FRA

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

Kerstin Buchinger and
Stefanie Dörnhöfer
Vienna, Austria
March 2009

Contents

Executive summary

Overview

[1]. Data protection in Austria is primarily based on the *Datenschutzgesetz 2000* (DSG 2000) [Data Protection Act 2000 (DPA 2000)].[1] Data protection jurisdiction is incumbent on the *Datenschutzkommission* (DSK) [Data Protection Commission (DPC)] and the civil courts.

Data Protection Authority

[2]. The Austrian Data Protection Commission is set up within the administrative framework of the Federal Chancellery, which raises serious doubts concerning its independence. Its duties and responsibilities cover the operation of the *Datenverarbeitungsregister* [Data Processing Register], the handling of individual complaints and various examination competencies. In addition, the Commission is partly engaged in awareness raising and counselling activities and takes part in international data protection processes.

Compliance

[3]. In Austria, registration is mandatory for most data applications and requires overriding legitimate interests of the controller. Prior checking is applied in specific cases, e.g. if sensitive data is concerned. The DPC may, in cases of imminent danger, temporarily prohibit the continuation of a data application by verdict. Although problems with compliance cannot be easily identified, large deficits concerning the registration of video surveillance measures exist. Due to the fact that the establishment of data protection agents within private organisations is not mandatory. Therefore, their role in raising awareness about the importance of compliance is rather limited.

[1] Austria/BGBl I 165/1999 (17.08.1999).

Sanctions, Compensation and Legal Consequences

[4]. While the DPC's tasks are limited to declaratory decisions in many cases, civil courts can in principle apply injunction judgements and award compensation if violations of DPA 2000 provisions have been found. However, compensation payments for infringements of the right to data protection have so far not been common.

Rights Awareness

[5]. Rights awareness concerning data protection and infringements of data protection rights is not an issue of major concern among Austrian citizens. This applies especially to video surveillance measures. The level of knowledge about data protection, risks of data abuse and the legal conditions in question is very low. Awareness raising activities are conducted mainly by NGOs, since the DPC is not provided with sufficient human resources to undertake such activities.

Analysis of deficiencies

[6]. The DPC is severely understaffed and therefore faces difficulties in performing the tasks designated to it. This is mainly relevant for examinations on its own initiative. Furthermore, the Commission's decision-making powers are in a large number of cases limited to declaratory decisions, creating deficiencies in effective data protection. 'Only indirectly personal' data (data that does not allow for establishing the identity of the data subject[2] by legal means) is *de facto* excluded from the regime of the DPA 2000.

Good Practice

[7]. In the course of the research activities undertaken, no specific good practice was discovered.

[2] The term 'data subject' refers to Art. 2 of Directive 95/46/EC and comprises identified or identifiable natural persons; in Austria, the term also covers legal persons.

Miscellaneous

[8]. Besides the DPC, data protection institutions to be mentioned are the *Datenschutzrat* [Data Protection Council] and the *Rechtsschutzbeauftragte* [Commissioners for Legal Protection].

1. Overview

1.1. International standards relevant for data protection in Austria

1.1.1. Standards under EU Law

[9]. The fundamental rights standards concerning data protection at the EU level, and thus relevant for Austria, are:

- Article 8 of the EU Charter of Fundamental Rights;
- Directive 95/46/EC of 24 October 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995, p. 31;
- Directive 2002/58/EC of 12 July 2002 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. (Directive on privacy and electronic communications), OJ L 201 of 31.07.2002, p. 37;
- Regulation 45/2001/EC of 18 December 2000 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data Official, OJ L 8 of 12.1.2001 and
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

1.1.2. Standards developed by the Council of Europe

[10]. Under the Council of Europe, the following instruments have been developed in order to protect personal privacy and private life:

- Article 8 of the European Convention on Human Rights (ECHR), including the case law of the European Court on Human Rights, on the protection of privacy and private life;
- the Basic Principles contained in the Appendix to the Recommendation Rec (87)15 addressed by the Committee of Ministers to the Member States of the Council of Europe, regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987, at 401st meeting of the Ministers' Deputies;
- the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981);
- the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow (2001) and
- the Convention on Human Rights and Biomedicine (1997), especially its Article 10 on 'Private life and right to information'.

1.1.3. Standards at the level of the United Nations

[11]. Within the United Nations, at least two important standards have to be mentioned:

- Article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1966) and General Comment No. 16 on Article 17 ICCPR (especially its paragraph 10 on personal data) and
- The Guidelines for the Regulation of Computerized Personal Data Files adopted by a resolution of the General Assembly of the United Nations on 14 December 1990.

1.2. Austrian constitutional standards relevant for data protection

1.2.1. Article 8 of the European Convention on Human Rights (ECHR)

[12]. In 1964, an amendment to the Austrian Constitution clarified the status of the ECHR as being fully equivalent to its original catalogue of fundamental rights, i.e. the *Staatsgrundgesetz 1867* [Basic Law of

1867].[3] Since then, the ECHR has had the rank of directly applicable federal constitutional law and any offences under the Convention can be claimed as violations of constitutionally guaranteed rights. As a result, all legislative, executive and judicial authorities are obliged to observe and implement the Convention within their sphere of action. Thus, the Austrian legislator has to respect the ECHR guarantees when enacting laws and all courts and administrative authorities have to apply and interpret the domestic legal provisions in line with the Convention.

[13]. Consequently, Art. 8 ECHR clearly serves as the constitutional basis in Austria when it comes to the protection of privacy and private life.

1.2.2. Section 1 of the Austrian Data Protection Act 2000 (DPA 2000)

[14]. Prior to the implementation of Directive 95/46/EC, the *Datenschutzgesetz* (DSG) [Data Protection Act (DPA)][4] dated from 1978. The *Datenschutzgesetz 2000* (DSG 2000) [Data Protection Act 2000 (DPA 2000)],[5] which was then passed in 1999 in order to ensure that Austria complied with the Directive, is the new foundation of data protection law in Austria. It has been in force since 1 January 2000.

[15]. Besides Art. 8 ECHR, the constitutional provision in its Section 1 stipulates a fundamental right to data protection within the framework of a sub-constitutional law, stating that everybody shall have the right to secrecy for the personal data concerning him/her, especially with regard to his/her private and family life, insofar as he/she has an interest deserving such protection. Such an interest is, however, not given when data is generally available or cannot be traced back to the data subject.

[16]. Insofar as personal data is not used in the vital interest of the data subject or with his/her consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of others. In case of an intervention by a public authority the restriction shall only be permitted based on laws necessary for the reasons stated in Art. 8 para. 2 ECHR.

---

3 Austria/RBl 142/1867 (22.12.1867).
4 Austria/BGBl I 565/1978 (28.11.1978).
5 Austria/BGBl I 165/1999 (17.08.1999); the unofficial translation of the DPA 2000, upon which this study is based, is available via the DPC's website under: http://www.dsk.gv.at/site/6230/default.aspx (28.01.2009).

[17]. Such laws may provide for the use of data that deserve special protection only in order to safeguard substantial public interests and shall provide suitable safeguards for the protection of the data subjects' interest in secrecy. Even in case of permitted restrictions, the intervention with fundamental right is to be carried out using only the least intrusive of all effective methods.

[18]. Everybody has, insofar as personal data concerning him/her are destined for automated processing or manual processing, i.e. in filing systems without automated processing, as provided for by law, 1. the right to obtain information as to who processes what data concerning him/her, where the data originated, for which purpose they are used, as well as to whom the data are transmitted and 2. the right to rectification of incorrect data and the right to erasure of illegally processed data.

[19]. Restrictions of the rights according to para. 3 are only permitted under the conditions laid out in para. 2. The fundamental right to data protection, except the right to information, shall be asserted before the civil courts against organisations that are established according to private law, as long as they do not act in execution of laws. In all other cases the *Datenschutzkommission* (DSK) [Data Protection Commission (DPC)] shall be competent to render the decision, unless an act of Parliament or a judicial decision is concerned.

[20]. The major part of the DPA 2000 bases upon sub-constitutional level and implements the details of the aforementioned data protection rights. In addition, the *Telekommunikationsgesetz* [Telecommunication Act][6] sets detailed standards on the use of data by private stakeholders, namely telecommunication and information services.

1.3. Relevant authorities and institutions regarding data protection

1.3.1. Data Protection Commission and Council

[21]. The Data Protection Commission's role is to safeguard data protection in accordance with the regulations of the DPA 2000. The Austrian Data Protection Council shares this role according to Section 35, para. 1 DPA 2000. For more details on both institutions, see chapters 2 and chapter 8, para. 1.

[6] Austria/BGBl I 70/2003, last amended by Austria/BGBl I 133/2005 (18.11.2005).

1.3.2. NGOs active in the field of data protection

[22]. The most relevant NGO in Austria in the field of data protection is the *Österreichische Gesellschaft für Datenschutz* (ARGE DATEN) [Austrian Association for Data Protection], which examines the interaction between the usage of computer science, information law and society since 1983. It is a non-profit, non-governmental organisation which finances itself through promotions, sponsoring, donations, membership fees and by individual projects on issues of data protection.

[23]. The association's main activities cluster around public relations and information services (website, newsletter, press and media interviews, and support in privacy issues).

2. Data Protection Authority

2.1. Type, Structure and Legal Basis

[24]. The Austrian Data Protection Commission, originally established in 1980 under the then *Datenschutzgesetz* (DSG) [Data Protection Act (DPA)],[7] is a governmental authority charged with data protection and at the same time the Austrian supervisory authority for data protection, equivalent to a national data protection commissioner. In 1999, the transposition of the Data Protection Directive 95/46/EC led to a new Austrian Data Protection Act, the *Datenschutzgesetz 2000* (DSG 2000) [Data Protection Act 2000 (DPA 2000)][8] and effected certain improvements in the formulation and mandate of the Commission.

2.2. Resources

[25]. The Commission is set up within the administrative framework of the Federal Chancellery, Section V - Constitutional Service. It is composed of six members/substitutes (including a chairperson and an executive member) appointed by the Federal President on a proposal of the Federal Government for a term of five years (re-appointments are permitted). All members/substitutes have legal expertise and one of the members is a judge.[9] Members of the Federal Government or of a State Government, Secretaries of State or persons who may not be elected for the National Council cannot be members/substitutes of the DPC.

[26]. According to Sec. 37 para. 1 DPA 2000 (constitutional provision), the members of the DPC are independent in the discharge of their functions and not bound by any instructions.

[27]. Pursuant to Sec. 38 para. 2 DPA 2000, the Federal Chancellor has to install a branch office and supply the necessary personnel and equipment to support the operation of the DPC. In line with the independence of the DPC, the officials working in the Commission's branch office are only bound by instructions of the chairperson and the executive member of the DPC with regard to their professional

7 Austria/BGBl I 565/1978 (28.11.1978).
8 Austria/BGBl I 165/1999 (17.08.1999).
9 Cf. Sec. 36 para. 1 DPA 2000.

work.[10] Apart from the officials working in the Data Processing Register (11.65 established posts), 8.5 posts have been established for the branch office itself. Consequently, the office of the DPC disposes of a total of 20 established posts.

[28]. The Commission does not have a budget at its own disposal, but is dependent on the budget allocated by the Federal Chancellor. Apart from figures concerning human resources, no official information on the Commission's budget is available. Since the DPC is incorporated in the structure of the Federal Chancellery, the concrete allocation of budget is subject to internal procedures.

[29]. As far as the resources of the DPC, especially regarding personnel, are concerned, the comparison with other European countries clearly shows that Austria is ranking at the bottom of the European scale, leaving only Italy, Romania, France and Portugal below it.[11] In Belgium, e.g., where the population is quite similar to Austria, the data protection authority has more than 37 officials at its disposal; Bulgaria and Sweden record 40 established posts; in the Czech Republic, even 85 officials work for the local data protection authority. Recent developments at the international level and the subsequently increasing scope of functions in the area of data protection make it necessary to increase the headcount of data protection authorities to European standards.

[30]. With regard to the guarantees of independence, it can be said that although the DPC is not bound by any instructions in the exercise of its functions, the legal provisions governing the nomination procedure leave ample room for the Federal Government to influence the composition of the Commission. Due to its structure and organisation, the DPC does not fulfil the standards set up by Directive 95/46/EC relating to independence, which is currently subject to infringement procedures against Austria. The incorporation of the DPC in the Federal Chancellery and the status of its members is incompatible with Art. 22 of Directive 95/46/EC. Furthermore, a lack of budgetary control and the appointment of DPC staff for limited time periods only, as well as the appointment of representatives of interest groups, raise severe doubts about the DPC's actual independence.

[10] Cf. Sec. 37 para. 2 DPA 2000.
[11] Cf. Datenschutzbericht 2007, pp. 12-13, available under: http://www.dsk.gv.at/DocView.axd?CobId=30637 (06.01.2009).

2.3. Main Powers and Procedures

[31]. The duties and responsibilities of the DPC in the area of data protection are manifold and comprehensive. Its role is to safeguard data protection in accordance with the regulations of the DPA 2000.

2.3.1. Operation of the Data Processing Register

[32]. A register for data applications, the so-called *Datenverarbeitungsregister* [Data Processing Register], is established under the DPC for the purpose of examining the legality of such applications and in order to allocate information to the data subjects (for further details see chapter 3.1. below).[12]

[33]. For the purpose of this study, the term 'controller' refers to natural or legal persons processing data for a specific purpose. The term 'processor' covers natural or legal persons who process data that were given to them for a commissioned work.[13]

2.3.2. Duties of Supervision – Ombudsperson-Procedure

[34]. Besides the formal complaints procedure under Sec. 31 DPA 2000 (see below under 2.3.3.), anyone has the right to lodge an (informal) application with the DPC because of an alleged infringement of his/her rights under the DPA 2000 by a controller or processor.[14] In cases of reasonable suspicion of an infringement, the DPC has the right to examine data applications. It can order the controller or processor of the examined data application to give all necessary clarifications and to grant access to data applications and other relevant documents.[15] The supervisory rights of the DPC are to be exercised in a way that least interferes with the rights of the controller or processor.[16]

[35]. Data applications subject to *Vorabkontrolle* [prior checking][17] may be examined by the DPC without a suspicion of illegal data use. The same applies to those fields of administration where a public sector controller claims that Sec. 26 para. 5 (cases where public interests require that no information is given to the data subject) and 27 para. 5

[12] Cf. Sec. 16 para. 1 DPA 2000.
[13] The definitions used were taken out of Sec. 4 DPA 2000.
[14] Cf. Sec. 30 para. 1 DPA 2000.
[15] Cf. Sec. 30 para. 2 DPA 2000.
[16] Cf. Sec. 30 para. 4 DPA 2000.
[17] Cf. Sec. 18 para. 2 DPA 2000.

(cases where public interest require that no rectification or erasure is effected) DPA 2000 are to be applied.

[36]. For inspection purposes the DPC has the right to enter rooms or premises where data applications are carried out, operate data processing equipment and make copies of the storage media to the extent absolutely required for the exercise of the right to examination. Prior to these supervisory measures, the DPC has to duly inform the owner of the mentioned rooms or premises as well as the controller/processor. The supervisory rights are to be exercised in a way that least interferes with the rights of the controller/processor. The controller/processor has to render the assistance necessary for the examination.

[37]. The information gathered by the DPC during such examinations may be used only for supervisory purposes in the context of the execution of data protection regulations. To establish the rightful state, the DPC can issue recommendations which, however, are not legally binding.[18]

[38]. When analysing the duties of supervision of the Commission in practice and against the background of its rather limited resources, it has to be mentioned that although the powers of the DPC to act on its own initiative are provided for by law (cf. Sec. 30 paras. 2 and 3 DPA 2000), they are ineffective, because due to lacking resources the DPC hardly ever makes use of them. This situation is also severely criticised by the DPC itself in its annual reports.[19]

2.3.3. Individual Complaint Procedure

[39]. In a formal procedure according to Sec. 31 para. 1 DPA 2000 the DPC decides upon request of the data subject on alleged infringements of the right to information[20] by the controller of a data application. This applies only, if the request for information does not concern the usage of data for acts of legislation or jurisdiction. Pursuant to Sec. 31 para. 2 DPA 2000, the DPC is competent to decide on an alleged infringement of the data subject's right to rectification and erasure[21] if the data subject filed a complaint against a public sector controller that is not an organ of legislation or jurisdiction. In cases of imminent danger, the DPC according to Sec. 31 para 3 DPA 2000 can (when dealing with a complaint pursuant to Sec. 31 para. 2) prohibit all further uses of data entirely or in part or can order the controller to

[18] Cf. Sec. 30 para. 6 DPA 2000.
[19] Cf. Datenschutzbericht 2007, p. 25, available at: http://www.dsk.gv.at/DocView.axd?CobId=30637 (10.03.2009).
[20] Cf. Sec. 26 DPA 2000.
[21] Cf. Sec. 1 para. 3 sub-para. 2 DPA 2000.

issue a so-called *Bestreitungsvermerk* [an entry about the dispute]. If the DPC e.g. comes to the conclusion that it was not justified to keep the processed data secret from the data subject, the disclosure of data is ordered by a ruling.[22]

2.3.4. Authorisations in cases of transborder transmission and committing of data

[40]. Insofar as a case of transborder data exchange is not exempted from authorisation according to Sec. 12 DPA 2000, the controller has to apply for a permit by the DPC before the act of transmission or *Überlassen von Daten* [committing of data].[23] The DPC may tie its authorisation on certain conditions and obligations.[24]

[41]. Pursuant to Sec. 13 para. 2 DPA 2000, an authorisation shall be given if the requirements of Sec. 12 para. 5 are met and, despite the lack of an adequate general level of data protection in the recipient state, either an adequate level of data protection exists for the transmission or committing outlined in the application for the permit in the specific case[25] or the controller can satisfactorily demonstrate that the data subject's interests in secrecy deserving protection concerning the planned data exchange will be respected outside of Austria.

[42]. Sec. 13 para. 1 DPA 2000 provides that a domestic processor may also apply for an authorisation if, in order to fulfil his/her contractual obligations vis-à-vis multiple controllers, he/she wishes to enlist the service of a specific processor outside Austria.

2.3.5. Other responsibilities at the European level

[43]. At the European level, the executive member of the Austrian DPC is a member of the Art. 29 Data Protection Working Party established under the Data Protection Directive 95/46/EC.

[44]. Moreover, members of the DPC are appointed as Austrian representatives to the joint supervisory data-protection bodies (the Joint Supervisory Authority of Schengen and the Europol Joint Supervisory Body).

---

22 Cf. Sec. 31 para. 4 DPA 2000.
23 Committing of data means the transfer of data from a controller to a processor.
24 Cf. Sec. 13 para. 1 DPA 2000.
25 This is then to be judged considering all circumstances relevant to the use of data.

[45]. Besides, the Austrian DPC is also member of the 'Policy Working Party', a sub-group of the spring conference of the European Data Protection Authorities, established to deal with the most important questions on data protection in relation to the third pillar of the EU.

2.3.6. Monitoring Role

[46]. The DPC's monitoring role is limited to the competences described under chapter 2.3.2. above.[26] However, due to lack of human and financial resources the DPC is unable to fulfil its monitoring role in practice.[27]

2.3.7. Limitations

[47]. In principle, the powers given to the Austrian DPC (which have been described above in detail) correspond to the minimum requirements set out in Art. 28 of Directive 95/46/EC. The Commission has investigative powers, powers of intervention as well as the power to engage in legal proceedings. However, and as stated in several other parts of this study, the Commission does not have the necessary resources to fulfil each of its powers in a sufficient way.

[48]. According to the *Datenschutzbericht 2007* [Data Protection Report 2007],[28] the DPC is able to tolerably cope with the complaints procedures it is engaged with as well as with cases in which it is giving legal advice to citizens.[29]

[49]. As far as the Commission's engagement in the Art. 29 Data Protection Working Party is concerned, the post established for this purpose was repealed from 1 July 2006, so that at the moment no officer in the DPC's branch office is concerned with this field of action.[30]

[50]. Moreover, the DPC's duties of supervision according to Sec. 30 paras. 2 and 3 DPA 2000 cannot be realised adequately. This is extremely dissatisfying for the DPC and its officials because the standards within

[26] Cf. Sec. 30 paras. 2 and 3 DPA 2000.
[27] Cf. Datenschutzbericht 2007, p. 25, available at: http://www.dsk.gv.at/DocView.axd?CobId=30637 (11.01.2009).
[28] Cf. Datenschutzbericht 2007, pp. 24-26, available at: http://www.dsk.gv.at/DocView.axd?CobId=30637 (11.01.2009).
[29] In most cases, the period of transaction did not exceed the limit of six months; cf. Datenschutzbericht 2007, p. 24, available under: http://www.dsk.gv.at/DocView.axd?CobId=30637 (11.01.2009).
[30] Cf. ibid., p. 25.

the European Economic Area clearly show that this kind of power is of immense significance.

[51]. The Commission's participation in the process of appraisal of draft legislation is not explicitly foreseen in the DPA 2000, although it must be heard every time before an ordinance based on the DPA 2000 or otherwise directly concerning important issues of data protection is enacted according to Sec. 38 para. 3 DPA 2000. Thus, the DPC is not regularly or formally consulted. However, the DPC has so far commented on amendments to various draft laws and/or regulations tackling issues of data protection, even in situations where it was not asked to do so by the competent ministries. The hearing of national data protection control units in cases of legislative intentions touching upon issues of data protection is a self-evident fact in most of the Member States of the EU; consequently, it seems to be absolutely necessary to establish a formal consultation process also for the Austrian DPC.[31]

[52]. As regards the cooperation of the DPC with civil society and its engagement in awareness raising, no formal procedure is foreseen. Also, the scarce human resources in the DPC's branch office limit the Commission's efforts in public relations to a minimum. However, and despite its limited resources, the DPC has in recent years initiated attempts to attract public interest in the importance of data protection. For example, on the occasion of the European Data Protection Day on 28 January 2007, the DPC published a brochure on data protection in order to raise awareness on data protection issues and to inform citizens of their rights and of good practices, thereby enabling and encouraging them to exercise these rights more effectively.

2.4. Decisions and Opinions of the DPC

[53]. Selected decisions of the DPC from the year 2000 onwards are readily available to the public via the Commission's website,[32] which is directly linked to the *Rechtsinformationssystem des Bundes* (RIS) [Legal Information System of the Republic of Austria], a computer-assisted information system on Austrian law, which is coordinated and operated by the Federal Chancellery.[33] Taking effect as of 22 July 2008, 800 decisions of the DPC are contained in this information

[31] Cf. Datenschutzbericht 2007, pp. 25-26, available under: http://www.dsk.gv.at/DocView.axd?CobId=30637 (06.01.2009).
[32] Cf. http://www.dsk.gv.at/site/6186/default.aspx (06.01.2009).
[33] Cf. http://www.ris2.bka.gv.at/Dsk/ (11.01.2009).

system, out of which 573 are available in full-text version.[34] The DPC's opinions can be accessed via the Commission's website too.[35]

2.5. The DPC's exposure to Opinions of the Working Party established under Art. 29 of Directive 95/46/EC

[54]. The extent to which the opinions of the Working Party established under Art. 29 of the Directive 95/46/EC represent a source of inspiration for the interpretation of the national legislation implementing EU legislation on data protection by the DPC is hard to identify due to lack of official information on this matter.

[55]. At any rate, the Working Party's opinions are definitely considered binding by the Commission. As mentioned above, the executive member of the Austrian DPC is also a member of the Art. 29 Working Party, fulfilling her tasks responsibly and with great effort. A separate chapter of each of the DPC's biannual reports is dedicated to the cooperation in the framework of the Art. 29 Working Party, making special reference to the main topics that were dealt with.[36] Moreover, detailed reference is made to the Working Party on the DPC's website.[37]

[34] Cf. http://www.dsk.gv.at/site/6186/default.aspx (06.01.2009).
[35] Cf. http://www.dsk.gv.at/site/6187/default.aspx (06.01.2009).
[36] Cf. e. g. Datenschutzbericht 2007, pp. 49-53, available under: http://www.dsk.gv.at/DocView.axd?CobId=30637 (06.01.2009).
[37] Cf. http://www.dsk.gv.at/site/6194/default.aspx (06.01.2009).

3. Compliance

3.1. The duties of registration and their level of compliance

[56]. A register for data applications, the so-called *Datenverarbeitungsregister* [Data Processing Register], is established under the DPC for the purpose of examining the legality of such applications and in order to allocate information to the data subjects.[38] The register may be inspected by any person. Access to the registration file including the licences contained in the file is granted if the person applying for inspection can satisfactorily demonstrate that he/she is a data subject and as far as no overriding interests in secrecy on part of the controller deserving protection are an obstacle to access.[39]

[57]. More specific regulations about the management of the register were laid down through an ordinance by the Federal Chancellor.[40] This was done taking into account the correctness and completeness of the register, the clarity and expressiveness of the entries and the ease of access. A possibility to notify (Sec. 17 and 19 DPA 2000) by means of automated processing was also provided for.[41]

[58]. According to Sec. 17 para. 1 DPA 2000, before commencing a data application, every controller has to (unless provided otherwise) file a notification with the DPC for the purpose of registration in the Data Processing Register. The contents of this notification are specified in Sec. 19 DPA 2000 (see below). The duty to notify also applies to all circumstances that afterwards lead to the incorrectness or incompleteness of a notification.

[59]. Sec. 18 para. 1 DPA 2000 provides that a data application which requires formal notification may in general be fully operated immediately after the notification has been submitted to the Data Processing Register.

---

38 Cf. Sec. 16 para. 1 DPA 2000.
39 Cf. Sec. 16 para. 2 DPA 2000.
40 Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2002 – DVRV 2002), Austria/BGBl II 24/2002 (18.01.2002).
41 Cf. Sec. 16 para. 3 DPA 2000.

[60]. Data applications subject to notification that neither correspond to a *Musteranwendung* [Model Application] pursuant to Sec. 19 para. 2 DPA 2000 nor concern the internal affairs of churches or religious communities recognised by the state, and that involve sensitive data or data about certain criminal offences or whose purpose is to give information on the data subjects' creditworthiness or that are carried out in the form of an *Informationsverbundsystem* [joint information system] can only be initiated after an examination (prior checking) by the DPC.[42]

[61]. Pursuant to Sec. 19 para. 1 DPA 2000, a notification must contain the name (or other destination) and address of the controller and of his/her representative, the registration number of the controller, the proof of statutory competence or of the legitimate authority that the controller's activities are permitted (if so required), the purpose of the data application to be registered and its legal basis, the categories of data subjects and the categories of data that are processed, (insofar an authorisation by the Commission is required) the file number of the DPC's authorisation as well as a general description of the data security measures taken pursuant to Sec. 14 DPA 2000, which enable a preliminary assessment of the appropriateness of the security measures.

[62]. A notification is insufficient if information is missing, obviously incorrect, inconsistent or so insufficient that persons accessing the register to safeguard their rights according to the DPA 2000 cannot obtain sufficient information as to the issue whether their interests in secrecy deserving protection could be infringed by the data application.[43]

[63]. According to Sec. 20 para. 1 DPA 2000, the Commission shall examine all notifications within two months. If it comes to the conclusion that the notification is insufficient in terms of Sec. 19 para. 3 DPA 2000 (e.g. if information is missing, obviously incorrect, inconsistent or so insufficient that persons accessing the register to safeguard their rights cannot obtain sufficient information as to the issue whether their interest in secrecy deserving protection could be infringed by the data application), the controller is ordered to correct the insufficiency within a set period of time within two months after receipt of the notification.

[64]. In case of imminent danger due to a serious infringement of the data subject's interest in secrecy deserving protection, the DPC shall

[42] Cf. Sec. 18 para. 2 DPA 2000.
[43] Cf. Sec. 19 para. 3 DPA 2000.

temporarily prohibit the continuation of the notified data application by verdict.[44]

[65]. For data applications subject to prior checking pursuant to Sec. 18 para. 2 DPA 2000, a decision must be rendered in conjunction with the order for correction stating whether processing may be commenced or whether it is not permitted for lack of proof of sufficient legal basis.[45]

[66]. If the order for correction is not complied with in a timely manner, the DPC shall, by ruling, refuse registration; otherwise, the notification is regarded as if it had been correct form the beginning.[46] If no order for correction is made within two months after notification, the obligation to notify is considered to be fulfilled. Data applications subject to prior checking may be commenced.[47]

[67]. Notifications pursuant to Sec. 19 DPA 2000 have to be entered into the Data Processing Register if 1. the verification procedure has shown that a registration is permitted or 2. two months have passed since the notification was submitted to the Commission or 3. the controller has made the corrections which were ordered in time.[48] For data applications subject to prior checking pursuant to Sec. 18 para. 2 DPA 2000, the execution of the data application may be permitted subject to conditions based on the findings of the checking procedure, insofar as this is necessary to safeguard interests of the data subject that are protected by the DPA 2000.[49] Afterwards, the sufficient registration shall be communicated to the controller in writing in the form of a *Registerauszug* [register statement].[50] Deletions and amendments to the register are carried out upon application of the registree or *ex officio*.[51]

[68]. In general, the level of compliance with regard to notifications cannot be assessed on the basis of available official data. Concerning video surveillance, the situation relating to compliance is highly unsatisfactory (see chapter 6 for more details).

44 Cf. Sec. 20 para. 2 DPA 2000.
45 Cf. Sec. 20 para. 3 DPA 2000.
46 Cf. Sec. 20 para. 4 DPA 2000.
47 Cf. Sec. 20 para. 5 DPA 2000.
48 Cf. Sec. 21 para. 1 DPA 2000.
49 Cf. Sec. 21 para. 2 DPA 2000.
50 Cf. Sec. 21 para. 3 DPA 2000.
51 Cf. Sec. 22 para. 1 DPA 2000.

3.2. Data protection agents within public or private organisations

[69]. The Austrian DPA 2000 does not provide for any obligation to nominate data protection agents within public or private organisations.

[70]. However, Sec. 6 para. 4 DPA 2000 stipulates that in order to determine more closely which use of data can be regarded as fair and lawful in a specific field, special interest groups established by law, other professional associations and comparable bodies may draw up codes of conduct for the private sector.

[71]. As far as public services are concerned, the *Gewerkschaft Öffentlicher Dienst* [Union of Public Services] demands the installation of data protection agents and tries to promote this issue among the relevant stakeholders and decision making bodies.[52]

[72]. With regard to the private sector, an amendment to the DPA 2000 was opened for public comment on 11 April 2008.[53] Among other issues, it contains a new provision (Sec. 15 lit. a) regarding *betriebliche Datenschutzbeauftragte* [internal data protection agents] in private organisations. According to this provision, each owner of a business or company employing more than 20 employees in the future shall have to appoint one of his/her (appropriate) staff members as an internal data protection agent. If the owner does not have an appropriate candidate among his/her employees, an external person will have to be appointed. It shall be the duty of the internal data protection agent to monitor intra-company compliance with provisions of the DPA 2000 and he/she shall have to advise the owner, the employees and the workers' council in matters of data protection. In cases where the internal agent becomes suspicious of a potential infringement of any data protection provision, he/she (eventually in cooperation with the owner) shall have to work towards a lawful status. In the exercise of his/her functions, the internal agent shall not be bound by any instructions. The appointment of an internal data protection agent in any case shall not affect the owner's liability for compliance with the provisions of data protection set out in the DPA 2000.

[52] Cf. Leitantrag Datenschutz, Gewerkschaft Öffentlicher Dienst, available under: www.goed-ooe.at/files/2007/2/26/leitantr.pdf (10.03.2009).

[53] Cf. Datenschutzgesetz-Novelle 2008, documents available under: http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00182/pmh.shtml (11.01.2009); the amendment has not passed the National Council yet due to the snap election process in Austria in autumn 2008.

[73]. However, as this provision is only at the stage of parliamentary discussions, the influence of internal data protection agents or their role in raising awareness regarding the importance of data protection and regarding compliance with relevant norms and procedures is rather limited.

3.3. Other evidence of compliance/non-compliance

[74]. Regarding any other evidence indicating compliance or lack of compliance with data protection legislation in practice, please refer to chapter 6 below.

4. Sanctions, Compensation and Legal Consequences

4.1. Complaints before the DPC

[75]. According to Sec. 41 DPA 2000, the Commission has the general power to make rulings on matters of data protection.

[76]. If the Commission issues recommendations to a data controller and he or she fails to comply, it can

a. initiate an administrative inquiry to check the registration,

b. bring a criminal charge with the authorisation of the injured party or

c. in case of a transgression by a state body, the competent highest authority can take measures to ensure that the recommendation of the Commission is complied with, or inform the Commission why the recommendation has not been complied with.[54]

[77]. In cases where there is probable cause to believe that a serious data protection infringement has been committed by a private sector controller, the DPC must – according to Sec. 32 para. 5 DPA 2000 – file an action for a *Feststellungsklage* [declaratory judgement] with the court that is competent pursuant to Sec. 32 para. 4 second sentence DPA 2000.

4.2. Court action

[78]. Claims of data subjects against private sector controllers for infringements of the right to secrecy, rectification or erasure have to be brought before the civil courts.[55]

[79]. If data have been used contrary to the provisions of the DPA 2000, the data subject has the right to sue for an end to such unlawful state.[56] In order to safeguard the legal right to put an end to such an unlawful

[54] Cf. Sec. 30 para. 6 DPA 2000.
[55] Cf. Sec. 32 para. 1 DPA 2000.
[56] Cf. Sec. 32 para. 2 DPA 2000.

state an injunction may be issued.[57] Complaints and applications for injunctions pursuant to the DPA 2000 shall in the first instance be lodged with the regional civil court in whose district the data subject has his or her domicile or seat. The data subject may bring an action before the regional civil court in whose district the controller or processor has his/her domicile or seat.[58]

[80]. Pursuant to Sec. 33 para. 1 DPA 2000, a controller or processor who has culpably used data contrary to the provisions of the DPA 2000 shall indemnify the data subject pursuant to the general provisions of Austrian civil law. The controller or processor shall also be liable for damage caused by their staff insofar as their action was causal for the damage.[59] On the other hand, the controller shall be free from liability if he/she can prove that the circumstances which caused the damage cannot be attributed to him/her or his/her staff. This also applies to the exclusion of the processor's liability.

[81]. The use of personal data that have been entrusted to or made accessible to someone out of professional reasons, or that have been acquired illegally is sanctioned with imprisonment up to one year, if the data is used for the offender's own interest or made available to others or published with the intention to make a profit or to harm others.[60]

4.3. Administrative Procedures before the District Administrative Authorities

[82]. Insofar as a violation does not fulfil the legal elements of a criminal offence subject to the jurisdiction of courts, certain administrative penalties may be imposed according to Sec. 52 DPA 2000. For such decisions, the *Bezirksverwaltungsbehörden* [District Administrative Authorities] at the controllers' or processors' domicile or seat shall be the competent authorities. Within these procedures, penalties may be applied for intentional as well as for negligent actions and can amount up to € 18.890 (intent)[61] and € 9.445 (negligence).[62]

[57] Cf. Sec. 32 para. 3 DPA 2000.
[58] Cf. Sec. 32 para. 4 DPA 2000.
[59] Cf. Sec. 33 para. 2 DPA 2000.
[60] Cf. Sec. 51 DPA 2000.
[61] Cf. Sec. 52 para. 1 DPA 2000.
[62] Cf. Sec. 52 para. 2 DPA 2000.

4.4. Analysis

[83]. Although legal consequences responding to data protection infringements are codified in the DPA 2000 and other national acts like e.g. the *Sicherheitspolizeigesetz* (SPG) [Security Police Act (SPA)][63] and the *Strafprozessordnung* (StPO) [Code of Criminal Procedure (CCP)],[64] the law enforcement practice in Austria in the field of data protection is quite unincisive. So far, no official data on case law has been published in the Legal Information System of the Republic of Austria.

[84]. As stated above under chapter 4.1., the DPC's own competencies concerning this matter are rather limited.

[85]. Moreover, and according to the available information, no compensation payments in matters of data protection have been awarded by the Austrian civil courts so far. This may have several reasons, which are more or less related to each other: it may e.g. have to do with the more than limited resources of the DPC together with its inexistent competence to issue legally binding and enforceable decisions. For a more detailed analysis of these deficiencies see chapter 6 below.

[86]. Another reason might be that data subjects in general are not sufficiently informed about their rights and options (especially with regard to bringing cases of infringements of data protection before courts). In addition, the legal assistance and representation in data protection cases is not institutionalised in Austria. There are no publicly funded NGOs or other organisations performing this function. Despite certain limited cases where legal aid is granted, the financial risk of legal procedures (court fees, fees of attorneys etc.) has to be carried by the data subject himself/herself.

4.5. Data collection and processing in the context of employment

[87]. Concerning the protection of personal data in the context of employment, the main legal source is the DPA 2000. Even though it does not contain specific provisions regarding relations between employees and employers as such, it is of major importance therefor,

63 Austria/BGBl 566/1991, last amended by Austria/BGBl. I 2/2008 (01.01.2008).
64 Austria/BGBl I 631/1975 (30.12.1975), last amended by Austria/BGBl I 109/2007 (28.12.2007).

especially with regard to the duties and obligations imposed on processors and controllers of personal data.

[88]. In addition to that, the implementation of controlling measures and technical systems to control employees requires the consent of the *Betriebsrat* [workers' council] if the measures or systems interfere with human dignity.[65]

[89]. Moreover, the implementation of systems for the collection, processing and transmission of personal data of employees, which go beyond general information on the person and his/her qualifications, again requires the workers' council's consent insofar as the use of data exceeds the fulfilment of obligations provided by law or collective or individual contract.[66] This also applies for the implementation of systems for the assessment of employees, insofar as this leads to the collection of data that is not justified by internal use.[67]

[65] Cf. Sec. 96 para. 1 sub-para. 3 Arbeitsverfassungsgesetz (ArbVG) [Labour Relations Act], Austria/BGBl I 22/1974 (14.12.1973), last amended by Austria/BGBl I 77/2007 (13.11.2007).
[66] Cf. Sec. 96 lit. a para. 1 sub-para. 1 Labour Relations Act.
[67] Cf. Sec. 96 lit. a para. 1 sub-para. 2 Labour Relations Act.

5. Rights Awareness

[90]. On 15 July 2008, a survey on the confidence of the Austrian population in data protection was launched by the market research institution OEKONSULT.[68] According to this survey (based on a sample of 1,213 Austrian inhabitants from the age of 16 and up), issues like data protection or surveillance are to a large extent unknown among Austrians.

[91]. According to this survey, 77 per cent of the respondents admitted to being more or less oblivious with regard to such topics. 92 per cent stated not to know whether (personal) data are being collected about themselves and if so, by whom. 76 per cent of the respondents were of the opinion that the Austrian population was not sufficiently informed about data protection, risks of data abuse or the legal conditions in question.

[92]. Regarding video surveillance, 55 per cent of the respondents declared that they were used to the fact that video cameras survey and record events and the behaviour of practically every person, regarding it rather as a commodity of modern life than a threat to fundamental rights. In another study by OEKONSULT,[69] concerning video surveillance of public space, even 81 per cent of the respondents declared that they accepted video cameras directed towards passers-by. 90 per cent admitted that they had got used to surveillance cameras everywhere.

[68] Vertrauen der ÖsterreicherInnen in den Datenschutz, available under: http://www.oekonsult.eu/datensicherheit2008.pdf (04.01.2009).

[69] Big Brother. Gefahr oder Normalität, available under: http://www.oekonsult.at/bigBrother_gesamtergebnisse_final.pdf (15.01.2009)

6. Analysis of deficiencies

[93]. As described in chapter 2.2. above, the DPC is severely understaffed and does not have a separate budget. This situation results in deficiencies especially concerning the examination of data applications pursuant to Sec. 30 paras. 2 and 3 DPA 2000, which suffer from a lack of resources.[70]

[94]. DPC decisions declaring an infringement of the data subject's rights deriving from the DPA 2000 by a public sector controller establish a legal duty for the controller to create a lawful situation but cannot be enforced by the DPC.[71] This does not comply with Art. 12 and Art. 24 of Directive 95/46/EC.

[95]. Video surveillance of public spaces for private purposes is currently not subject to specific rules. The recording of data in conjunction with video surveillance constitutes a data application and is subject to the duty to notify for the purpose of registration in the Data Processing Register.[72] If the data application involves data about acts and omissions punishable by courts or administrative authorities,[73] it is subject to prior checking.[74] *De facto*, the vast majority of surveillance cameras is not registered at all and thus not under the supervision and control of the DPC.

[96]. A major deficiency concerning the right to information results from the practice of the DPC, who usually requires about six months to decide on a case. However, if information is provided during this time, the DPC rejects the original claim irrespective of the completeness and legality of the information, which then requires the introduction of new proceedings. As a consequence, proceedings may take a very long time.

[97]. Sec. 24 para. 3 DPA 2000 allows an exemption from the obligation to inform the data subject about a use of data if the data was collected through transmission either from a different application purpose of the same controller or from the data application of another controller, if the use of data is provided for by law or ordinance. This provision excludes a large number of uses of data from the right to information, especially relating to data transmissions to the police.[75] This provision

[70] Cf. Sec. 30 paras. 2 and 3 DPA 2000.
[71] Cf. Sec. 40 para. 4 DPA 2000.
[72] Cf. Sec. 17 DPA 2000.
[73] Cf. Sec. 8 para. 4 DPA 2000.
[74] Cf. Sec. 18 para. 2 sub-para. 2 DPA 2000.
[75] Cf. Sec. 53 and Sec. 53 lit. a SPA.

severely restricts the fundamental rights of data subjects, because they do not get informed about an infringement, which would be a crucial condition to allow the respective data subject to take the necessary steps to have the legality of the intervention reviewed.

[98]. The DPA 2000 distinguishes between personal data and data that is 'only indirectly personal', meaning data relating to the data subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means.[76] Due to the obligations set up in Recital 26 of Directive 95/46/EC, 'only indirectly personal' data is not formally excluded, but in fact does not enjoy the protection of the DPA 2000 since the use of 'only indirectly personal' data does not constitute an infringement of interests in secrecy deserving protection[77] and data applications which contain 'only indirectly personal' data are excluded from the duty of the controller to notify.[78] In addition, the use of 'only indirectly personal' data does not entitle the data subject to exercise the rights granted in Secs. 26 to 28 DPA 2000 (right to information, right to rectification and erasure, right to object).[79]

[99]. Regarding the effectiveness of the DPC in general, an increase of human resources would be necessary to perform the tasks assigned to it on a level that complies with the European standard.[80] This would have positive effects on the currently rather long duration of proceedings (especially in the field of registration procedures) and the ability of the DPC to perform examinations of data applications as assigned by Sec. 30 paras. 2 and 3 DPA 2000. Furthermore, a separate budget would be necessary to ensure substantial independence of the DPC.

[100]. The term 'only indirectly personal data',[81] which is currently exempted from the protection of the DPA 2000, should be removed to ensure full protection of personal data.

[101]. As for video surveillance, there is a pressing need for specific regulations to improve the current situation, which is highly unsatisfying. The aforementioned planned amendment to the DPA 2000 shall establish specific rules for video surveillance. However, from a data protection perspective, the changes will be rather negative since real-time video surveillance (without recording) for the purpose

[76] Cf. Sec. 4 para. 1 sub-para. 1 DPA 2000.
[77] Sec. 8 para. 2 DPA 2000.
[78] Sec. 17 para. 2 sup-para. 3 DPA 2000.
[79] Sec. 29 DPA 2000.
[80] Cf. Datenschutzbericht 2007, p. 12, available under: http://www.dsk.gv.at/DocView.axd?CobId=30637 (11.01.2009).
[81] Sec. 4 sub-para. 1 DPA 2000.

of property protection shall be legal in any case irrespective of further requirements such as overriding interests.[82]

[82] Cf. Sec. 50a para. 3 sub-para. 4 Datenschutzgesetz-Novelle 2008, documents available under: http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00182/pmh.shtml (11.01.2009)

7. Good practices

[102]. With regard to important relevant legal provisions, practices and legal interpretations relating to the current data protection situation in Austria, no specific good practices could be detected.

8. Miscellaneous

[103]. Besides the DPC certain other institutions are also partly engaged with issues of data protection. The most important ones to be mentioned here are the *Datenschutzrat* [Data Protection Council] and the *Rechtsschutzbeauftragte* (RSB) [Commissioners for Legal Protection (CLP)].

8.1. Data Protection Council

[104]. Like the Data Protection Commission, the Data Protection Council must safeguard data protection in accordance with the regulations of the DPA 2000 without prejudice to the competence of the Federal Chancellor and the ordinary courts.[83]

[105]. Established within the Federal Chancellery, the Council advises the *Bundesregierung* [Federal Government] and the *Landesregierungen* [State Governments] upon their request in political matters of data protection.[84] For this purpose, it can deliberate on questions of fundamental importance for data protection; it has the opportunity to give its opinion on draft bills insofar as these are significant for data protection; public sector controllers must present their projects to the Council for evaluation insofar as these are significant for data protection; it has the right to request information and documents from public sector controllers insofar as this is necessary to evaluate projects of significant impact on data protection; it may ask private sector controllers to give their opinion on developments of general importance and it may transmit its observations, concerns and suggestions for improvements of data protection in Austria to the Federal Government and to the State Governments as well as to the legislative bodies.[85]

[106]. The Data Protection Council is composed of several representatives of Austrian political parties, one representative each from the *Bundeskammer für Arbeiter und Angestellte* [Federal Chamber of Labour] and the *Wirtschaftskammer Österreich* [Austrian Federal Economic Chamber], two representatives of the *Bundesländer* [States], one representative each of the *Gemeindebund* [Association of Municipalities] and the *Städtebund* [Association of Towns] as well as one member of the *Bund* [Federation] appointed by the Federal

[83] Cf. Sec. 35 para. 1 DPA 2000.
[84] Cf. Sec. 41 paras. 2 and 3 DPA 2000.
[85] Cf. Sec. 41 para. 2 DPA 2000.

Chancellor.[86] Each representative has one substitute.[87] According to Sec. 42 para. 4 DPA 2000, members of the Federal Government or a State Government, secretaries of state or persons who may not be elected for the *Nationalrat* [National Council] cannot be members of the Data Protection Council. The members serve on an honorary basis.[88]

[107]. Following Sec. 43 para. 3 DPA 2000, the Federal Chancellery is responsible for the operation of the Council. It supplies the necessary personnel.

[108]. For the preparation, appraisal and handling of specific issues, the Data Protection Council may install permanent or ad hoc working groups.[89]

[109]. The deliberations of the Council shall, according to Sec. 44 para. 7 DPA 2000, be confidential as long as the Council itself does not decide otherwise.

8.2. Commissioners for Legal Protection

[110]. Three Commissioners for Legal Protection were set up in Austria in order to control interferences with fundamental rights occurring through surveillance measures undertaken by security or criminal police as well as by military authorities. The first Commissioner was established in 1997[90] within the administrative framework of the Federal Ministry of Justice under Sec. 146 and 147 *Strafprozessordnung* (StPO) [Code of Criminal Procedure (CCP)].[91] The second one was set up in 2000[92] within the Federal Ministry of the Interior under Sec. 91 lit. a to d. SPA. Finally, the third Commissioner for Legal Protection was installed within the administrative framework of the Federal Ministry of Defence under Sec. 57 *Militärbefugnisgesetz* (MBG) [Armed Forces Authorisation Act (AFAA)].[93]

[111]. The Commissioners are established within the administrative frameworks of the Ministry of Justice, the Ministry of the Interior and

86 Cf. Sec. 42 para. 1 DPA 2000.
87 Cf. Sec. 42 para. 3 DPA 2000.
88 Cf. Sec. 42 para. 6 DPA 2000.
89 Cf. Sec. 44 para. 4 DPA 2000.
90 Austria/BGBl I 105/1997 (19.08.1997).
91 Austria/BGBl I 631/1975 (30.12.1975), last amended by Austria/BGBl I 109/2007 (28.12.2007).
92 Austria/BGBl I 85/2000 (10.08.2000).
93 Austria/BGBl I 86/2000 (10.08.2000), last amended by Austria/BGBl I 103/2002 (16.07.2002).

the Ministry of Defence. According to Art. 20 para. 2 of the Austrian Federal Constitution, the Commissioners can be exempted from being bound to instructions of superior organs. Thus and by operation of law, all Commissioners are independent and not bound by instructions in the exercise of their functions.[94]

[112]. Appointed by the competent ministers, the CLPs can be qualified as preventive control mechanisms pre-empting possible human rights interferences. The mandate of the CLP within the Ministry of Justice for example comprises the assessment and control of commands, approvals, sanctions and enforcement activities of police authorities with regard to e.g. covert investigations, simulated transactions, optic or acoustic observations and electronic data reconciliation.[95] The CLP within the Ministry of the Interior has to be informed on any inquiry of personalised data undertaken by security authorities.[96] Finally, the CLP within the Ministry of Defence is established to control the lawfulness of measures of the military intelligence service.[97] With regard to certain specific investigation measures, both the CLPs within the Ministry of Justice and within the Ministry of the Interior have to give prior consent.

[113]. Whenever the CLP within the Ministry of the Interior observes that the rights of individuals have been violated by any processing of personalised data without the knowledge of the persons concerned, the CLP is authorised to either inform these individuals or – in case this is not possible for reasons specified under Sec. 26 para. 2 DPA 2000 – to raise an appeal before the Data Protection Commission.[98] A similar authorisation applies for the CLP under the Ministry of Defence.[99]

94 Cf. Sec. 146 para. 4 CCP; Sec. 91 lit. a para 1 SPA; Sec. 57 para. 1 AFAA.
95 Cf. Sec. 147 CCF.
96 Cf. Sec. 91 lit c para. 1 SPA.
97 Cf. Sec. 57 para. 1 AFAA.
98 Cf. Sec. 91 lit. d para. 3 SPA.
99 Cf. Sec. 57 para. 6 AFAA.

Annexes

Annex 1 – Tables and Statistics[100]

	2000	2001	2002	2003	2004	2005	2006	2007[101]
Budget of data protection authority	No data available.[102]							
Staff of data protection authority	19,5[103]	16,25[104]	n/a	13,25[105]	20	19,25[106]	20	20

[100] Cf. Datenschutzbericht 2001, available under: http://www.dsk.gv.at/DocView.axd?CobId=30639 (11.01.2009), Datenschutzbericht 2005, available under: http://www.dsk.gv.at/DocView.axd?CobId=30638 (11.01.2009) and Datenschutzbericht 2007, available under: http://www.dsk.gv.at/DocView.axd?CobId=30637 (11.01.2009).

[101] Data available from 01.01.2007 until 30.06.2007.

[102] No separate budget available.

[103] 01.01.2000.

[104] 31.12.2001.

[105] February 2003.

[106] 01.07.2005.

Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative[107]	2	2	3	5	6	No data available.		
Number of data protection registrations[108]	-	4	approx. 770[109]			83		
Number of data protection approval procedures	No data available.							
Number of complaints received by data protection authority[110]	47	56	46	69	83	101	139	50
Number of complaints upheld by data protection authority	< 50%[111]		No data available.			54 of 242[112]		

[107] Examination of data applications (Sec. 30 paras. 2 and 3 DPA 2000).
[108] Data Processing Register (Sec. 16-22 DPA 2000).
[109] Mainly concerning 'banks' warning list'.
[110] Individual Complaints Procedure (Sec. 31 DPA).
[111] Datenschutzbericht 2005, p. 14, available under: http://www.dsk.gv.at/DocView.axd?CobId=30639 (11.01.2009).
[112] Datenschutzbericht 2007, p. 18, available under: http://www.dsk.gv.at/DocView.axd?CobId=30637 (11.01.2009).

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.)[113]	70	77	57	68	70	82	173	70
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)	No data available.							
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	No data available.							
Use of data for the purpose of Scientific Research and Statistics[114] and Transmission of Addresses to Inform or Interview Data Subjects[115]	7	9	7	8	3	4	7	1

[113] Ombudsperson Procedure (Sec. 30 DPA 2000).
[114] Sec. 46 DPA 2000.
[115] Sec. 47 DPA 2000.

Transborder Transmission and Committing of Data Subject to Licensing[116]	10	10	11	17	10	23	31	20
Legal Advice	No data available.			100	107	176	286	267
Proceedings before the Constitutional Court and the Administrative Court	13	2	4	6	23	33	33	16
Information (Schengen Information System)	No data available.		5	20	20	19	53	9

[116] Sec. 13 DPA 2000.

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	
Decision date	15.12.2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	6 Ob 275/05 t *Oberster Gerichtshof* [Supreme Court]
Key facts of the case (max. 500 chars)	The data subject, a lawyer, was registered on the 'banks' warning list' by his bank after refusing to pay a (contested) claim. The 'warning list' is an instrument of creditor protection and risk minimisation used by banks and contains data on breaches of contracts by customers. The measure resulted in severe (economic) consequences for the data subject. The Supreme Court held that putting the data subject on the warning list without prior information constituted a violation of his fundamental right to data protection (Sec. 1 DPA 2000). He was therefore entitled to compensation.
Main reasoning/argumentation (max. 500 chars)	Pursuant to Sec. 6 para. 1 DPA 2000, data shall only be used fairly and lawfully. Considering the severe consequences for the data subject, prior information would have been mandatory to allow the data subject to prevent or oppose his registration on the list. Putting a person on the banks' warning list in violation of the principle of fair use of data is an excessive interference with the data subject's fundamental right to data protection provided by Sec. 1 DPA 2000 that is not justified by creditor interests, and constitutes a violation of this right.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The principle of fair use of data implies that a data subject must be able to prevent or oppose a use of data if it is unjustified in his/her eyes and affects his/her creditworthiness in a severe manner. The registration on the banks' warning list, despite its factual truth and despite serving the legitimate purpose of creditor interests, constitutes a disproportionate interference with the data subject's interests deserving protection if it is carried out without prior information. The data subject's consent on a use of data requires that the he knows which data shall be used for which purpose.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The data subject is entitled to compensation.
Proposal of key words for data base	Data protection, fair use of data, proportionality, creditworthiness, banks' warning list, creditor protection

Case title	
Decision date	01.10.2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	6 Ob 195/98g *Oberster Gerichtshof* [Supreme Court]
Key facts of the case (max. 500 chars)	The data controller runs a credit agency ('Kreditinform') not authorised by law. The filing system contains data on creditworthiness that is open to inspection by the public, including information on execution proceedings. It is open to customers (mainly banks, mail-order and telecommunication businesses) who can prove overriding legitimate interests requiring the use of data. The Supreme Court held that the data subject has the right to object the inclusion of his/her data in a filing system which is not authorised by law (Sec. 28 para. 2 DPA 2000). The controller's refusal to erase the data constitutes a

	violation of the data subject's right to object a use of data.
Main reasoning/argumentation (max. 500 chars)	The 'Kreditinform' filing system is not authorised by law. The right to objection deriving from Sec. 28 para. 2 DPA 2000, which ensures that the erasure of data is subject only to the convenience of the data subject, allows a fair balance of interests: credit agencies, which are regarded as necessary and useful by the majority of the population, may legally exist, while specific interests of the data subject are still respected.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The right to object a use of data pursuant to Sec. 28 para. 2 DPA does not require any reasoning by the data subject. It covers the objection to the inclusion of data in a filing system, but also the (minor) right to erasure of particular data from the filing system. The legitimacy of collecting data relating to creditworthiness as provided for by the *Gewerbeordnung* [Trade, Commerce and Industry Regulation Act][117] does not curtail the data subject's right to objection pursuant to Sec. 28 para 2 DPA 2000.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The controller is obliged to erase the data as requested by the data subject.
Proposal of key words for data base	Data protection, creditworthiness, right to objection, erasure of data, credit agency, filing system, creditor interests

Case title	
Decision date	20.06.2008

[117] Austria/BGBl. 194/1994, last amended by Austria/BGBl. I 68/2008 (7.5.2008).

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	K600.054-001/0002-DVR/2008 *Datenschutzkommission* [Data Protection Commission]
Key facts of the case (max. 500 chars)	A school headmaster applied for registration of the data application 'video surveillance of aisles and the entry hall for the purpose of property protection (and the prevention of crimes), which shall be analysed only in cases defined by the purpose', reasoning that due to recent school-intern incidents a latent threat to life and security of the pupils, which could not be prevented by personal supervision, existed. The registration of the video surveillance was dismissed by the DPC due to lack of sufficient legal basis.
Main reasoning/argumentation (max. 500 chars)	The supervision of students is part of the teacher's obligation to teaching and education work (see Sec. 51 para. 3 *Schulunterrichtsgesetz* [School Education Act])[118] not also during lessons, but also before and after school and during breaks and school-related events. The use of technical surveillance measures in schools within teaching and educational work is subject to the strict reservation of statutory powers for interventions by public authorities. Any such interventions with the right to data protection require an expressed legal basis.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The prevention of endangerment of pupils through other pupils in school is part of the responsibility assigned to teachers by Sect. 51 para. 3 School Education Act and an aspect of the educational work of schools. Restrictions of the right to secrecy by interventions of public authorities must be based upon a substantial legal basis.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The application for registration of video surveillance is dismissed.
Proposal of key words for data base	Data protection, video surveillance, intervention of public authorities, reservation of statutory powers, school

[118] Austria/BGBl. 472/1986, last amended by Austria/BGBl. I 117/2008 (08.08.2008).

Case title	
Decision date	2.10.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	B 227/05-8 *Verfassungsgerichtshof* [Constitutional Court]
Key facts of the case (max. 500 chars)	The 'Herold Marketing CD private' contains data (such as name, address, age, number of children, partners and spending power) of approximately 2 million private persons collected by a marketing firm. It is up for sale to companies. The data controller refused to deliver a complete list of recipients of the CD to a data subject who requested information. The DPC decided that naming only categories of recipients did not violate the data subject's right to information. However, according to the Constitutional Court, the DPC failed to assess the legal situation correctly several times and thus violated the data subject's right to equality.
Main reasoning/argumentation (max. 500 chars)	The DPC's decision lacks a balance of interests between the data protection interests of the Herold Business Data GmbH & Co KG and its customers and the interests of the data subject, which would have been necessary to assess whether overriding legitimate interests are an obstacle to information to the data subject.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Registered data transmissions are subject to the data security measures provided in Sec. 14 paras. 1 and 2 DPA 2000. The right to information is subject to a balance of interests, but in general covers all data available. It does not only enable the data subject to prevent further use of data, but also serves the purpose of allowing the data subject to know where his/her data is available.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The DPC's decision is overruled.
Proposal of key words for data base	Data protection, right to information, registration, data collection, balance of interests

Case title	
Decision date	20.03.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	4 Ob 221/06p *Oberster Gerichtshof* [Supreme Court]
Key facts of the case (max. 500 chars)	The following provisions in standard business terms of a bank do not meet the requirements of the law: (a) A provision allowing the bank to exchange data on creditworthiness with enquiry offices usually employed by the bank, and to obtain information necessary to safeguard its legitimate interests. (b) A clause providing the borrower's consent to the transmission of his data to any company within the corporate group of the bank for marketing and advertisement purposes. According to the Supreme Court, both clauses allege consent of the data subject that is void and put the consumer at gross disadvantage.
Main reasoning/argumentation (max. 500 chars)	(a) Release from the banking secrecy through a provision in general business terms is not possible. Concerning the exchange of data, the bank must name the enquiry offices and the data concerned. (b) A clause allowing transmission of data for advertisement purposes must expressly refer to the consumer's possibility to withdraw his/her consent. Consent requires that the consumer knows the companies, products and form of advertisement in question.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Release from the banking secrecy through the customer must be expressly declared in written form. The transmission of data requires overriding legitimate interests of the bank. Data exchange requires express consent of the data subject referring to the category of data and to the information service in question.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The bank may not refer to the clauses in question in business relations with consumers. For the future, it has to omit the use of such clauses in standard business terms.
Proposal of key words for data base	Data protection, standard business terms, transmission of data, banking secrecy, data exchange, consent

Case title	
Decision date	10.08.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	K073.028-0004-DSK/2007 *Datenschutzkommission* [Data Protection Commission]
Key facts of the case (max. 500 chars)	The data subject claimed execution of an earlier DPC decision declaring that his right to information had been violated through insufficient information by the Federal Ministry of Finance. The DPC rejected his claim reasoning that it had no power to enforce its decisions on violations by public sector controllers.
Main reasoning/argumentation (max. 500 chars)	Sec. 40 para. 4 DPA 2000 provides that 'if the DPC has established that an infringement of provisions of this Federal Act [*Bundesgesetz*] by a public sector controller has taken place, said controller shall without delay and with all means at his disposal create the state expressed in the legal opinion of the DPC'. The provision does not arrange for any enforcement by the DPC.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Towards public sector controllers, the DPC is only entitled to declare violations of the right to data protection. Its decisions cause a legal obligation for the public authority to establish a lawful condition, but cannot be enforced by the DPC.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The data subject's application is dismissed.
Proposal of key words for data base	Data Protection, enforcement, declaratory decision, right to information, intervention, public sector controller

Case title	
Decision date	28.03.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	6 Ob 6/06 k *Oberster Gerichtshof* [Supreme Court]
Key facts of the case (max. 500 chars)	The controller used an (allegedly) fake surveillance camera to act as a deterrent instrument to protect his property. Due to the way the camera was installed, parts of the neighbour's premises were also covered by its field of vision. The Supreme Court held that this constitutes a severe interference with the neighbour's right to privacy and secrecy. However, the controller is entitled to use a surveillance camera as long as its field of vision is limited to his own property.

Main reasoning/argumentation (max. 500 chars)	It was not possible for the neighbour to distinguish whether the surveillance camera was real or fake. He had to assume that it would be used for recording at least on a few occasions and was therefore exposed to the permanent pressure of surveillance. Since the neighbour had to feel observed whenever he entered or left his house or spent time in his garden, the video surveillance constituted a severe interference with his right to privacy and secrecy despite being a fake.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The use of surveillance measures for the purpose of property protection is permitted if it is restricted to the property of the controller. The installation of a fake camera may violate the right to privacy and secrecy of data subjects in the same way and intensity as a real camera does if it puts a permanent pressure of observation on the data subject.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The surveillance of the controller's own property by use of a video camera is permitted. However, the camera's field of vision must not cover the property of the data subject.
Proposal of key words for data base	Data protection, video surveillance, fake camera, property protection, pressure of surveillance