tb/tb20.pdf (02.02.09), whereas the 21st activity report covering the period 2006 and 2007 does not make reference to the registers, http://www.datenschutz.rlp.de/downloads/tb/tb21.pdf (02.02.09).

an automated way are obliged to appoint a data protection officer in written form. In so far as the Federal Data Protection Law prescribes a duty of all responsible bodies to appoint a data protection officer, it goes beyond the requirements of article 18 para 2 of Directive EC/95/46. However, some limitations of the duty to appoint data protection officers were introduced in 2006. The duty to appoint data protection officers does not apply to private bodies which generally employ a maximum of nine employees to carry out the automated processing of personal data on an ongoing basis, unless they carry out automated processing operations which are subject to prior checking or they process personal data in the course of business activities for the purposes of transfer or anonyms transfer.

[132]. Under the influence of the EC data protection directive almost all *Länder* have either envisaged[187] or prescribed[188] the appointment of a data protection officer in public *Länder* bodies by law.

B.1. Data protection officers in private bodies and public bodies at the federal level

[133]. According to article 4 f and g of the Federal Data Protection Law public bodies at the federal level and non public bodies are obliged to appoint such an officer within a month after commencement of their activities. The same applies if personal data are collected, processed and used in a different way and if usually at least 20 persons are involved in these activities.

[134]. The decision about the person to be appointed as data protection officer rests with the responsible public or non-public body. Very often companies also use the possibility to appoint external data protection officers who either support an internal officer in the discharge of his or her duties or who provide relevant data protection services independently.[189] At the same time, the data protection officer is often supported by persons responsible for data protection ('Datenschutzverantwortliche') who carry out clearly defined tasks within companies which have established a systematic organisation of data protection. Sometimes they develop into real experts in their area

[187] Art. 10 DPL Baden-Württemberg, art. 10 DPL Schleswig-Holstein, art. 8 DPL Saarland.

[188] For example art. 19a para 1 DPL Berlin, art. 7a DPL Brandenburg, art. 5 DPL Hessen; art. 8a para 2 DPL Niedersachsen, art. 32a DPL Nordrhein-Westfalen, art. 11 DPL Rheinland-Pfalz, art. 10a DPL Thüringen.

[189] See R-B. Abel in A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 905, Germany/Bundesarbeitsgericht [Federal Labour Court]/ Judgement of 13 March 2007, case no.: 9 AZR 612/05, http://datenschutz.eu/urteile/Bundesarbeitsgericht--20070313.html

of responsibility, and the data protection officer can rely on their expertise.[190]

[135]. In accordance with article 4 f para 2 FDPL only a person with the knowledge and trustworthiness required for the fulfilment of these obligations may be appointed as data protection officer. The level of knowledge required depends on the amount and extent of data processing of the relevant institution as well as the need for protection of personal data which the institution collects or and processes, an amendment introduced in August 2006. This amendment addresses what was shown already in practice, that is, that there can neither be a comprehensive standard education nor detailed requirements for the qualification of data protection officers in all kinds of companies.[191] No clear regulation exists, however, regarding the education and training for data protection officers. [192]

[136]. The appointment can only take place on a voluntary basis and the data protection officer shall be directly subordinate to the head of the public or private body. He shall be free in the use of his specialised knowledge and free from instructions in the area of data protection. Appointed and acting data protection officers must not be disadvantaged as a result of their activities ('Benachteiligungsverbot').

[137]. According to article 4 f para 3 4th sentence the appointment of data protection officers can be withdrawn only in exceptional cases, if the responsible body cannot reasonably be expected to keep the person as a data protection officer[193] or – in private bodies – at the request of the supervisory authority.

[138]. The form of appointment and resignation ('Abberufung') has been the subject of case law.[194] It is important to note that the regulations of the FDPL on the appointment of data protection officers do not exclude the possibility of a regular dismissal by way of proper notice of

---

[190] W. Hülsman/K. Schuler, p. 110, Th. Königshofen in A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 888

[191] W. Hülsman/K. Schuler *Zur Qualifizierung betrieblicher Datenschutzbeauftragter – Ein Plädoyer für Inhalt statt Form*, DANA 3/2006, p. 108.

[192] W. Hülsman/K. Schuler, p. 109.

[193] By way of application *mutatis mutandis* of article 626 of the *Bürgerliches Gesetzbuch* (BGB) [Civil Code] regulating the case of dismissal without notice for compelling reasons.

[194] For example Germany/Landesarbeitsgericht Niedersachsen [Labour Court of the state Niedersachsen], Judgment of 16 June 2003, case no.: 8 Sa 1968/02, http://www.bfdi.bund.de/cln_007/nn_532046/DE/GesetzeUndRechtsprechung/Rechtsprechung/BDSGDatenschutzAllgemein/Artikel/160603_DatenschutzbeauftragterKeinenEigenstaendigenKuendigungsschutz.html (02.02.09), Germany/Bundesarbeitsgericht [Federal Labour Court]/ Judgement of 13 March 2007, case no.: 9 AZR 612/05, http://datenschutz.eu/urteile/Bundesarbeitsgericht--20070313.html (02.02.09).

termination (‘ordentliche Kündigung’) and that the appointment as data protection officer automatically ceases to be valid upon termination of employment.[195] Thus, data protection officers in private companies have a rather weak position and do not enjoy the same status and protection as, for example, the Works Councils. Therefore, it is often proposed to strengthen their position and to make it actually comparable to Works Councils.[196]

B.2. Data protection officers in public bodies at the level of the *Länder*

[139]. As already mentioned almost all *Länder* have either envisaged[197] or prescribed[198] the appointment of a data protection officer in public *Länder* bodies by law. Concerning public bodies at the level of the *Länder* the legal position of the data protection officer depends on whether the position is already regulated by law or still regulated on the basis of internal administrative provisions.

[140]. Some *Länder* laws (Nordrhein-Westfalen, Berlin und Hessen) also require the appointment of a deputy.[199] Some *Länder* laws also expressly prescribe the obligation to appoint a data protection officer for agencies of a certain size. For example, in Thüringen the basic number of employees is 5, in Rheinland-Pfalz it is at least 10.

[141]. In case the appointment of a data protection officer is expressly regulated by law, the appointment constitutes a legal determination of a special area of responsibility in a functional sense and accordingly, has to be considered an official function (‘Amt’). It is transferred to the administrative data protection officer by way of (partial) transfer (‘Teilversetzung’) or by secondment (‘Abordnung’).[200] Therefore, and

---

[195] See Germany/Landesarbeitsgericht Niedersachsen [Labour Court of the state Niedersachsen], Judgment of 16 June 2003, case no.: 8 Sa 1968/02, http://www.bfdi.bund.de/cln_007/nn_532046/DE/GesetzeUndRechtsprechung/Rechtsprechung/BDSGDatenschutzAllgemein/Artikel/160603__DatenschutzbeauftragterKeinenEigenstaendigenKuendigungsschutz.html (27.01.09), Germany/Arbeitsgericht Dresden/Judgment of 9 February 1994, case no.: 3 Ca 7628/93, RDV 1994, p. 141.

[196] FDP-Bundestagsfraktion Positionspapier Datenschutz im öffentlichen und nichtöffentlichen Bereich, Beschluss der FDP-Bundestagsfraktion vom 14. Oktober 2008, http://www.gisela-piltz.de/files/6076/Positionspapier_Datenschutz_-Fassung_Fraktionsbeschluss__2_.pdf (03.02.09).

[197] Art. 10 DPL Baden-Württemberg, art. 10 DPL Schleswig-Holstein, art. 8 DPL Saarland.

[198] For example art. 19a para 1 DPL Berlin, art. 7a DPL Brandenburg, art. 5 DPL Hessen; art. 8a para 2 DPL Niedersachsen, art. 32a DPL Nordrhein-Westfalen, art. 11 DPL Rheinland-Pfalz, art. 10a DPL Thüringen.

[199] Art. 32a DPL Nordrhein-Westfalen, art. DPL Berlin, art. 5 DPL Hessen.

[200] Art. 6 and 27 *Bundesbeamtengesetz* (BBG) [Federal Civil Service Law]. The Civil Service Laws of the Länder contain corresponding provisions.

because the tasks of this official function are regulated by law, the fulfilment of these tasks must be considered an official duty ('Dienstpflicht') for civil servants and other employees of the public service, the violation of which can trigger the relevant disciplinary sanctions of the civil service law.

[142]. On the other hand, the fiduciary duty ('Fürsorgepflicht') of the (civil service) employer ('Dienstherr') applies in favour of the administrative data protection officer, which implies, amongst others, that the data protection officer must not be exposed to a conflict with other official duties and that he or she has to be appropriately supported. The deployment of data protection officers in the public sphere is however often problematic. Requirements regarding the qualification of data protection officers are also not clearly regulated.

B.3. Evidence regarding compliance in private bodies

[143]. It appears that a significant number of private companies that are by law obliged to appoint data protection officers do not comply with this obligation and that those companies that do comply with the general obligation to appoint data protection officers very often do not facilitate the efficient and effective work of those appointed. Even within bigger companies of medium sized business ('Mittelstand') only 10 to 50 % of the weekly time of work is actually foreseen for the fulfilment of data protection activities. In these cases the engagement of the data protection officers cannot realistically be called a professional activity ('Berufsausübung').[201] Only in bigger companies or in corporations the data protection officers can devote more than 50% of their time to data protection activities.

[144]. Thus, it cannot be ignored that the majority of medium-sized ('mittelständische') companies still display a range of data protection deficits, which is due to the fact that the appointed data protection officers – in case they are appointed at all – cannot initiate the required relevant changes to data protection as a result of lack of time for their own vocational training as well as for the discharge of their responsibilities. In this context the adoption of the law on the data protection audit could improve the situation.

[145]. In any event, the increasing role of internal data protection officers becomes more obvious. Therefore, it is being discussed whether they

[201] W. Hülsman/K. Schuler *Zur Qualifizierung betrieblicher Datenschutzbeauftragter – Ein Plädoyer für Inhalt statt Form,* DANA 3/2006, p. 110

should not only be given additional competencies but also a protection similar to the works councils.[202]

B.4. Evidence regarding compliance in public bodies

[146]. With the entry into force of legislation transposing EC Directive 95/46/EC, the relevant data protection laws included the obligation to appoint data protection officers within administrations. While the implementation of the relevant provisions was initially unsatisfactory in that data protection officers, if appointed, were not given sufficient time to discharge their duties as data protection officers, the situation improved in recent years. In relation to the federal level, the Federal Commissioner for Data Protection criticized the inadequacy of the system in 2005, and the government, in the meantime, expressly accepted that the obligation to support the data protection officers as laid down in article 4 f para 5 FDPL also includes the duty to discharge them from other duties.[203]

C. Compliance or lack of compliance with data protection legislation in practice

[147]. The recent scandals mentioned above involving both private and public institutions highlight extensive and serious cases of data and privacy violations on a large scale.[204] These cases involve, amongst others, severe violations of privacy rights by spying on or secretly observing employees by video, or by computerized profile searches against employees at the work place. Others relate to data trading in unprecedented amounts without the prior approval given by the data

---

[202] Expert opinion of the Federal Commissioner for Data Protection for the hearing on the topic of "modernization of data protection" before the Committee for Interior of Parliament, p. 8, http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung05/Stellungnahmen/Stellungnahme03.pdf (02.02.09).

[203] See the 21st activity report of the Federal Data Protection Officer, p.21, http://www.bfdi.bund.de/cln_007/nn_531940/SharedDocs/Publikationen/Taetigkeitsberichte/21-Taetigkeitsbericht-2005-2006,templateId=raw,property=publicationFile.pdf/21-Taetigkeitsbericht-2005-2006.pdf (02.02.09).

[204] http://www.heise.de/tp/r4/artikel/28/28579/1.html (29.01.09), http://www.dorstenerzeitung.de/nachrichten/politik/blickpunkt/art302,350317 (29.01.09), http://www.tagesschau.de/inland/datenschutz110.html (29.01.09), http://www.sol.de/news/welt/tagesthema/Datenschutz;art7325,2705543 (29.01.09), http://www.ruhrnachrichten.de/nachrichten/politik/blickpunkt/art302,433610 (29.01.09), http://ez.omg.de/?id=20&nid=29923. (29.01.09). http://www.handelsblatt.com/unternehmen/handel-dienstleister/rasterfahndung-bei-der-bahn;2136145 (29.01.09).

subjects.[205] The failure of appropriate criminal prosecution often exacerbates the problem.

[148]. In addition, reference is made to the activity reports of the Commissioners for Data Protection, which highlight cases of non-compliance with data protection legislation. It should however also be noted that in many cases, the work and advice of the Commissioners for Data Protection has resulted in (improved) compliance with data protection legislation. These "success stories" are usually difficult to report as they usually take place on the basis of a respectful relationship developed between the Commissioner and the respective organization and would not be disclosed publicly.

4. Sanctions, Compensation and Legal Consequences

A. Sanctions

[149]. Concerning sanctioning mechanisms available to the Commissioners for Data Protection a certain degree of variance needs to be noted. In most *Länder* jurisdictions and at the Federal level an infringement upon certain data protection provisions may be considered an *Ordnungswidrigkeit* [administrative offence] or a criminal offence depending on the intention of the offender. If the act in question was carried out with the intent to damage someone else or to enrich oneself it is contemplated a crime and can be punished by imprisonment of up to two years.[206] The Data Protection Law of the Land Schleswig-Holstein, however, does not criminalise data protection violations at all, but merely lays down an administrative offence.

[150]. Moreover, differences in the diverse *Länder* Data Protection Laws exist regarding the exact elaboration of the elements of the offences laid down therein.[207] For example, five *Länder* have decided to already make the attempt of the criminal offences against data

[205] See http://www.aufrecht.de/news/view/article/illegaler-handel-mit-adress-und-kontodaten-sprengt-alle-grenzen.html (29.01.09).
[206] Art. 43 para 1 and 2, art. 44 para 1 FDPL; art. 40 para 1, art. 41 DPL Baden-Württemberg; art. 38 para 1, art. 39 DPL Sachsen; pursuant to art. 37 para 1 DPL Rheinland-Pfalz the maximum sentence is only one year.
[207] S. Simitis, *Kommentar zum Bundesdatenschutzgesetz* (5th edition, Baden-Baden 2003), article 44 para 2, notes 17-21.

protection provisions punishable.[208] Also in three *Länder* jurisdictions the punishment under the norms of the respective Data Protection Laws is in general subsidiary to other criminal offences at the *Länder* or federal level.[209]

[151]. In relation to administrative offences, the level of fines imposed for the commission of an administrative offence are usually determined by the severity of the infringement and can range from 25,000 € to 250,000 € in the different jurisdictions.

[152]. According to article 36 para 1 *Ordnungswidrigkeitengesetz* (OWiG) [Law on Administrative Offences][210] the general rule is that the materially competent *Oberste Landesbehörde* [Supreme State Authority] imposes the fine unless an administrative authority has been specifically charged with the task by law. Thus regarding the supervision of the private sector only the competent *Länder* Commissioners for Data Protection and the otherwise appointed non-public supervision authorities can impose fines in the first place, whilst in the public sector the Commissioners for Data Protection are responsible for the imposition of fines according to the delineation of their supervisory competences depending on whether the violated law is a Federal or a *Länder* law.[211]

[153]. In the *Länder* Baden-Württemberg, Nordrhein-Westfalen and Sachsen a special allocation in the sense of article 36 para 1 no. 1 of the Law on Administrative Offences has occurred, with the first two assigning the imposition of fines to regional administrative bodies, whereas the *Land* Sachsen explicitly mandated its Commissioner for Data Protection.[212] In three more *Länder* jurisdictions the legal situation is equally clear because the Commissioners for Data Protection are unequivocally referred to as supreme *Landesbehörde* in the respective *Länder* Data Protection Laws,[213] so that their competency derives from the wording of article 36 para 1 no. 2a of the Law on Administrative Offences. In four *Länder*, namely Berlin, Mecklenburg-Vorpommern, Rheinland-Pfalz and Thüringen the *Länder* Data Protection Laws do not prescribe an administrative offence at all but exclusively impose penal provisions. Yet in the

---

[208] Art. 41 DPL Baden-Württemberg, art. 32 para 2 DPL Hamburg, art. 28 para 1 DPL Niedersachsen, art. 33 para 1 DPL Nordrhein-Westfalen, art. 37 para 2 DPL Rheinland-Pfalz.
[209] Art. 32 para 4 DPL Hamburg, art. 40 para 2 DPL Hessen, art. 35 para 2 DPL Saarland.
[210] http://www.gesetze-im-internet.de/bundesrecht/owig_1968/gesamt.pdf (16.12.08).
[211] S. Simitis *Kommentar zum Bundesdatenschutzgesetz* (5th edition, Baden Baden 2003), article 43 III, paras 86-90.
[212] Art. 40 para 1 DPL Baden-Württemberg, art. 34 para 1 DPL Nordrhein-Westfalen, art. 38 para 1 DPL Sachsen.
[213] Art. 22 para 1 1st sentence DPL Berlin, art. 22 DPL Hessen, art. 23 para 3 DPL Rheinland-Pfalz.

remaining six *Länder* and also with a view to the Federal Commissioner for Data Protection a legal clarification is lacking with the consequence that the gap in the delimitation of the competence to impose the fines has to be closed by analogy.

B. Compensation payments

[154]. As concerns the compensation regimes in place in Germany, all *Länder* data protection laws as well as the federal data protection law stipulate that compensation needs to be paid to persons affected by data protection violations. These violations are commonly prescribed as the impermissible or incorrect collection, the processing or use of personal data.[214] Thus compensation will be awarded at either the federal or the *Länder* level depending on the violated norms and whether the offender was a private party or a state agency. For this reason some *Länder* data protection laws also contain explicit subsidiarity clauses in order to clarify the hierarchy of the norms involved.[215]

[155]. At the federal level article 7 FDPL refers only to violations committed by non-public controllers whose obligation to pay does not arise if they have exercised due care in accordance with the circumstances of the case concerned. This leads to an inversed burden of proof, since the affected person does not have to prove fault but rather the violator will have to prove the absence of fault. In that regard it is also recommended to regulate a strict liability ('Gefährdungshaftung') also for non-public bodies.[216]

[156]. Article 8 FDPL on the other hand applies to public bodies causing harm through the impermissible or incorrect automated collection, processing or use of personal data. They are responsible for any kind of violation irrespective of any fault. Para 2 of article 8 further prescribes that in case of a grave violation of privacy the affected person is entitled to receive adequate pecuniary compensation for the immaterial harm caused, too. This has to be seen in the context of

---

[214] See http://www.bfdi.bund.de/cln_027/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf (20.01.2009).

[215] Art. 18 para 2 DPL Berlin, art. 20 para 3 DPL Hamburg, art. 20 para 3 DPL Hessen, art. 20 p ara 4 DPL Nordrhein-Westfalen, art. 24 para 4 DPL Saarland, art 23 para 6 DPL Sachsen, art. 18 para 4 DPL Thüringen.

[216] See A. Roßnagel/A. Pfitzmann/H. Garstka, *Modernisierung des Datenschutzrechts* [Modernisation of Data Protection Law], Gutachten im Auftrag des Bundesministeriums des Innern [Expert Opinion provided at the Request of the Federal Ministry of the Interior], 2001, p. 19, http://www.computerundrecht.de/media/gutachten.pdf (01.02.09)

article 253 para 1 of the *Bürgerliches Gesetzbuch* (BGB) [Civil Code] which requires a specific norm to provide for pecuniary compensation in case of immaterial harm. Yet violations of the right to informational self-determination have long been recognised as the basis for such claims in a standing jurisprudence which relied on an interpretation in conformity with the constitutional requirements imposed by the rulings of the Constitutional Court. Para 3 of article 8 FDPL limits the claims that can be made to a total amount of 130.000 €. Most *Länder* have also chosen to make the referral to article 253 para 1 Civil Code in cases of immaterial harm explicit and have included a similar clause in the provisions of their respective data protection laws. Also some have limited the level of claims to a certain sum ranging between 125,000 € and 250,000 €.[217] At the *Länder* level differences arise concerning the required standard of proof. In nine *Länder* laws the burden of proof was shifted, requiring the violator to proof the absence of fault.[218] The remaining seven *Länder* laws require no fault at all.[219]

[157]. Case law on compensation payments based on the relevant compensation provisions of data protection does not appear to be extensive, however, some leading cases exist.[220] Compensation is also granted on the basis of the general compensation provision of article 823 para 1 of the Civil Code, which continues to apply for claims for compensation of immaterial damage against non-public bodies for violations of personal rights.[221]

---

[217] Art. 14 para 2 3rd sentence DPL Bayern, art. 20 para 1 3rd sentence DPL Hessen, art. 27 para 3 DPL Mecklenburg- Vorpommern, art. 18 para 1 2nd sentence DPL Niedersachsen.

[218] Art. 25 para 1 DPL Baden-Württemberg, art. 14 para 2 3rd sentence DPL Bayern, art. 20 para 1 3rd sentence DPL Brandenburg, art. 23 para 1 DPL Bremen, art. 20 para 1 1st sentence DPL Hessen, art. 18 para 1 1st sentence DPL Niedersachsen, art. 24 para 4 DPL Saarland, art. 18 para 1 DPL Thüringen.

[219] Art. 18 para 1 DPL Berlin, art. 20 para 1 1st sentence DPL Hamburg, art. 27 para 1 DPL Mecklenburg- Vorpommern, art. 20 para 1 DPL Nordrhein-Westfalen, art. 21 para 1 DPL Rheinland-Pfalz, art. 23 para 1 DPL Sachsen, art. 30 para 1 DPL Schleswig-Holstein.

[220] See Germany/Oberlandesgericht [Regional Court] Düsseldorf/Decision of 14 December 2006, case no.: I-10 U 69/06, DUD 2007, pp. 58-60, http://medien-internet-und-recht.de/volltext.php?mir_dok_id=503, http://www.kostenlose-urteile.de/newsview3521.htm. Proceedings involving compensation claims also often end with a settlement. See, for example, Germany/Amtsgericht [Municipal Court] Kassel, case no.: 424 G 1260/98. http://www.test.de/themen/steuern-recht/meldung/-Schmerzensgeld/18488/18488/.

[221] S. Simitis *Kommentar zum Bundesdatenschutzgesetz* 5th edition, Baden-Baden 2003, p. 631, Germany/Bundesgerichtshof [Federal Court of Justice]/Judgment of 22 May 1984, case no.: VI ZR 105/82, BGHZ 91, 233 (238), Germany/Bundesgerichtshof [Federal Court of Justice]/Judgment of 19 May 1981, case no.: VI ZR 273/79, BGHZ 80, 311 (318s.).

C. Follow up activities by the data protection authorities

[158]. Follow up activities are often carried out by data protection authorities or other bodies as described above. The Commissioners for Data Protection often make use of the possibilities provided by law, for example, requesting criminal proceedings or applying (administrative) fines, however given their budgetary and other restrictions, their capacity in this context remains limited (see above). Also, very often the problem at hands is solved by way of active involvement of the Commissioner for Data Protection, short of launching administrative or criminal proceedings. In that context the advisory activities of the Commissioners for Data Protection play a very important role. Another aspect sometimes mentioned is that the individuals concerned are not always interested in proceeding legal actions against the person or body violating their data protection rights.

D. Personal initiative of data subjects and assistance

[159]. Enforcement of legislation largely depends on the personal initiative of data subjects, which is often highlighted as one of the main problems in the context of efficient data protection. Legal advice can, by and large, only be provided by admitted attorneys and support during legal proceedings, if they are commenced at all, is regulated in accordance with the general principles of legal aid. The Commissioners for Data Protection are not sufficiently staffed to engage in all cases that would be appropriate to be supported and secondly (and maybe more importantly), they cannot substitute themselves for admitted attorneys as the right to provide legal advice is basically limited in accordance with the *Rechtsberatungsgesetz* [Law on Legal Advice].

E. Data protection in the context of employment

[160]. Special legislation regulating data protection in the sphere of private employment does not exist. The Federal Commissioner for Data Protection together with other Commissioners in the context of the Data Protection Conference, amongst others, have repeatedly requested the adoption of relevant legislation ('Arbeitnehmer-Datenschutzgesetz'), especially in the light of a number of recent data protection scandals in the employment sphere, involving the spying, video surveillance etc. of employees. The applicable standards were mainly developed through case law of the competent labour courts dealing with disputes arising of data protection violations in the

context of employment limiting the rights of employers to process data.[222]

[161]. Employees can exercise their specific data protection rights resulting, for example from the employment contract and/or relevant legislation, such as article 83 of the *Betriebsverfassungsgesetz* (BetrVG) [Law on the Works Constitution] through the Works Councils.[223]

5. Rights Awareness

[162]. Clearly relevant studies or surveys on awareness regarding data protection law and rights in the population do not seem to exist. There are, however, a couple of research projects carried out at the initiate of private companies dealing with the question, amongst others, as to how much privacy and self-determination individuals are willing to compromise or even sacrifice in (business) situations that seem to offer financial or other gains.[224] Some project aim at raising awareness of people about data protection issues.[225]

6. Analysis of deficiencies

A. Main deficiencies from a fundamental rights perspective

[163]. Data protection is considered as protection of fundamental rights and at the same time as one of the core conditions for the functioning of a democratic society. Already the Constitutional Court, in the Census Judgment, stressed that the right to informational self-determination is an essential condition for the functioning of a democratic society based on the rule of law.[226] It is the fundament of the personal

---

[222] For example regulating the admissibility of video cameras at the work place, Germany/Landesarbeitsgericht [Regional Labour Court] Köln/Decision of 28 December 2005, case no.: 9 Ta 361/05, http://www.verdi-bub.de/urteil/61/ (02.02.09), Germany/Bundesarbeitsgericht [Federal Labour Court]/Decision of 29 June 2004, case no.: 1 ABR 21/03, http://www.verdi-bub.de/urteil/38/ (02.02.09).

[223] A. Büllesbach in A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 970

[224] http://www.imittelstand.de/themen/topthema_100230.html

[225] See above, project initiated by the Federal Commissioner for Data Protection on the Charter for Digital Data Protection and Freedom of Information, http://www.bfdi.bund.de/cln_007/nn_533554/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM_32_08_ChartaDigitalerDatenschutz.html (30.01.09), or the 'Data Party' organized by the Commissioner for Data Protection of Saarland, http://www.datenparty.de (30.01.09) and the website www.datenschutz.de run by the Independent Centre for Data Protection Schleswig Holstein.

[226] See above, Chapter 1 para 2; A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 2.

development and protects the individual freedom. As a fundament for the exercise of personal freedom it is also the basis of other fundamental rights. Data protection, however, does not cover the right to property and the ownership of persons of "their" data. The individual does not have a right in the sense of an absolute, unlimited sovereignty over 'his or her' data, the individual is rather a person who, being dependent on communication, develops his personality within a society. Information, also if it is personal, is a reflection of social reality which cannot be only ascribed to the individual.[227]

[164]. Against this, it a multi-dimensional concept is required which has its "centre of gravitation" within the informational self-determination and the guiding principle of which is not the secrecy of data, but the protection of self-determination within a data traffic system.[228]

[165]. The deficiencies mentioned above, therefore, do not always have a direct impact on fundamental rights, but rather hamper the full enjoyment of fundamental rights in a given context. For example, the violation of data protection principles committed in the context of data trading involving considerable financial gains on the side of the traders or violations of privacy rights do not necessarily amount to a violation of the right to property of the data subject, but the right of the individual to decide on the processing and use of his data.[229]

[166]. In many cases, data protection violations constitute severe violations of personal rights of individuals, for example, in the case of secret (video) surveillance of workers at their work place. The right to personal self-determination is frequently violated if data subjects are not or only insufficiently informed about the use and/or processing of their data.

[167]. The complexity of the data protection legislation body as well as the deficiencies in the supervisory and enforcement system also raise concerns in the context of the right to an effective remedy given that it is often difficult if not impossible for the individuals to effectively pursue their claims.

---

[227] Germany/Bundesverfassungsgericht/Judgement of 15 December 1985, BVerfGE 65, 1 (pp. 43-44).

[228] H.-H. Trute in: A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 161.

[229] See for example, Germany/Amtsgericht Kassel [Municipal Court Kassel]/Decision of 2 April 2007, case no.: 413 C 1751/07, http://www.datenschutz.eu/urteile/Amtsgericht-Kassel-20070402.html (29.01.09).

B. Areas not covered by data protection law

[168]. As mentioned above, a couple of areas are currently not covered by legislation, for example the area of data protection in employment. While it would be preferable to regulate this area by law, it would not be appropriate to argue that there are no standards developed at all, since a rather extensive body of case law on data protection in the employment world exists.[230] However, case law is incomplete and therefore, the relevant practice is inconsistent.[231]

[169]. The general concern also is that data protection legislation is too fragmented and at the same time usually lagging behind new technological developments.[232]

C. Possible improvements of deficiencies

[170]. The deficiencies described above could be filled or at least be reduced in many ways. These could include both legal and practical means. In general, the whole body of data protection legislation has to be simplified, while at the same time some currently under-regulated areas should become subject of legislation.

[171]. A stricter application of the relevant criminal legislation would also help to rectify a number of problems. In that context, training of the relevant officials within all spheres of government as well as within the private sphere in data protection issues should have a positive impact on the situation.

[172]. At the same time, awareness raising becomes more important as people need to be sensitized first about the need for and the way in which they can protect themselves from data protection or privacy violations. Moreover, people need to be better informed about the rights and remedies they can exercise in case a data protection

---

[230] For example on the dismissal for using of the internet for private purposes at the work place Germany/Bundesarbeitsgericht/Judgment of 31 May 2007, case no.: 2 AZR 200/06, DuD 2007, 777; on personal data included in the personnel file and access thereto, Germany/Bundesarbeitsgericht/Judgment of 12 September 2006, case no.: 9 AZR 271/06, DuD 2007, 538; on the use of email for campaigning purposes by the trade union, Germany/Arbeitsgericht Frankfurt a.M./Judgment of 12 April 2007, case no. 11 Ga 60/07, RDV 2007, 215; on the secret filming of staff, Germany/Landesarbeitsgericht Köln/Decision of 28 December 2005, case no.: 9 Ta 361/05, RDV 2006, 171, see http://www.datenschutz.eu/urteile (03.02.09).

[231] http://www.bfdi.bund.de/cln_007/nn_530440/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/Arbeitnehmerdatenschutzgesetz.html (03.02.09), http://www.datenschutz.de/news/detail/?nid=3313 (04.02.09).

[232] See above, Chapter 1 para 3.

violation has taken place. Some of the Commissioners for Data Protection have already actively become involved in relevant activities. It is a common position that the area of data protection law is far too complicated for a layperson to understand his or her rights. The capacity to provide advice by the Commissioners for Data Protection is currently limited, also since they are by law not officially entitled to provide "legal advice" on the basis of the *Rechtsberatungsgesetz* [Law on Legal Advice] and to represent individuals and thus the individuals have to pursue their claims through the regular, often very complicated and lengthy proceedings.

[173]. While the inclusion of a data protection provision in the (federal) Constitution might send a strong signal regarding the importance of the respective rights involved, its real impact should not be overestimated.[233]

[174]. Almost all Commissioners for Data Protection highlight the need to increase their financial and staffing resources, especially in the light of the additional responsibilities in the area of freedom of information and the Commissioners for Data Protection of the *Länder* especially in so far as they are responsible for the control of the non-public sector.

[175]. Legal amendments should go hand in hand with the strengthening of the supervisory authorities, otherwise even severe violations of data protection regulations might remain without redress. In addition, the right to take legal action ('Klagerechte') of associations ('Verbraucherverbände') has to be extended to also include data protection issues. It should not be left to individuals to make sure that data protection rights are not constantly violated.[234] Tools should be developed which would enable individuals to independently control the fate of their data, that is, to control their data trace.[235]

---

[233] See S. Simitis *Kommentar zum Bundesdatenschutzgesetz* 5th edition, Baden-Baden 2003, p. 113.

[234] See Federal Commissioner for Data Protection, press statement given at the occasion of the presentation of draft amendments to the Federal Data Protection Law, 10 December 2008, http://www.bfdi.bund.de/cln_007/nn_531002/sid_41D4163A1A85BAA275285EB8D9936E54/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM__35__08__BMIGesetzesentwurf.html (28.01.09).

[235] See *Datenschutz im Informationszeitalter* [Data Protection in the Information Era], Blickpunkt Bundestag Spezial, October 2008, p. 5, http://www.bundestag.de/blickpunkt/pdf/BB_0804_spezial.pdf.

7. Good Practice

A. Jurisprudence of the Federal Constitutional Court

[176]. The continuous development of the right to informational self-determination by the Constitutional Court in the last decades has had a significant impact on the codification of data protection legislation as well as on the relevant data protection practice. The Constitutional Court, as described above in Chapter 1, has consistently elaborated upon the untouchable and inviolable sphere of private life and has clearly delineated the admissibility of data protection activities.

B. Practice of the *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (ULD) [Independent Centre for Data Protection Schleswig Holstein]

[177]. Despite the fact that the Commissioner for Data Protection in the Land Schleswig-Holstein on the basis of the legislative framework does not enjoy full independence[236], the innovative and progressive work of the *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (ULD) [Independent Centre for Data Protection Schleswig Holstein][237] should be noted. This includes the functioning implementation and practice of a data protection audit as well as a data protection seal of quality ('Datenschutzgütesiegel) for a couple of years, the adoption of which has been under discussion for years at the federal level.[238] With the support of almost all German-speaking Data Protection Authorities, the Centre is running a website containing extensive information on latest developments, court cases, reports and press releases and a database on key concepts.[239]

[178]. The Independent Centre for Data Protection also runs extensive training programs in the form of a data protection academy established in the early 1990ies. The Academy has developed comprehensive and systematic training programs for all areas of administration. These are applied throughout the state Schleswig-

---

[236] being subject to the administrative supervision by the Prime Minister, art. 35 para 5 1st sentence DPL Schleswig Holstein.
[237] https://www.datenschutzzentrum.de/ (03.02.09).
[238] https://www.datenschutzzentrum.de/audit/index.htm, https://www.datenschutzzentrum.de/guetesiegel/index.htm (29.01.09).
[239] http://www.datenschutz.de

Holstein, and have already started to have an impact on data protection training beyond the *Land* in other parts of the country.[240]

C. Information on self-protection

[179]. The Commissioner for Data Protection of Saarland has set up a comprehensive homepage with information on how to protect oneself against data protection violations, especially aiming at teachers and other persons in so called 'multiplier functions'.[241]

D. Appointment of data protection officers

[180]. The Article 29 Working Group, in its Working Paper 106, highlighted as good example the German practice of appointment of data protection officers both within private and public institutions as an exception to the notification duty under article 18 para 2 of the EC Directive 95/46/EC.[242]

8. Miscellaneous

[181]. Nothing to report.

---

[240] See R-B. Abel in: A. Roßnagel, *Handbuch Datenschutzrecht*, München 2003, p. 207, https://www.datenschutzzentrum.de/akademie/index.htm (29.01.09).

[241] http://www.datenparty.de/ (30.01.09).

[242] Report on the Obligation to Notify the National Supervisory Authorities, the Best Use of Exceptions and Simplification and the Role of the data protection officers in the European Union 10211/05/EN, Working Paper No. 106 of the Article 29 Working Party, adopted on 18 January 2005, pp. 15-18, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf (29.01.09), https://www.gdd.de/nachrichten/news/berufsbild-datenschutzbeauftragter-eine-deutsche-201esuccess-story201c-mit-vorbildwirkung (29.01.09).

Annexes

Annex 1 - Tables and Statistics

As elaborated on above, due to the federal structure of the German state 17 Data Commissioners (one federal and one for each *Bundesland*) exist in the public sector. In an additional seven *Länder* special authorities have been separately assigned with the supervision of the private sector. These supervisory authorities have published their respective activities in their numerous annual or biannual reports, with a considerably varying degree of statistical information included. Thus the following tables and statistics cannot attempt to draw a conclusive and complete picture but rather represent the information as it was readily available. Therefore the fragmentary nature of the statistics and inconsistencies therein need to be excused with a view to the multitude and diversity of the supervisory authorities in existence and the widely differing degree of availability of statistical information in the reports on their activities.

Bundesdatenschutzbeauftragter (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									4,511 Million €
Staff of data protection authority									69
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Baden-Württemberg (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									
Staff of data protection authority									15
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Baden-Württemberg [Innenministerium] (only private sector)**:**	2000	2001	2002	2003	2004	2005 & 2006	2007
Budget of data protection authority							
Staff of data protection authority							
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative:							
Number of data protection registrations						87	
Number of data protection approval procedures							
Number of complaints received by data protection authority: General requests:						850 420	
Number of complaints upheld by data protection authority							

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.) [Bußgeldbescheide]						10	
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)							
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)							

Landesdatenschutzbeauftragter Bayern (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									1,597,300 €
Staff of data protection authority									24
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Bayern [Regierung Mittelfranken] (only private sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority								
Staff of data protection authority								
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative: [Kontrollen]					18	21		
Number of data protection registrations						115		
Number of data protection approval procedures								
Number of complaints received by data protection authority: General requests:					564 418	514 496		
Number of complaints upheld by data protection authority					198	251		
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow						12	3	

up activity: settlement, warning issued, opinion issued, sanction issued etc.) [Bußgeldbescheide]								
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)								
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)								

Landesdatenschutzbeauftragter Berlin (public and private sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									2,4 Million €
Staff of data protection authority									31
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative:									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority: Individual complaints concerning the public sector: Individual complaints concerning the private sector: General requests:				924 268 296 360	1064 299 284 481	1137 321 350 466	1432 392 525 515	1427 400 413 614	

Number of complaints upheld by data protection authority									
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Brandenburg (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									1,077,700 €
Staff of data protection authority									16
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Brandenburg [Innenministerium] (only private sector)**:**	2000	2001	2002	2003	2004 & 2005	2006 & 2007
Budget of data protection authority						
Staff of data protection authority						
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative:						
Number of data protection registrations						9
Number of data protection approval procedures						
Number of complaints received by data protection authority: General requests:					173 74	266 28
Number of complaints upheld by data protection authority						

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)						
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)						
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)						

Landesdatenschutzbeauftragter Bremen (public and private sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									
Staff of data protection authority									12
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Hamburg (public and private sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									
Staff of data protection authority									20
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative:									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority:			562	542	569	647	643	690	
Number of complaints upheld by data protection authority									
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									

Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Hessen (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									
Staff of data protection authority									15
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Hessen [Regierungspräsidium] (only private sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority								
Staff of data protection authority								
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative:								
Number of data protection registrations								
Number of data protection approval procedures								
Number of complaints received by data protection authority: General requests:							603 294	658 289
Number of complaints upheld by data protection authority								108
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow								

up activity: settlement, warning issued, opinion issued, sanction issued etc.)								
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)								
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)								

Landesdatenschutzbeauftragter Mecklenburg-Vorpommern (public and private sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									
Staff of data protection authority									22
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Niedersachsen (public and private sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									
Staff of data protection authority									20
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Nordrhein-Westfalen (public and private sector)**:**	2001	2002	2003	2004	2005	2006	2007	2008	2009
Budget of data protection authority								3,238,900 €	2,989,700 €
Staff of data protection authority								48	45
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Rheinland-Pfalz (public and private sector):	2001	2002	2003	2004	2005	2006	2007	2008	2009
Budget of data protection authority									1,159,700 €
Staff of data protection authority									13 2/3 (11 full and 4 part time)
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Saarland (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority								681,100 €	640,700 €
Staff of data protection authority								12	12
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Saarland [Innenministerium] (only private sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority								
Staff of data protection authority								
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative								
Number of data protection registrations								
Number of data protection approval procedures								
Number of complaints received by data protection authority								
Number of complaints upheld by data protection authority								

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)								
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)								
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)								

Landesdatenschutzbeauftragter Sachsen (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008 and 2009
Budget of data protection authority									1,27 Million €
Staff of data protection authority									23
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Sachsen [Innenministerium] (only private sector)**:**	2000	2001 & 2002	2003 & 2004	2005 & 2006	2007
Budget of data protection authority					
Staff of data protection authority					
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative:					
Number of data protection registrations					
Number of data protection approval procedures					
Number of complaints received by data protection authority:		116	147	164	
Number of complaints upheld by data protection authority		50	65	62	
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity:					

settlement, warning issued, opinion issued, sanction issued etc.)					
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)					
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)					

Landesdatenschutzbeauftragter Sachsen-Anhalt (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									
Staff of data protection authority									15
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Sachsen-Anhalt [Landesverwaltungsamt] (private sector)**:**	2000	2001	2002	2003	2004	01.06.2005 – 31.05.2007
Budget of data protection authority						
Staff of data protection authority						
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative:						
Number of data protection registrations						
Number of data protection approval procedures						
Number of complaints received by data protection authority: General requests:						94 57
Number of complaints upheld by data protection authority						

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)						
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)						
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)						

Landesdatenschutzbeauftragter Schleswig Holstein (public and private sector):	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority									1,8 Million €
Staff of data protection authority									25 permanent + 14 project related
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Landesdatenschutzbeauftragter Thüringen (only public sector)**:**	2000	2001	2002	2003	2004	2005	2006	2007	2008 and 2009
Budget of data protection authority									1,781,600 €
Staff of data protection authority									14
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative									
Number of data protection registrations									
Number of data protection approval procedures									
Number of complaints received by data protection authority									
Number of complaints upheld by data protection authority									

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)									
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)									

Thüringen [Landesverwaltungsamt] (only private sector)**:**	2000	2001	2002	2003 & 2004	2005 & 2006	2006	2007
Budget of data protection authority							
Staff of data protection authority							
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative:							
Number of data protection registrations							
Number of data protection approval procedures							
Number of complaints received by data protection authority: General requests:				67 77	99 63		
Number of complaints upheld by data protection authority					58		

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.) [Bußgeldbescheide]					2		
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)							
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)							

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2 – Case Law

Case title	*Mikrozensusgesetz* [Law on the Micro Census]
Decision date	16 July 1969
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Bundesverfassungsgericht (BVerfG) [Federal Constitutional Court], case no.: 1 BvL 19/63
Key facts of the case (max. 500 chars)	The case at hand was about the relevant norms of the *Mikrozensusgesetz* [Law on the Micro Census], a law which called for the compilation of a representative official statistic on the population of Germany and professional life in Germany. Select groups of persons were to be questioned on their vacation habits by the administration and one of the people concerned, when refusing to comply, was charged with procedures to pay an administrative fee. The competent court considered the pertinent provisions of the law to be incompatible with the Constitution and thus referred the point of law to the Federal Constitutional Court.
Main reasoning/argumentation (max. 500 chars)	In the case at hand the Constitutional Court did not consider that the inviolable sphere of private life as guaranteed for by the combination of article 2 para 1 and 1 para 1 of the German Constitution was indeed infringed upon. Rather the Court held that the pertinent provisions were in accordance with the Constitution, since they ensured sufficient anonymisation and were proportional.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	In this case the Constitutional Court laid down the basic foundations in the area of data protection. According to the decision the right to personal freedom enshrined in article 2 para 1of the German Constitution read in conjunction with the right to human dignity enshrined in article 1 para 1 of the Constitution protect an inviolable sphere of private life which must not be subjected to infringements by the public authorities. The Constitutional Court also generally held that it is incompatible with the right to human dignity, if the state forcibly registers and catalogues the human being. Even if the collection of the statistics is carried out anonymously the State has to take adequate precautions to ensure the constitutional rights relates to the privacy of information.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Even though the Constitutional Court did not find a violation of the Constitution in the concrete case at hand, the decision was nevertheless very important as it was a precursor of and laid the groundwork for the future development by the Constitutional Court's jurisprudence of data protection and the constitutional foundation of individual rights in this respect.
Proposal of key words for data base	Statistical Data collection, inviolable sphere of privacy

Case title	*Volkszählungsurteil* [Judgment on the Census]
Decision date	15 December 1983
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Bundesverfassungsgericht (BVerfG) [Federal Constitutional Court], case no.: 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83
Key facts of the case (max. 500 chars)	According to the *Volkszählungsgesetz* (VolkszählungsG) [Law on Census] of 1983 all inhabitants of the Federal Republic of Germany were to be statistically registered. The law contained detailed provision on the questionnaire which was to be conducted and on what was to happen with the collected information. Several concerned citizens filed a constitutional complaint against this and questioned the constitutionality of the law.
Main reasoning/argumentation (max. 500 chars)	The Constitutional Court, in response to the dangers associated with modern information technology, now explicitly developed the fundamental right to informational self-determination out of the general right to personal freedom as embodied in article 2 para 1 combined with the right to human dignity of article 1 para 1 of the German Constitution. The Court held, that the parts of the provision which dealt with the use of the obtained information were not in accordance with the Constitution, since the conditions upon which data could be passed on to other state bodies did not comply with the requirements of procedural restraints necessary.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	In this case the Federal Constitutional Court postulated the specific fundamental right to informational self-determination based on the right to freedom of personal development in article 2 para 1 and the right to human dignity of article 1 para 1 of the German Constitution. This newly created fundamental right gives citizens the right to principally determine themselves, which personal data on them can be collected, stored, and passed on.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The right to informational self-determination was proclaimed to be an essential condition for the functioning of a democratic society based on the rule of law. Despite some initial reluctance the right to informational self-determination as developed by the Constitutional Court is now unanimously accepted and the decision at hand is often referred to as a milestone for the German data protection framework. Also, the Constitutional Court made it clear, that under the prevailing conditions of modern data processing no singe piece of information is in itself inconsequential.
Proposal of key words for data base	General right to personal freedom, informational self-determination

Case title	*Urteil zur Rasterfahndung* [Judgment on Computerised Profile Searches]
Decision date	4 April 2006
Reference details	Bundesverfassungsgericht (BVerfG) [Federal Constitutional Court], case no.: 1 BvR 518/02
Key facts of the case (max. 500 chars)	This case was about the so called computerised profile searches ('Rasterfahndung'), which are computer-aided searches for wanted persons whereby the data of a large number of persons are checked against existing data in a database with modern means of data processing. This practice was instituted after the September 11th terrorist attacks of 2001 in order to counter the perceived threat to national security by fundamentalist terrorism by detecting so called "sleepers" at an early stage in their preparation. The criteria used to determine potential terrorists were widespread, of a quite common nature and especially targeted a certain group of people (male, age 18 to 40, student or former student, Islamic confession, etc.). The applicant of the constitutional complaint fell himself within this target group and requested review of judicial decisions in all instances upholding the ruling to initiate the computerised profile search.
Main reasoning/argumentation (max. 500 chars)	The Constitutional Court held that such a computerised profile search, if carried out with preventive purpose is only compatible with the right to informational self determination as enshrined in article 2 para 1 and article 1 para 1 of the German Constitution in case a concrete danger for highly important objects of legal protection ('Rechtsgüter'), such as the existence and safety of the state or for personal integrity, life, or freedom of a person exists. A computerised profile search cannot be justified in the phase preceding the actual prevention of danger ('Gefahrenabwehr'). Thus in the case at hand the Court found a violation of the applicants right to informational self determination based on the incorrect balancing of legal interests in contradiction with the constitutional value system.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Constitutional Court confirmed its position and further elaborated upon the balancing of the right to informational self determination with national security interests, arguing that it is not in itself unproportional to impair this right in the face of danger to other high ranking constitutional goods but that the state has to act in accordance with the rule of law and tie such infringements to sufficiently concrete dangers. This is due to the reality that computerised profile searches infringe upon constitutional rights of a large number of non violators without any grounds of suspicion against them. Therefore, computerised profile searches may be ordered only in circumstances of a concrete and ample likelihood that in the foreseeable future damage to legally protected interests of paramount importance will occur.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	A generally dangerous situation, as existed with regard to terrorist attacks after September 11th of 2001, is in itself insufficient to justify the use of means such as computerised profile searches, which infringe upon the right to informational self determination of a large number of innocent citizens. Rather additional facts have to be on hand which lead to the conclusion that there is indeed a concretely dangerous situation, e.g. concerning the preparation of a concrete terrorist attack.
Proposal of key words for data base	Right to informational self determination, prevention of danger, national security

Case title	*Urteil zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* [Judgment on the confidentiality and integrity of systems of information technology]
Decision date	27 February 2008
Reference details (type and title of court/body; in original language and English [official translation, if available])	Bundesverfassungsgericht (BVerfG) [Federal Constitutional Court] , case no.: 1 BvR 370/07; 1 BvR 595/07
Key facts of the case (max. 500 chars)	The applicants filing the constitutional complaints were a journalist, a member of the regional division of the left party "Die Linke" and three lawyers. They alleged that Article 5 (2) no 11 of the *Verfassungsschutzgesetz* [Law on the Protection of the Constitution] of the Land Nordrhein-Westfalen was unconstitutional with regard to the right to the confidentiality and integrity of systems of information technology deriving from the general right to personal freedom under Art. 2 (1) combined with Art. 1 (1) of the Constitution. The relevant norm entitled the *Landesverfassungschutz* [Office for the Protection of the Constitution] of the Land Nordrhein-Westfalen to secretly search systems of technical information e.g. computer hard disks via remote online access and to monitor and activities in the internet.
Main reasoning/argumentation (max. 500 chars)	The pertinent provision does interfere with the the right to the confidentiality and integrity of systems of information technology deriving from the general right to personal freedom under Art. 2 (1) combined with Art. 1 (1) of the Constitution. In particular the norm of the *Verfassungsschutzgesetz* is not in line with the principle of proportionality. Considering the intensity of the intrusion into the private sphere of the concerned individuals, only concrete danger to a predominant public good could justify such an intrusion, if ordered by a judge. Moreover the norm does not contain sufficient precautions and safeguards to avoid or limit intrusion in the absolute core of the private conduct of life. Additionally, the monitoring and reconnoitring of online activities in certain constellations infringes upon the right to the secrecy of telecommunication as protected by Art. 10 (1) of the Constitution.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Constitutional Court decided on the question of the constitutionality of "online searches" and declared the relevant provisions of the *Verfassungsschutzgesetz* [Law on the Protection of the Constitution] of the Land Nordrhein-Westfalen, allowing online searches, to be unconstitutional. Article 5 (2) no 11 of the relevant law, regulating the secret access to systems of technical information, violates the right to personal freedom, as the infringement is held to be disproportionate. The secret infiltration of information systems is only acceptable in case a legally protected interest of paramount importance is concretely jeopardized. In addition, the infringement has to be approved of by a judge.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The constitutional complaints by the plaintiffs are successful and the pertinent provision is declared null and void.
Proposal of key words for data base	General right to personal freedom, intelligence gathering, confidentiality of personal information.

Case title	*Vorratsdatenspeicherung* [Retention of Data]
Decision date	11 March 2008
Reference details (type and title of court/body; in original language and English [official translation, if available])	Bundesverfassungsgericht (BVerfG) [Federal Constitutional Court], case no.: 1 BvR 256/08
Key facts of the case (max. 500 chars)	The eight applicants filed a constitutional complaint and asked for an interim order to halt the effects of the "*Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*", which amended the *Telekommunikationsgesetzes* (TKG) [Law on Telecommunication] by two new provisions providing for the retention and use of telecommunication data. The new article 113a TKG requires providers of telecommunication services to retain data such as the location and details of the use of landlines, cell phones, email and internet for a period of six months. article 113b TKG in turn regulates the use of the retained data for the purpose of prosecution of crime, the repelling of dangers to public security and the fulfilment of the tasks of the intelligence agencies. Yet, the norm does not contain an entitlement of its own to request the data but instead relies on other provisions which do so and refer to it, as has so far only happened in article 100g of the *Strafprozessordnung* (StPO) [Code of Criminal Procedural Law].
Main reasoning/argumentation (max. 500 chars)	Since the Court did not deem the constitutional complaint to be *prima facie* inadmissible or unsubstantiated it exclusively had to evaluate the effects of not issuing an interim order and later deciding in favour of the applicants, compared to the situation if issuing an interim order now and later deciding that the constitutional complaint is unsuccessful, without entering into the merits of the case. Concerning the use of the retained data the Court saw serious negative impacts, if the information thus collected was to be used in a widespread manner and in its impact assessment came to the conclusion that the public interest in the execution of the norm had to stand back, considering its potential results for concerned individuals. The Constitutional Court therefore in its interim order modified and restricted the necessary conditions for the use of the retained data. The Court held that the transmission of the retained data is permissible only under the aggravating circumstances according to article 100a StPO, in the concrete case of a major crime, based on reasonable suspicion and if the investigation of the facts would otherwise be considerably more difficult or even impossible. However, the Court did not issue an order halting the retention of data itself because no immediate irreparable negative effects stem from it.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Constitutional Court - in an interim order - decided on the questions raised by the retention of data as regulated by the transposition of EC directive 2006/24/EC of 15th March 2006 into domestic law. Pending a final decision, the Court declared that the law is probably unconstitutional in so far as it allows the forwarding of data in cases concerning persons against who a reasonable suspicion of having committed a crime does not exist. The retention of data as such, however, has not been declared unconstitutional.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The interim order is issued and all administrative measures, concerning the transmission of retained data in cases concerning persons against who a reasonable suspicion of having committed a crime does not exist, are halted, pending the final decision of the case. Yet the Constitutional Court did not halt the implementation and execution of article 113a TKG relating to the retention of data.

Annex 3 – Overview of the mandate of the Commissioners for Data Protection and their position in the administrative structure (German)

Ebene	Datenschutz im öffentlichen Bereich	Dienstaufsicht	Aufsichtsbehörde im nicht öffentlichen Bereich	Rechtsaufsicht	Fachaufsicht
Bund	Bundesdatenschutzbeauftragter	§ 22 V 2 BDSG → BMI	Jurisdiktion der Bundesländer (§ 38 VI BDSG)	X (§ 22 IV BDSG)[1] → Bundesregierung	-
Baden-Württemberg	Landesdatenschutzbeauftragter Baden-Württemberg	§ 26 III 1 LDSG-BW → Landes-innenministerium[2]	Landesinnenministerium[3]	X	X
Bayern	Landesdatenschutzbeauftragter Bayern	§ 29 II 2 BayDSG → Präsident des Landtags	Regierung Mittelfranken[4]	X	X
Berlin	Landesdatenschutzbeauftragter Berlin	§ 22 II 2 BinDSG → Präsident des Abgeordnetenhauses	Landesdatenschutzbeauftragter Berlin	X (§ 33 I BinDSG) → Senat	-
Brandenburg	Landesdatenschutzbeauftragter Brandenburg	§ 22 IV 3 BbgDSG → Präsident des Landtags[5]	Landesinnenministerium[6]	X	X
Bremen	Landesdatenschutzbeauftragter Bremen	§ 25 S. 2 BremDSG → Senat	Landesdatenschutzbeauftragter Bremen[7]	??	??

[1] Die Rechtsaufsicht ist beim Bundesbeauftragte für den öffentlichen Bereich explizit angeordnet und wir durch die Bundesregierung ausgeübt.
[2] Gemäß § 26 III S. 3 LDSG-BW reicht die Dienstaufsicht nur soweit die Unabhängigkeit des Landesdatenschutzbeauftragten dadurch nicht beeinträchtigt wird.
[3] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG durch Rechtsverordnung seitens der Landesregierung (DSZuVO), so dass die Aufsicht im privaten Bereich nicht speziell geregelt ist - aber von einer Einbeziehung in die allgemeinen Verwaltungsstrukturen ausgegangen werden kann.
[4] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG durch Rechtsverordnung seitens der Landesregierung (DSchVO), so dass die Aufsicht im privaten Bereich nicht speziell geregelt ist - aber von einer Einbeziehung in die allgemeinen Verwaltungsstrukturen ausgegangen werden kann.
[5] In § 22 IV S. 4 - S. 8 BbgDSG finden sich spezifische Vorgaben hinsichtlich der verschiedenen dienstaufsichtsrechtlichen Aspekte.
[6] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG durch Rechtsverordnung seitens der Landesregierung (DSZuVO), so dass die Aufsicht im privaten Bereich nicht speziell geregelt ist - aber von einer Einbeziehung in die allgemeinen Verwaltungsstrukturen ausgegangen werden kann.
[7] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG durch Rechtsverordnung seitens der Landesregierung. Allerdings wurde hier gerade der Landesdatenschutzbeauftragte selbst mit der Beaufsichtigung des privaten Bereiches betraut, so dass wegen der nicht vorliegenden Einbeziehung in den allgemeinen Verwaltungsaufbau unklar bleibt, ob dessen grundsätzliche Unabhängigkeit (§§ 25 S. 1 BremDSG) auch hinsichtlich des Privatsektors bestehen bleibt oder die betreffende Rechtsverordnung für den nicht öffentlichen Bereich speziell ein Aufsichtsregime anordnet, da diese elektronisch nicht verfügbar ist.

Hamburg	Landesdatenschutzbeauftragter Hamburg	§ 22 I 3 HmbDSG → Senat	Landesdatenschutzbeauftragter Hamburg[8]	??	??
Hessen	Landesdatenschutzbeauftragter Hessen	§§ 32 II 2 und 21 IV 4 HDSG → **??**[9]	Regierungspräsidium Darmstadt[10]	X	X
Mecklenburg-Vorpommern	Landesdatenschutzbeauftragter Mecklenburg-Vorpommern	§ 29 VI 2 LDSG-MV → Präsident des Landtags[11]	Landesdatenschutzbeauftragter Mecklenburg-Vorpommern	X (§ 33a LDSG-MV) → Landesregierung	-
Niedersachsen	Landesdatenschutzbeauftragter Niedersachsen	§ 21 II 2 NDSG → Landesregierung[12]	Landesdatenschutzbeauftragter Niedersachsen	X (§ 22 VI NDSG) → Landesregierung	X (§ 22 VI NDSG) → Landesregierung
Nordrhein-Westfalen	Landesdatenschutzbeauftragter Nordrhein-Westfalen	§ 21 III 3 DSG-NRW → Landes-innenministerium[13]	Landesdatenschutzbeauftragter Nordrhein-Westfalen	X (§ 22 VI DSG-NRW) → Innenministerium	X (§ 22 VI DSG-NRW) → Innenministerium
Rheinland-Pfalz	Landesdatenschutzbeauftragter Rheinland-Pfalz	§ 23 I 2 LDSG-RP → Präsident des Landtags	Landesdatenschutzbeauftragter Rheinland-Pfalz	X (§ 24 I LDSG-RP)	-
Saarland	Landesdatenschutzbeauftragter Saarland	§ 25 III 2 SDSG → Präsident des Landtags[14]	Landesinnenministerium[15]	X	X
Sachsen	Landesdatenschutzbeauftragter Sachsen	§ 25 IV 2 Sächs-DSG → Präsident des Landtags[16]	Landesdatenschutzbeauftragter Sachsen	X (§ 30a Sächs-DSG)	-

[8] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG in Verbindung mit § 23 VII HmbDSG durch Rechtsverordnung seitens der Landesregierung. Allerdings wurde hier gerade der Landesdatenschutzbeauftragte selbst mit der Beaufsichtigung des privaten Bereiches betraut, so dass wegen der nicht vorliegenden Einbeziehung in den allgemeinen Verwaltungsaufbau unklar bleibt, ob dessen grundsätzliche Unabhängigkeit (§ 22 I 1 HmbDSG) auch hinsichtlich des Privatsektors bestehen bleibt oder die betreffende Rechtsverordnung für den nicht öffentlichen Bereich speziell ein Aufsichtsregime anordnet, da diese elektronisch nicht verfügbar ist.

[9] Die angeführten Vorschriften regeln einzelne dienstrechtliche Aspekte. Da die Dienstaufsicht jedoch nicht ausdrücklich angeordnet ist fragt sich, ob die in § 22 HDSG angeordnete grundsätzliche Unabhängigkeit des Landesdatenschutzbeauftragten uneingeschränkt greift.

[10] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG durch Rechtsverordnung seitens der Landesregierung (DSZuVO), so dass die Aufsicht im privaten Bereich nicht speziell geregelt ist - aber von einer Einbeziehung in die allgemeinen Verwaltungsstrukturen ausgegangen werden kann.

[11] § 29 VII, VIII LDSG-MV regeln einige dienstaufsichtsrechtliche Details.

[12] Gemäß § 21 III 1 NDSG ist die Geschäftsstelle de Landesdatenschutzbeauftragte beim Landesinnenministerium angesiedelt. Außerdem regelt die Norm einige dienstaufsichtsrechtliche Details. Die Unabhängigkeit des Landesdatenschutzbeauftragten wird im gesamten NDSG nicht ausdrücklich gesetzlich festgeschrieben.

[13] § 21 IV, V DSG-NRW regeln einige dienstaufsichtsrechtliche Details.

[14] Gemäß § 25 III S. 2, 2. HS SDSG reicht die Dienstaufsicht außerdem nur soweit die Unabhängigkeit des Landesdatenschutzbeauftragten dadurch nicht beeinträchtigt wird. § 25 III S. 1 SDSG stellt ferner die Weisungsfreiheit des Landesdatenschutzbeauftragten positiv fest.

[15] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG durch Rechtsverordnung seitens der Landesregierung (DSZuVO), so dass die Aufsicht im privaten Bereich nicht speziell geregelt ist - aber von einer Einbeziehung in die allgemeinen Verwaltungsstrukturen ausgegangen werden kann.

Sachsen-Anhalt	Landesdatenschutzbeauftragter Sachsen-Anhalt	§ 21 I 2 DSG-SA → Präsident des Landtags[17]	Landesverwaltungsamt[18]	X	X
Schleswig-Holstein	Landesdatenschutzbeauftragter Schleswig-Holstein	§ 35 V 1 LDSG-SH → Ministerpräsident[19]	Landesdatenschutzbeauftragter Schleswig-Holstein	X (§ 38 LDSG-SH)	-
Thüringen	Landesdatenschutzbeauftragter Thüringen	§ 36 I 2 Thür-DSG → Präsident des Landtags[20]	Landesverwaltungsamt[21]	X	X

[16] Gemäß § 25 IV S. 2, 2. HS Sächs-DSG reicht die Dienstaufsicht außerdem nur soweit die Unabhängigkeit des Landesdatenschutzbeauftragten dadurch nicht beeinträchtigt wird und der restliche Absatz IV sowie Absatz V regeln weitere dienstaufsichtsrechtliche Details.
[17] Die Norm regelt außerdem einige aufsichtsrechtliche Details.
[18] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG durch eine elektronisch nicht verfügbare Rechtsverordnung seitens der Landesregierung, so dass die Aufsicht im privaten Bereich nicht speziell geregelt ist - aber von einer Einbeziehung in die allgemeinen Verwaltungsstrukturen ausgegangen werden kann.
[19] Terminologisch ist hier nicht von Dienstaufsicht sondern nur vom Dienstvorgesetzten die Rede.
[20] Die Absätze II bis VI des § 26 Thür-DSG regeln einige dienstaufsichtsrechtliche Details.
[21] Die Übertragung erfolgte aufgrund der Ermächtigungsgrundlage des § 38 VI BDSG durch eine elektronisch nicht verfügbare Rechtsverordnung seitens der Landesregierung, so dass die Aufsicht im privaten Bereich nicht speziell geregelt ist - aber von einer Einbeziehung in die allgemeinen Verwaltungsstrukturen ausgegangen werden kann.

Annex 4 - Overview of competences of the Commissioners for Data Protection at the Federal and at the *Länder* level (German)

Ebene	Datenschutz (im öffentlichen Bereich)	Stellungnahmen [22]	Gutachten [23]	Empfehlungen [24]	Tätigkeitsberichte
Bund	Bundesdatenschutzbeauftragter	(-) BDSG	§ 26 II BDSG	§ 26 III BDSG	§ 26 I BDSG → alle zwei Jahre
Baden-Württemberg	Landesdatenschutzbeauftragter Baden-Württemberg	§ 31 III 2 [25] LDSG-BW	§ 31 II LDSG-BW	§ 31 III 1 LDSG-BW	§ 31 I LDSG-BW → alle zwei Jahre
Bayern	Landesdatenschutzbeauftragter Bayern	(-) BayDSG	§ 30 VI BayDSG	(-) BayDSG	§ 30 V BayDSG → alle zwei Jahre
Berlin	Landesdatenschutzbeauftragter Berlin	(-) [26] BinDSG	§ 29 I, III BinDSG	§ 24 I, III BinDSG	§ 29 II BinDSG → jährlich
Brandenburg	Landesdatenschutzbeauftragter Brandenburg	§ 23 V [27] BbgDSG	§ 23 IV BbgDSG	§ 23 II BbgDSG	§ 27 BbgDSG → alle zwei Jahre
Bremen	Landesdatenschutzbeauftragter Bremen	(-) [28] BremDSG	§ 32 I BremDSG	§ 27 I BremDSG	§ 33 I BremDSG → jährlich
Hamburg	Landesdatenschutzbeauftragter Hamburg	(-) HmbDSG	§ 23 III 1 HmbDSG	§ 23 II HmbDSG	§ 23 III 2 HmbDSG → alle zwei Jahre
Hessen	Landesdatenschutzbeauftragter Hessen	§ 21 V HDSG	§ 25 I HDSG	§ 24 I HDSG	§ 30 I HDSG → jährlich

[22] Obligatorische Einbeziehung in das Gesetzgebungsverfahren bei Datenschutzrelevanz
[23] Auf Ersuchen der jeweiligen (Landes-)Regierung oder des jeweiligen (Landes-)Parlaments.
[24] Initiativ durch den Datenschutzbeauftragten in sämtlichen relevanten Bereichen (d.h. auch im Gesetzgebungsverfahren).
[25] ausschließlich bezüglich der Verarbeitung personenbezogener Daten.
[26] Zwar wird dies nicht konkret gesetzlich angeordnet – jedoch besteht mit § 24 I 3 BinDSG eine dynamische Verweisung auf internationale und europäische Rechtsakte (vgl:: Art. 28 III Richtlinie 95/46/EC
[27] Fakultative Formulierung („kann an den Sitzungen des Landtages und seiner Ausschüsse teilnehmen und Stellung nehmen"; „Der Landtag und seine Ausschüsse können seine Anwesenheit und seine mündliche oder schriftliche Stellungnahme verlangen").
[28] Gemäß § 27 II Nr. 2 BremDSG besteht aber eine Unterrichtungspflicht bezüglich datenschutzrelevanten Gesetzgebungsvorhaben.

Mecklenburg-Vorpommern	Landesdatenschutzbeauftragter Mecklenburg-Vorpommern	§ 33 II 4[29] LDSG-MV	§ 33 II 3 LDSG-MV	§ 33 II 2 LDSG-MV	§ 33 I LDSG-MV → alle zwei Jahre
Niedersachsen	Landesdatenschutzbeauftragter Niedersachsen	§ 22 I 4 [30] NDSG	§ 22 II 4, 5 [31] NDSG	§ 22 I 3 [32] NDSG	§ 22 III 1 NDSG → alle zwei Jahre
Nordrhein-Westfalen	Landesdatenschutzbeauftragter Nordrhein-Westfalen	(-) [33] DSG-NRW	§ 22 IV DSG-NRW	§ 22 I DSG-NRW	§ 27 DSG-NRW → alle zwei Jahre
Rheinland- Pfalz	Landesdatenschutzbeauftragter Rheinland-Pfalz	§ 23 VIII [34] LDSG-RP	§ 24 V LDSG-RP	§ 24 III, IV [35] LDSG-RP	§ 29 II LDSG-RP → alle zwei Jahre
Saarland	Landesdatenschutzbeauftragter Saarland	(-) SDSG	§ 26 IV SDSG	§ 26 II 1 SDSG	§ 29 SDSG → alle zwei Jahre
Sachsen	Landesdatenschutzbeauftragter Sachsen	§ 26 [36] Sächs-DSG	§ 30 III Sächs-DSG	§ 30 IV Sächs-DSG	§ 30 I Sächs-DSG → alle zwei Jahre
Sachsen-Anhalt	Landesdatenschutzbeauftragter Sachsen-Anhalt	(-) DSG-SA	§ 22 VI DSG-SA	§ 22 IV DSG-SA	§ 22 IVa DSG-SA → alle zwei Jahre
Schleswig-Holstein	Landesdatenschutzbeauftragter Schleswig-Holstein	(-) [37] LDSG-SH	§ 39 IV 1 LDSG-SH	§ 39 III LDSG-SH	§ 39 IV 2 LDSG-SH → jährlich
Thüringen	Landesdatenschutzbeauftragter Thüringen	(-) Thür-DSG	§ 40 IV Thür-DSG	§ 40 VII Thür-DSG	§ 40 I 1 Thür-DSG → alle zwei Jahre

[29] Anhörungspflicht hinsichtlich des Erlasses oder der Änderung von Rechts- oder Verwaltungsvorschriften die das Recht auf informationelle Selbstbestimmung berühren.
[30] Anhörungspflicht hinsichtlich des Erlasses oder der Änderung von Rechts- oder Verwaltungsvorschriften die das Recht auf informationelle Selbstbestimmung berühren.
[31] Als Untersuchungsersuchen bezeichnet und grundsätzlich mündlich möglich, es sei denn in bedeutsamen Fällen.
[32] Als Beratung bezeichnet.
[33] Gemäß § 22 III 2 DSG-NRW besteht aber eine Unterrichtungspflicht bezüglich Gesetzgebungsvorhaben welche personenbezogene Daten betreffen.
[34] Fakultative Formulierung („kann an den Sitzungen des Landtags teilnehmen“; „Landtag und seine Ausschüsse können seine Anwesenheit verlangen“; „kann sich in Ausschusssitzungen zu Fragen äußern“).
[35] Als Vorschläge bzw. Beratung bezeichnet.
[36] Anhörungspflicht hinsichtlich des Erlasses oder der Änderung von Rechts- oder Verwaltungsvorschriften die das Recht auf informationelle Selbstbestimmung berühren.
[37] Allerdings ordnet das LDSG-SH in § 5 III (Datenschutzsicherheitsmaßnahmen der Landesregierung) und § 16 III (Datenübermittlung an ausländische Stellen) eine spezifische Anhörungspflicht des Landesdatenschutzbeauftragten in bestimmten Teilbereichen an.

Ebene	Datenschutz (im öffentlichen Bereich)	Anrufungen	Beanstandungen	Informationsfreiheit
Bund	Bundesdatenschutzbeauftragter	§ 21 BDSG	§ 25 BDSG	X
Baden-Württemberg	Landesdatenschutzbeauftragter Baden-Württemberg	§ 27 I LDSG-BW	§ 30 LDSG-BW	-
Bayern	Landesdatenschutzbeauftragter Bayern	§ 9 BayDSG	§ 31 I BayDSG	-
Berlin	Landesdatenschutzbeauftragter Berlin	§ 27 BinDSG	§ 26 I BinDSG	X
Brandenburg	Landesdatenschutzbeauftragter Brandenburg	§ 21 BbgDSG	§ 25 BbgDSG	X
Bremen	Landesdatenschutzbeauftragter Bremen	§ 22b BremDSG	§ 29 I BremDSG	X
Hamburg	Landesdatenschutzbeauftragter Hamburg	§ 26 I HmbDSG	§ 25 I HmbDSG	-
Hessen	Landesdatenschutzbeauftragter Hessen	§ 28 I HDSG	§ 27 I HDSG	-
Mecklenburg-Vorpommern	Landesdatenschutzbeauftragter Mecklenburg-Vorpommern	§ 26 LDSG-MV	§ 32 LDSG-MV	X
Niedersachsen	Landesdatenschutzbeauftragter Niedersachsen	§ 19 I NDSG	§ 23 I 1 NDSG	-
Nordrhein-Westfalen	Landesdatenschutzbeauftragter Nordrhein-Westfalen	§ 25 I DSG-NRW	§ 24 I DSG-NRW	X
Rheinland- Pfalz	Landesdatenschutzbeauftragter Rheinland-Pfalz	§ 29 I LDSG-RP	§ 25 I LDSG-RP	-
Saarland	Landesdatenschutzbeauftragter Saarland	§ 23 I SDSG	§ 27 I SDSG	X
Sachsen	Landesdatenschutzbeauftragter Sachsen	§ 24 I Sächs-DSG	§ 29 Sächs-DSG	-
Sachsen-Anhalt	Landesdatenschutzbeauftragter Sachsen-Anhalt	§ 19 DSG-SA	§ 24 I DSG-SA	X
Schleswig-Holstein	Landesdatenschutzbeauftragter Schleswig-Holstein	§ 40 LDSG-SH	§ 42 II LDSG-SH	X
Thüringen	Landesdatenschutzbeauftragter Thüringen	§ 11 I Thür-DSG	§ 39 I Thür-DSG	-

Annex 5 – Overview of sanctions available at the Federal ad at the Länder level (German)

Ebene	Datenschutz (im öffentlichen Bereich)	Straftaten	Ordnungswidrigkeiten
Bund	Bundesdatenschutzbeauftragter	§ 44 I BDSG [38] → bis zu zwei Jahre	§ 43 I, II BDSG § 43 III → bis 250.000 €
Baden-Württemberg	Landesdatenschutzbeauftragter Baden-Württemberg	§ 41 LDSG-BW [39] → bis zu zwei Jahre	§ 40 I LDSG-BW [40] § 40 II → bis 25.000 €
Bayern	Landesdatenschutzbeauftragter Bayern	§ 37 III 1 BayDSG [41] → bis zu zwei Jahre	§ 37 I, II BayDSG [42] § 37 I, II → bis 25.000 €
Berlin	Landesdatenschutzbeauftragter Berlin	§ 32 I, II BinDSG [43] → bis zu zwei Jahre	(**-**) BinDSG
Brandenburg	Landesdatenschutzbeauftragter Brandenburg	§ 38 III BbgDSG [44] → bis zu zwei Jahre	§ 38 I BbgDSG § 38 II → bis 50.000 €

[38] Gemäß § 44 II 1 BDSG handelt es sich um ein Antragsdelikt; Antragsberechtigt sind gemäß § 44 II 2 BDSG der Betroffene, der Bundesdatenschutzbeauftragte und die Aufsichtsbehörde (welche für den nicht-öffentlichen Bereich gemäß § 38 VI BDSG von der jeweiligen Landesregierung bestimmt wurde).
[39] § 41 S. 2 LDSG-BW ordnet die Strafbarkeit des Versuchs an.
[40] Als Verwaltungsbehörden i.S.v. § 36 I Nr. 1 OWIG sind die Regierungspräsidien bestimmt.
[41] Gemäß § 37 III 2 BayDSG handelt es sich um ein Antragsdelikt; der Landesdatenschutzbeauftragte ist gemäß § 37 III 3 BayDSG antragsberechtigt.
[42] 50.000 DM
[43] Nach § 33 II BinDSG ist nur Strafbarkeit von bis zu einem Jahr angeordnet, wenn keine Schädigungs- oder Bereicherungsabsicht vorliegt.
Gemäß § 32 III 1 BinDSG handelt es sich um ein Antragsdelikt; der Landesdatenschutzbeauftragte ist gemäß § 32 III 2 BinDSG antragsberechtigt.
Der Landesdatenschutzbeauftragte ist nach § 32 III 3 BinDSG auch gegen den Willen des Betroffenen antragsberechtigt!
[44] Gemäß § 38 III 2 BbgDSG handelt es sich um ein Antragsdelikt; der Landesdatenschutzbeauftragte ist gemäß § 38 III 3 BbgDSG antragsberechtigt.

Bremen	Landesdatenschutzbeauftragter Bremen	§ 37 BremDSG → bis zu zwei Jahre	§ 38 I BremDSG § 38 II → bis 25.000 €
Hamburg	Landesdatenschutzbeauftragter Hamburg	§ 32 I HmbDSG [45] → bis zu zwei Jahre	§ 33 I HmbDSG § 33 II → bis 25.000 €
Hessen	Landesdatenschutzbeauftragter Hessen	§ 40 I HDSG [46] → bis zu zwei Jahre	§ 41 I HDSG § 41 II → bis 25.000 € [47]
Mecklenburg-Vorpommern	Landesdatenschutzbeauftragter Mecklenburg-Vorpommern	§ 42 I,II, III LDSG-MV [48] → bis zu zwei Jahre	(-) LDSG-MV
Nordrhein-Westfalen	Landesdatenschutzbeauftragter Nordrhein-Westfalen	§ 33 I DSG-NRW [49] → bis zu zwei Jahre	§ 34 I DSG-NRW [50] § 34 II → bis 50.000 €
Rheinland- Pfalz	Landesdatenschutzbeauftragter Rheinland-Pfalz	§ 37 I LDSG-RP [51] → bis zu einem Jahr	(-) LDSG-RP
Saarland	Landesdatenschutzbeauftragter Saarland	§ 35 I SDSG [52] → bis zu zwei Jahre	§ 36 I SDSG § 36 II → bis 50.000 €

[45] § 32 II HmbDSG ordnet die Strafbarkeit des Versuchs an.
Gemäß § 32 III HmbDSG handelt es sich um ein Antragsdelikt.
§ 32 IV HmbDSG stellt eine allgemeine Subsidiaritätsklausel auf.
[46] § 40 II HDSG stellt eine allgemeine Subsidiaritätsklausel auf.
[47] 50.000 DM
[48] Gemäß § 42 IV LDSG-MV handelt es sich um ein Antragsdelikt; der Landesdatenschutzbeauftragte ist antragsberechtigt.
Nach Absatz I und II ist nur Strafbarkeit von bis zu einem Jahr angeordnet, wenn keine Schädigungs- oder Bereicherungsabsicht vorliegt.
[49] In § 33 I a.E. ist die Strafbarkeit des Versuchs angeordnet.
[50] § 34 II a DSG-NRW bestimmt die Bezirksregierung als Verwaltungsbehörde i.S.v. § 36 I Nr. 1 OWIG für das DSG-NRW, während für die Zwecke des § 43 BDSG der Landesdatenschutzbeauftragte NRW.
[51] § 37 II NDSG ordnet die Strafbarkeit des Versuchs an.
[52] § 35 II SDSG stellt eine allgemeine Subsidiaritätsklausel auf.

Sachsen	Landesdatenschutzbeauftragter Sachsen	§ 39 Sächs-DSG → bis zu zwei Jahre	§ 38 I Sächs-DSG [53] § 38 II → bis 25.000 €
Sachsen-Anhalt	Landesdatenschutzbeauftragter Sachsen-Anhalt	§ 31 DSG-SA [54] → bis zu zwei Jahre	§31a I, II DSG-SA § 31a III → bis 250.000 €
Schleswig-Holstein	Landesdatenschutzbeauftragter Schleswig-Holstein	(**-**) LDSG-SH	§ 44 I LDSG-SH § 44 II → bis 50.000 €
Thüringen	Landesdatenschutzbeauftragter Thüringen	§ 42 I,II,III Thür-DSG [55] → bis zu zwei Jahre	(**-**) Thür-DSG

[53] Interessant ist § 38 III Sächs-DSG welcher den Sächsischen Datenschutzbeauftragten zur Verwaltungsbehörde i.S.v. § 36 I Nr. 1 OWIG macht.

[54] Gemäß § 31 III DSG-SA handelt es sich um ein Antragsdelikt, es sei denn, dass besonderes öffentliches Strafverfolgungsinteresse besteht. Allerdings ist der Landesdatenschutzbeauftragte nach § 22 VIII DSG-SA berechtigt Strafverfolgung zu beantragen.

[55] Gemäß § 42 IV Thür-DSG handelt es sich um ein Antragsdelikt; der Landesdatenschutzbeauftragte ist antragsberechtigt.
Nach Absatz I und II ist nur Strafbarkeit von bis zu einem Jahr angeordnet, wenn keine Schädigungs- oder Bereicherungsabsicht vorliegt.

Annex 6 - Overview of relevant provisions of the Länder Constitutions (German)

Ebene	Datenschutz i.d. Landesverfassung	Beauftragter für Datenschutz i.d. Landesverfassung
Baden-Württemberg	**(-)**	**(-)**
Bayern	**(-)**	Art. 33a
Berlin	Art. 47	Art. 47
Brandenburg	Art. 11	Art. 74
Bremen	Art. 12	**(-)**
Hamburg	**(-)**	**(-)**
Hessen	**(-)**	**(-)**
Mecklenburg-Vorpommern	Art. 6	Art. 37
Niedersachsen	**(-)**	Art. 62
Nordrhein-Westfalen	Art. 4 para 2	Art. 77a
Rheinland- Pfalz	Art. 4a	**(-)**
Saarland	Art. 2	**(-)**
Sachsen	Art. 34	Art. 57
Sachsen-Anhalt	Art. 6	**(-)**
Schleswig-Holstein	**(-)**[56]	**(-)**
Thüringen	Art. 6 para 2	Art. 69

See: http://www.verfassungen.de/de/

[56] Indirekte Bezugnahmen auf den Datenschutz in Art. 23 para 3 bezüglich des Frage- und Auskunftsrechts der Abgeordneten.

Annex 3 – Overview of the mandate of the Commissioners for Data Protection and their position in the administrative structure (English)

Level	Data Protection (in the public sector)	Administrative Supervision	Data Protection Authority in the private sector	Legal Supervision	Technical Supervision
Bund	Federal Commissioner for Data Protection	Art. 22 V 2 DPL → Federal Ministry of the Interior	Jurisdiction of the Länder (Art. 38 VI DPL)	X (Art. 22 IV DPL)[57] → Federal Government	-
Baden-Württemberg	Landes Commissioner for Data Protection Baden-Württemberg	Art. 26 III 1 DPL-BW → Landes Ministry of the Interior[58]	Landes Ministry of the Interior[59]	X	X
Bayern	Landes Commissioner for Data Protection Bayern	Art. 29 II 2 DPL-Bay → President of the Landes Parliament	Local Executive of Mittelfranken[60]	X	X
Berlin	Landes Commissioner for Data Protection Berlin	Art. 22 II 2 DPL-Berlin → President of the Landes Parliament	Landes Commissioner for Data Protection Berlin	X (Art. 33 I DPL-Berlin) → Landes Executive	-
Brandenburg	Landes Commissioner for Data Protection Brandenburg	Art. 22 IV 3 DPL-Bbg → President of the Landes Parliament[61]	Landes Ministry of the Interior[62]	X	X
Bremen	Landes Commissioner for Data Protection	Art. 25 S. 2 DPL-Bremen → Landes	Landes Commissioner for Data Protection Bremen[63]	??	??

[57] Concerning the Federal Commissioner for Data Protection the Legal Supervision of the public sector supervision authority is explicitly provided for and is exercised by the Federal Government.
[58] According to Art. 26 III S. 3 DPL-BW the Administrative Supervision does only extend to the point of not infringing upon the independence of the Landes Commissioner for Data Protection.
[59] The transferral of authority is based upon the empowerment of Art. 38 VI DPL by way of ordinance on the part of the Landes Government (DSZuVO), thus the supervision of the private sector has not been specifically provided for in the law, yet it is to be supposed that the data protection authority is included in the general administrative hierarchy and therefore subjected to the full degree of supervision.
[60] The transferral of authority is based upon the empowerment of Art. 38 VI DPL by way of ordinance on the part of the Landes Government (DSchVO), thus the supervision of the private sector has not been specifically provided for in the law, yet it is to be supposed that the data protection authority is included in the general administrative hierarchy and therefore subjected to the full degree of supervision.
[61] Art.22 IV 4 - 8 DPL-Bbg lays down specifications concerning certain aspects limiting the scope of the Administrative Supervision.
[62] The transferral of authority is based upon the empowerment of Art. 38 VI DPL by way of ordinance on the part of the Landes Government (DSZuVO), thus the supervision of the private sector has not been specifically provided for in the law, yet it is to be supposed that the data protection authority is included in the general administrative hierarchy and therefore subjected to the full degree of supervision.

	Bremen	Executive			
Hamburg	Landes Commissioner for Data Protection Hamburg	Art. 22 I 3 DPL-Hamburg → Landes Executive	Landes Commissioner for Data Protection Hamburg[64]	??	??
Hessen	Landes Commissioner for Data Protection Hessen	Arts.32 II 2 und 21 IV 4 DPL-H → **??**[65]	Local Executive Darmstadt[66]	X	X
Mecklenburg-Vorpommern	Landes Commissioner for Data Protection Mecklenburg-Vorpommern	Art. 29 VI 2 DPL-MV → President of the Landes Parliament[67]	Landes Commissioner for Data Protection Mecklenburg-Vorpommern	X (Art. 33a DPL-MV) → Landesregierung	-
Niedersachsen	Landes Commissioner for Data Protection Niedersachsen	Art. 21 II 2 DPL-N → Landes Executive[68]	Landes Commissioner for Data Protection Niedersachsen	X (Art. 22 VI DPL-N) → Landes Executive	X (Art. 22 VI DPL-N) → Landes Executive

[63] The transferral of authority is based upon the empowerment of Art. 38 VI DPL by way of ordinance on the part of the Landes Government. Yet in this case the Landes Commissioner for Data Protection and not another supervision authority was mandated to supervise the private sector with the result that due to the lacking inclusion into the administrative hierarchy it remains unclear whether or not the principally prescribed independence of the Commissioner (Art. 25 S. 1 DPL-Bremen) remains in effect to the full extent regarding the supervision of the private sector or if the pertinent ordinance (which is not available online or in electronic form) provides for a greater degree of supervision of the Commissioner in this area.

[64] The transferral of authority is based upon the empowerment of Art. 38 VI DPL in combination with Art. 23 VII DPL-Hamburg by way of ordinance on the part of the Landes Government. Yet in this case the Landes Commissioner for Data Protection and not another supervision authority was mandated to supervise the private sector with the result that due to the lacking inclusion into the administrative hierarchy it remains unclear whether or not the principally prescribed independence of the Commissioner (§ 22 I 1 DPL-Hamburg) remains in effect to the full extent regarding the supervision of the private sector or if the pertinent ordinance (which is not available online or in electronic form) provides for a greater degree of supervision of the Commissioner in this area.

[65] The cited norms lay down specifications concerning certain aspects limiting the scope of the Administrative Supervision. Since the Administrative Supervision is not explicitly prescribed in the law it is questionable whether the principle independence of the Commissioner as provided for in Art. 22 DPL-Hessen is granted to its full extent.

[66] The transferral of authority is based upon the empowerment of Art. 38 VI DPL by way of ordinance on the part of the Landes Government (DSZuVO), thus the supervision of the private sector has not been specifically provided for in the law, yet it is to be supposed that the data protection authority is included in the general administrative hierarchy and therefore subjected to the full degree of supervision.

[67] Art 29 VII, VIII DPL-MV lays down specifications concerning certain aspects limiting the scope of the Administrative Supervision.

[68] According to Art. 21 III 1 DPL-N the office of the Landes Commissioner for Data Protection resides at the Landes Ministry of the Interior. Also the norm lays down specifications concerning certain aspects limiting the scope of the Administrative Supervision. The independence of the Commissioner is not provided for explicitly in the DPL-N at all.

Nordrhein-Westfalen	Landes Commissioner for Data Protection Nordrhein-Westfalen	Art. 21 III 3 DPL-NRW → Landes Ministry of the Interior[69]	Landes Commissioner for Data Protection Nordrhein-Westfalen	X (Art. 22 VI DPL-NRW) → Ministry of the Interior	X (Art. 22 VI DPL-NRW) → Ministry of the Interior
Rheinland-Pfalz	Landes Commissioner for Data Protection Rheinland-Pfalz	Art. 23 I 2 DPL-RP → President of the Landes Parliament	Landes Commissioner for Data Protection Rheinland-Pfalz	X (Art. 24 I DPL-RP)	-
Saarland	Landes Commissioner for Data Protection Saarland	Art. 25 III 2 DPL-S → President of the Landes Parliament[70]	Landes Ministry of the Interior[71]	X	X
Sachsen	Landes Commissioner for Data Protection Sachsen	Art. 25 IV 2 DPL-Sachsen → President of the Landes Parliament[72]	Landes Commissioner for Data Protection Sachsen	X (Art. 30a DPL-Sachsen)	-
Sachsen-Anhalt	Landes Commissioner for Data Protection Sachsen-Anhalt	Art. 21 I 2 DPL-SA → President of the Landes Parliament[73]	Regional Administrative Body[74]	X	X
Schleswig-Holstein	Landes Commissioner for Data Protection Schleswig-Holstein	Art. 35 V 1 DPL-SH → Head of the Landes Executive[75]	Landes Commissioner for Data Protection Schleswig-Holstein	X (Art. 38 DPL-SH)	-
Thüringen	Landes Commissioner for Data Protection Thüringen	Art. 36 I 2 DPL-Thüringen → President of the Landes Parliament[76]	Regional Administrative Body[77]	X	X

[69] Art. 21 IV, V DPL-NRW lays down some specifications concerning certain aspects limiting the scope of the Administrative Supervision.
[70] According to Art. 25 III 2 SDSG the Administrative Supervision does only extend to the point of not infringing upon the independence of the Landes Commissioner for Data Protection. Furthermore Art. 25 III 1 SDSG positively provides for the freedom of the Commissioner from subjection to orders in the administrative hierarchy.
[71] The transferral of authority is based upon the empowerment of Art. 38 VI DPL by way of ordinance on the part of the Landes Government (DSZuVO), thus the supervision of the private sector has not been specifically provided for in the law, yet it is to be supposed that the data protection authority is included in the general administrative hierarchy and therefore subjected to the full degree of supervision.
[72] According to Art. 25 IV S. 2, 2. HS DPL-Sachsen the Administrative Supervision does only extend to the point of not infringing upon the independence of the Landes Commissioner for Data Protection. The remainder of Art. 25 IV as well as Art. 25 V lay down specifications concerning certain aspects limiting the scope of the Administrative Supervision.
[73] The cited norm also lays down some specifications concerning certain aspects limiting the scope of the Administrative Supervision.
[74] The transferral of authority is based upon the empowerment of Art. 38 VI DPL by way of ordinance on the part of the Landes Government which is not available online. Thus the supervision of the private sector supervision authority is no explicitly laid down, yet it is to be supposed that the data protection authority is included in the general administrative hierarchy and therefore subjected to the full degree of supervision.
[75] The norm does not use the term Administrative Supervision but refers to the administrative Superior.
[76] Art. 26 II – VI DPL-Thüringen lays down specifications concerning certain aspects limiting the scope of the Administrative Supervision.

Annex 4 - Overview of competences of the Commissioners for Data Protection at the Federal and at the *Länder* level (English)

Level	Data Protection (in the public sector)	Statements [78]	Opinions [79]	Recommendations [80]	Reports
Bund	Federal Commissioner for Data Protection	(-) DPL	Art. 26 II DPL	Art. 26 III DPL	Art. 26 I DPL → every two years
Baden-Württemberg	Landes Commissioner for Data Protection Baden-Württemberg	Art. 31 III 2 [81] DPL-BW	Art. 31 II DPL-BW	Art. 31 III 1 DPL-BW	Art. 31 I DPL-BW → every two years
Bayern	Landes Commissioner for Data Protection Bayern	(-) DPL-Bay	Art. 30 VI DPL-Bay	(-) DPL-Bay	Art. 30 V DPL-Bay → every two years
Berlin	Landes Commissioner for Data Protection Berlin	(-) [82] DPL-Berlin	Art. 29 I, III DPL-Berlin	Art. 24 I, III DPL-Berlin	Art. 29 II DPL-Berlin → every year
Brandenburg	Landes Commissioner for Data Protection Brandenburg	Art. 23 V [83] DPL-Bbg	Art. 23 IV DPL-Bbg	Art. 23 II DPL-Bbg	Art. 27 DPL-Bbg → every two years

[77] The transferral of authority is based upon the empowerment of Art. 38 VI DPL by way of ordinance on the part of the Landes Government which is not available online. Thus the supervision of the private sector supervision authority is no explicitly laid down, yet it is to be supposed that the data protection authority is included in the general administrative hierarchy and therefore subjected to the full degree of supervision.
[78] Inclusion into the legislative process if data protection is concerned.
[79] Upon request of the respective (Landes-)government ort he respective (Landes-)parliament.
[80] On the initiative of the Commissioner for Data Protection in all relevant areas (thus possibly also in the legislative process)
[81] Exclusively concerning the processing of personal data.
[82] Even though it is not explicitly provided for by the norm it is a dynamic reference to international and European legal act (cf.: Art. 28 III Directive 95/46/EC).
[83] Facultative wording („may take part…"; „…may request opinions").

Bremen	Landes Commissioner for Data Protection Bremen	(-) [84] DPL-Bremen	Art. 32 I DPL-Bremen	Art. 27 I DPL-Bremen	Art. 33 I DPL-Bremen → every year
Hamburg	Landes Commissioner for Data Protection Hamburg	(-) DPL-Hamburg	Art. 23 III 1 DPL-Hamburg	Art. 23 II DPL-Hamburg	Art. 23 III 2 DPL-Hamburg → every two years
Hessen	Landes Commissioner for Data Protection Hessen	Art. 21 V DPL-H	Art. 25 I DPL-H	Art. 24 I DPL-H	Art. 30 I DPL-H → every year
Mecklenburg-Vorpommern	Landes Commissioner for Data Protection Mecklenburg-Vorpommern	Art. 33 II 4 [85] DPL-MV	Art. 33 II 3 DPL-MV	Art. 33 II 2 DPL-MV	Art. 33 I DPL-MV → every two years
Niedersachsen	Landes Commissioner for Data Protection Niedersachsen	Art. 22 I 4 [86] DPL-N	Art. 22 II 4, 5 [87] DPL-N	Art. 22 I 3 [88] DPL-N	Art. 22 III 1 DPL-N → every two years
Nordrhein-Westfalen	Landes Commissioner for Data Protection Nordrhein-Westfalen	(-) [89] DPL-NRW	Art. 22 IV DPL-NRW	Art. 22 I DPL-NRW	Art. 27 DPL-NRW → every two years
Rheinland- Pfalz	Landes Commissioner for Data Protection Rheinland-Pfalz	Art. 23 VIII [90] DPL-RP	Art. 24 V DPL-RP	Art. 24 III, IV [91] DPL-RP	Art. 29 II DPL-RP → every two years
Saarland	Landes Commissioner for Data Protection Saarland	(-) DPL-S	Art. 26 IV DPL-S	Art. 26 II 1 DPL-S	Art. 29 DPL-S → every two years
Sachsen	Landes Commissioner for Data Protection Sachsen	Art. 26 [92] DPL-Sachsen	Art. 30 III DPL-Sachsen	Art. 30 IV DPL-Sachsen	Art. 30 I DPL-Sachsen → every two years
Sachsen-Anhalt	Landes Commissioner for Data Protection	(-)	Art. 22 VI DPL-SA	Art. 22 IV DPL-SA	Art. 22 IVa DPL-SA → every two years

[84] According to Art. 27 II Nr. 2 DPL-Bremen there is a duty to notify with respect to legislative bills relevant to data protection.
[85] Duty to have a hearing concerning the enactment or change of legal or administrative norms pertaining to the right to informational self-determination.
[86] Duty to have a hearing concerning the enactment or change of legal or administrative norms pertaining to the right to informational self-determination.
[87] Termed a request for examination and principally conducted verbally except in particularly significant cases.
[88] Termed consultation.
[89] According to Art. 22 III 2 DPL-NRW there is a duty to notify with respect to legislative bills relevant to data protection.
[90] Facultative wording („may take part…"; „…may request the Data Commissioners presence"; „may issue an opinion").
[91] Termed proposals or consultation respectively.
[92] Duty to have a hearing concerning the enactment or change of legal or administrative norms pertaining to the right to informational self-determination.

	Sachsen-Anhalt	DPL-SA			
Schleswig-Holstein	Landes Commissioner for Data Protection Schleswig-Holstein	(-) [93] DPL-SH	Art. 39 IV 1 DPL-SH	Art. 39 III DPL-SH	Art. 39 IV 2 DPL-SH → every year
Thüringen	Landes Commissioner for Data Protection Thüringen	(-) DPL-Thüringen	Art. 40 IV DPL-Thüringen	Art. 40 VII DPL-Thüringen	Art. 40 I 1 DPL-Thüringen → every two years

Level	**Data Protection (in the public sector)**	**Appeals**	**Complaints**	**Freedom of Information authority**
Bund	Federal Commissioner for Data Protection	Art. 21 DPL	Art. 25 DPL	X
Baden-Württemberg	Landes Commissioner for Data Protection Baden-Württemberg	Art. 27 I DPL-BW	Art. 30 DPL-BW	-
Bayern	Landes Commissioner for Data Protection Bayern	Art. 9 DPL-Bay	Art. 31 I DPL-Bay	-
Berlin	Landes Commissioner for Data Protection Berlin	Art. 27 DPL-Berlin	Art. 26 I DPL-Berlin	X
Brandenburg	Landes Commissioner for Data Protection Brandenburg	Art. 21 DPL-Bbg	Art. 25 DPL-Bbg	X
Bremen	Landes Commissioner for Data Protection Bremen	Art. 22b DPL-Bremen	Art. 29 I DPL-Bremen	X
Hamburg	Landes Commissioner for Data Protection Hamburg	Art. 26 I DPL-Hamburg	Art. 25 I DPL-Hamburg	-
Hessen	Landes Commissioner for Data Protection Hessen	Art. 28 I DPL-H	Art. 27 I DPL-H	-

[93] But the DPL-SH in Art. 5 III (data protection security measures by the government) and Art. 16 III (data transmission to foreign agencies) does prescribe a specific duty to hear the Commissioner for Data Protection in certain areas.

Mecklenburg-Vorpommern	Landes Commissioner for Data Protection Mecklenburg-Vorpommern	Art. 26 DPL-MV	Art. 32 DPL-MV	X
Niedersachsen	Landes Commissioner for Data Protection Niedersachsen	Art. 19 I DPL-N	Art. 23 I 1 DPL-N	-
Nordrhein-Westfalen	Landes Commissioner for Data Protection Nordrhein-Westfalen	Art. 25 I DPL-NRW	Art. 24 I DPL-NRW	X
Rheinland- Pfalz	Landes Commissioner for Data Protection Rheinland-Pfalz	Art. 29 I DPL-RP	Art. 25 I DPL-RP	-
Saarland	Landes Commissioner for Data Protection Saarland	Art. 23 I DPL-S	Art. 27 I DPL-S	X
Sachsen	Landes Commissioner for Data Protection Sachsen	Art. 24 I DPL-Sachsen	Art. 29 DPL-Sachsen	-
Sachsen-Anhalt	Landes Commissioner for Data Protection Sachsen-Anhalt	Art. 19 DPL-SA	Art. 24 I DPL-SA	X
Schleswig-Holstein	Landes Commissioner for Data Protection Schleswig-Holstein	Art. 40 DPL-SH	Art. 42 II DPL-SH	X
Thüringen	Landes Commissioner for Data Protection Thüringen	Art. 11 I DPL-Thüringen	Art. 39 I DPL-Thüringen	-

Annex 5 – Overview of sanctions available at the Federal ad at the Länder level (English)

Level	Data Protection (in the public sector)	Crimes	Administrative Offences
Bund	Federal Commissioner for Data Protection	Art. 44 I DPL [94] → up to two years	Art. 43 I, II DPL Art. 43 III → up to 250.000 €
Baden-Württemberg	Landes Commissioner for Data Protection Baden-Württemberg	Art. 41 DPL-BW [95] → up to two years	Art. 40 I DPL-BW [96] Art. 40 II → up to 25.000 €
Bayern	Landes Commissioner for Data Protection Bayern	Art. 37 III 1 DPL-Bay [97] → up to two years	Art. 37 I, II DPL-Bay [98] Art. 37 I, II → up to 25.000 €
Berlin	Landes Commissioner for Data Protection Berlin	Art. 32 I, II DPL-Berlin [99] → up to two years	(-) DPL-Berlin
Brandenburg	Landes Commissioner for Data Protection Brandenburg	Art. 38 III DPL-Bbg [100] → up to two years	Art. 38 I DPL-Bbg Art. 38 II → up to 50.000 €
Bremen	Landes Commissioner for Data Protection Bremen	Art. 37 DPL-Bremen → up to two years	Art. 38 I DPL-Bremen Art. 38 II → up to 25.000 €

[94] According to Art. 44 II 1 DPL it is considered an *Antragsdelikt*, meaning that criminal proceedings by the public prosecutors office are dependent on the lodging of a complaint by the victim or alternatively the initiation of the prosecution by a competent public authority; Pursuant to Art. 44 II 2 DPL the persons and bodies entitled to do so are the victim, the Federal Commissioner for Data Protection and the Supervision Authority (which has been determined by the Landes Government based upon the empowerment of Art. 38 VI DPL).

[95] Art. 41 S. 2 DPL-BW provides for the criminal liability for the attempt of violation.

[96] The Regional Administrative Bodies have been assigned as Administrative Authorities within the scope of Art. 36 I Nr. 1 OWIG.

[97] According to Art. 37 III 2 DPL-Bay it is considered an *Antragsdelikt*, meaning that criminal proceedings by the public prosecutors office are dependent on the lodging of a complaint by the victim or alternatively the initiation of the prosecution by a competent public authority; Pursuant to Art. 37 III 3 DPL-Bay the Landes Commissioner for Data Protection is entitled to do so.

[98] 50.000 DM

[99] Based upon Art. 33 II DPL-Berlin the sentence is only one year, if no intent to damage the victim or enrich oneself was given. According to Art. 32 III 1 DPL-Berlin it is considered an *Antragsdelikt*, meaning that criminal proceedings by the public prosecutors office are dependent on the lodging of a complaint by the victim or alternatively the initiation of the prosecution by a competent public authority; According to Art. 32 III DPL-Berlin the Landes Commissioner for Data Protection is entitled to do so, even contrary to the express wishes of the victim.

[100] According to Art. 38 III 2 DPL-Bbg it is considered an *Antragsdelikt*, meaning that criminal proceedings by the public prosecutors office are dependent on the lodging of a complaint by the victim or alternatively the initiation of the prosecution by a competent public authority. Pursuant to 38 III 3 DPL-Bbg the Landes Commissioner for Data Protection is entitled to do so.

Hamburg	Landes Commissioner for Data Protection Hamburg	Art. 32 I DPL-Hamburg [101] → up to two years	Art. 33 I DPL-Hamburg Art. 33 II → up to 25.000 €
Hessen	Landes Commissioner for Data Protection Hessen	Art. 40 I DPL-H [102] → up to two years	Art. 41 I DPL-H Art. 41 II → up to 25.000 € [103]
Mecklenburg-Vorpommern	Landes Commissioner for Data Protection Mecklenburg-Vorpommern	Art. 42 I,II, III DPL-MV [104] → up to two years	(-) DPL-MV
Nordrhein-Westfalen	Landes Commissioner for Data Protection Nordrhein-Westfalen	Art. 33 I DPL-NRW [105] → up to two years	Art. 34 I DPL-NRW [106] Art. 34 II → up to 50.000 €
Rheinland- Pfalz	Landes Commissioner for Data Protection Rheinland-Pfalz	Art. 37 I DPL-RP [107] → up to one year	(-) DPL-RP
Saarland	Landes Commissioner for Data Protection Saarland	Art. 35 I DPL-S [108] → up to two years	Art. 36 I DPL-S Art. 36 II → up to 50.000 €
Sachsen	Landes Commissioner for Data Protection Sachsen	Art. 39 DPL-Sachsen → up to two years	Art. 38 I DPL-Sachsen [109] Art. 38 II → up to 25.000 €
Sachsen-Anhalt	Landes Commissioner for Data Protection Sachsen-Anhalt	Art. 31 DPL-SA [110] → up to two years	Art.31a I, II DPL-SA Art. 31a III → up to 250.000 €

[101] Art. 32 II DPL-Hamburg provides for the criminal liability for the attempt of violation. Pursuant to Art. 32 III DPL-Hamburg it is considered an *Antragsdelikt*, meaning that criminal proceedings by the public prosecutors office are dependent on the lodging of a complaint by the victim or alternatively the initiation of the prosecution by a competent public authority. Art. 32 IV DPL-Hamburg is a general subsidiarity clause.

[102] Art. 40 II DPL-H is a general subsidiarity clause.

[103] 50.000 DM

[104] According to Art. 42 IV LDSG-MV it is considered an *Antragsdelikt*, meaning that criminal proceedings by the public prosecutors office are dependent on the lodging of a complaint by the victim or alternatively the initiation of the prosecution by a competent public authority; the Landes Commissioner for Data Protection is entitled to do so. Based on Art. 42 I and II the sentence is only one year, if no intent to damage the victim or enrich oneself was given.

[105] Art. 33 I DPL-NRW provides for the criminal liability for the attempt of violation..

[106] Pursuant to Art. 34 II a DPL-NRW the Local Executive have been assigned as Administrative Authorities within the scope of Art. 36 I Nr. 1 OWIG for the purposes of the DLP-NRW, while for the purposes of Art. 43 DPL it is the Landes Commissioner for Data Protection.

[107] § 37 II DPL-N provides for the criminal liability for the attempt of violation..

[108] § 35 II DPL-S is a general subsidiarity clause.

[109] Art. 38 III DPL-Sachsen assigns the Landes Commissioner for Data Protection as Administrative Authorities within the scope of Art. 36 I Nr. 1 OWIG.

[110] According to Art. 31 III DSG-SA it is a *Antragsdelikt*, except for those cases which are of public interest. Yet based on Art. 22 VIII DPL-SA the Landes Commissioner for Data Protection is entitled to lodge a complaint thus leading to the initiation of proceedings.

Schleswig-Holstein	Landes Commissioner for Data Protection Schleswig-Holstein	(**-**) DPL-SH	Art. 44 I DPL-SH Art. 44 II → up to 50.000 €
Thüringen	Landes Commissioner for Data Protection Thüringen	Art. 42 I,II,III DPL-Thüringen [111] → up to two years	(**-**) DPL-Thüringen

[111] According to Art. 42 IV DPL-Thüringen it is considered an *Antragsdelikt*, meaning that criminal proceedings by the public prosecutors office are dependent on the lodging of a complaint by the victim or alternatively the initiation of the prosecution by a competent public authority; the Landes Commissioner for Data Protection is entitled to do so. Based on Art. 42 DPL-Thüringen I and II the sentence is only one year, if no intent to damage the victim or enrich oneself was given..

Annex 6 - Overview of relevant provisions of the Länder Constitutions (English)

Level	Data Protection in the Landes Constitution	Office of the Commissioner for Data Protection in the Landes Constitution
Baden-Württemberg	**(-)**	**(-)**
Bayern	**(-)**	Art. 33a
Berlin	Art. 47	Art. 47
Brandenburg	Art. 11	Art. 74
Bremen	Art. 11	**(-)**
Hamburg	**(-)**	**(-)**
Hessen	**(-)**	**(-)**
Mecklenburg-Vorpommern	Art. 6	Art. 37
Niedersachsen	**(-)**	Art. 62
Nordrhein-Westfalen	Art. 4 para 2	Art. 77a
Rheinland- Pfalz	Art. 4a	**(-)**
Saarland	Art. 2	**(-)**
Sachsen	Art. 34	Art. 57
Sachsen-Anhalt	Art. 6	Art. 41 para 1
Schleswig-Holstein	**(-)**	**(-)**
Thüringen	Art. 6 para 2	Art. 69

http://www.verfassungen.de/de/