Project Identification	
Project number	AAL 2012-5-199
Duration	1st May 2013– 30th April 2016
Coordinator	Martin Morandell
Coordinator Organisation	AIT Austrian Institute of Technology GmbH, Austria
Website	www.relaxedcare.eu

Ethical Manual

Document Identification	
Deliverable ID:	D-2.1 Ethical Manual
Release number/date	V1.0
Checked and released by	Martin Morandell
Work Status	Finished
Review Status	Accepted

Key Information from "Description of Work"	
Deliverable Description	Ethical Manual for the RelaxedCare Project
Dissemination Level	PU=Public
Deliverable Type	R = Report
Original due date	Request for changes, Accepted

Authorship& Reviewer Information	
Editor	Martin Morandell, AIT
Partners contributing	All
Reviewed by	Full Name of Responsible of Del, (Partner Name)

The project RelaxedCare is co-funded by the European AAL JP and the following national authorities and R&D programmes from Austria, Switzerland, Slovenia and Spain

Release History

Release Number	Date	Author(s)	Release description /changes made Please make sure that the text you enter here is a brief summary of what was actually changed; do not just repeat information from the other columns.
V 01	15.05.2013	MMo/AIT	First Version of Ethical Manal
V02	30.05.2013	MMo/AIT	Second Version of the Ethichal Manual
V03	10.12.2014	MMo/AIT	Added Data Protection Agreement

Relaxed Care Consortium

Relaxed Care (AAL 2012-5-199.) is a project within the AAL Joint Program Call 5
The consortium members are:

Partner 1	***AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GmbH (AIT, Project Coordinator, AT)***
Contact person:	Martin Morandell
Email:	martin.morandell@ait.ac.at

Partner 2	***Hochschule Luzern Technik & Architektur – iHomeLab (IHL, CH)***
Contact person:	Martin Biallas
Email:	Martin.Biallas@hslu.ch

Partner 3	***50plus GmbH (50p, AT)***
Contact person:	Frauke Lettmann
Email:	frauke.lettmann@50plusgmbh.com

Partner 4	***New Design University (NDU, AT)***
Contact person:	Sandra Dittenberger
Email:	sandra.dittenberger@ndu.ac.at

Partner 5	***Mobili (MOB, SI)***
Contact person:	Jure Lampe
Email:	jure.lampe@mobili.si

Partner 6	***Szenographie (SZE, CH)***
Contact person:	Ralph Eichenberger
Email:	contact@szenografie.com

Partner 7	***Ibernex (IBE, ES)***
Contact person:	Antonio Remartinez
Email:	antonio.remartinez@ibernex.es

Partner 8	***Soultank AG (SOUL, CH)***
Contact person:	Bianca Redel
Email:	bianca.redel@soultank.ch

Partner 9	***Schweizerisches Rote Kreuz Luzern (SRK, CH)***
Contact person:	Beatrice Burch
Email:	beatrice.burch@srk-luzern.ch

Table of Contents

Abbreviations

Abbrev.	*Description*
usw.:	und so weiter

1 Introduction

1.1 Background

This ethical manual is intended for the research and development project RelaxedCare. The project is financed by the European Union (EU), through the AAL Joint Program, and by national authorities in the respective countries represented in the consortium (National Contact Points).

The goal of the RelaxedCare project is to develop a system that helps informal caregivers to stay informed about the status of the assisted person and to enhance the communication in care situations.

Extensive end user involvement will be a vital part of the project, in order to guarantee that the new products and services are of relevance for the intended target group. Relevant literature suggests that end user involvement has generally positive effects, especially on user satisfaction, and involving end users as a primary source of information is an effective means of capturing user requirements when developing new products and services.

1.2 Purpose of the Ethical Manual

This ethical manual stipulates the code of conduct for the researchers, developers and administrative persons involved in the RelaxedCare project. The manual refers to main regulations that apply in the European Union and the respective states/countries of the participating project partners, as regards the protection of personal data security, in order to ensure that all project partners uphold maximum security during and after the project.

It is a binding document that contains ethical guidelines and principles, and the ethical manual builds the framework for the self-regulation of all personnel working within the RelaxedCare Project.

It also serves the purpose to uphold the trust between all persons collaborating within the project, such as researchers, developers, end users, etc

1.3 .Definitions

For a common understanding the following definitions should be used throughout the project:

1.3.1 Test phase

A “test phase” is a defined period of time where developed products and services will be tested in practice. For the tests, statistical and analytical methods will be used in order to gather information and knowledge about the applicability, usability and usefulness of the products and services tested.

The outcome of the test phase will be made public only in such a way that it does not interfere with the consent given by the participants in the test.

1.3.2 Test leader

The test leader is an organisation, represented by an appointed person that is responsible for the organisation and execution of the tests. This role can vary from test to test, but has to be assigned to a specific organisation and person in advance.

1.3.3 Interviewee

An interviewee is any person or organisation, from whom data and information is collected in a structured way, other than by practically testing devices or services.

1.3.4 Interview

An interview is defined as any form of contact with an interviewee in order to collect information and data to reach a certain goal.

1.3.5 Test Subject

A test subject is any person involved in practical trials of products and/or services, in order to collect feedback and user experiences as regards the tested device and/or service.

1.3.6 Test

A test is the attempt to try out developed products and services in a practical way, in order to gather information about the applicability, usability and operability.

2 Project Description

The goal of the RelaxedCare project is to take stress from the informal caregiver by providing unobtrusive about the wellbeing state of the assisted person. Furthermore it will provide a very simple way of communication to be able to send messages with a certain meaning to the other party.

The target groups are:

Informal Caregivers: People who are taking care of someone, maybe not in the sense nursing care, but looking after someone, feeling responsible for someone with the need to know about the wellbeing.

Assisted Persons: People who receive care, in many cases they still live on their own, but someone is looking after them.

The main goal of the project is to improve the quality of life of the informal caregivers by providing reassurance.

2.1 User-centered design - UCD

User-centered design (UCD) is an approach to design that grounds the process in information about the people who will use the product or service. UCD processes focus on users through the planning, design and development of a product or service (Ref.1: Usability Professionals' Association).

There is an international standard that is the basis for many UCD methodologies. This standard ISO 9241 part 210 (formally known as ISO 13407 Human-centred design process) defines a general process for including human-centered activities throughout a development life-cycle, but it does not specify exact methods.

Once the need to use a human-centered design process has been identified, four activities form the main cycle of work:

1. **Specify the context of use:**
   Identify the people who will use the product or service, what they will use it for, and under what conditions they will use it.
2. **Specify requirements:**
   Identify the user goals and business requirements that must be met for the product / service to be successful.
3. **Create design solutions:**
   This part of the process may be done in stages, building from a rough concept to a complete design.
4. **Evaluate designs:**
   The most important part of this process is, that the evaluation – ideally performed through usability testing with actual users, – is an integral part of quality testing for good software development.

The UCD process ends – and the product / service can be released – once the requirements are met.

Based on the methodology of User-centered Design, the RelaxedCare project will be executed according to the following steps/work packages (WP):

1. Requirements / Analysis Phase (WP2)
2. Design Phase (WP3-5)
3. System Integration & Test (WP6)

4. Pilot / Field Trials (WP7)

2.1.1 Requirements

The main objective of this phase is to understand the needs and wishes of the target groups addressed by the project, in order to guarantee that the outcome of the project will benefit the end users.

End-user requirements will be gathered through Photo-Study, Cultural Probes, Focus Groups, Design Workshop (including Emotion-Letters, Brainstorming, Collage, Semantic Differential and Modelling), Questionnaires and Interviews.

In addition, the requirements of the project's business and research partners, as well as other stakeholders, must be established, with the aim of securing a successful dissemination and exploitation of the result of the project.

2.1.2 Design

The design phase will consist of three blocks:

1. **Platform and Service Development**

   The establishment of a basic software infrastructure, onto which a range of ICT-based applications and services will be developed.

2. **Behaviour Pattern Recognition Modules**

   The aim is to find suitable mathematical methods for pattern recognition to model the different activities of daily living and other areas of interest.

3. **Pervasive In-/Output Modalities**
   The aim is to design pervasive, but at the same time unobtrusive, interfaces used for interaction with the informal carer on one side and the person in need of care at the other side.

2.1.3 System Integration & Test

The main purpose of this phase is to integrate all components developed into a running system. All prototypes will be tested and validated, in order to guarantee the safety of the test subjects in the following field trials.

2.1.4 Pilot / Field Trials

The objective of the field trials is to get the products, applications and services developed within the project tested by actual end users, with the aim of evaluating their functionality, usability and user benefits.

Evaluation of the test, results and the feedback and input from the test subjects, will cause improvements of the prototypes.

The main purpose of the field trials is to ensure that the outcome of the project benefits the end user also in reality.

3 Ethical Principles & Guidelines

3.1 Fundamental Principles

The following fundamental principles apply to all RelaxedCare project partners for the full duration of the project;

- Persons working for the RelaxedCare project must perform all their work strictly following the principles, guidelines and national regulations as stated in this document.
- Persons working for the RelaxedCare project must behave ethically correct and in such a way that they do not harm the project, any of its partners or the field of research in general.
- All persons participating in interviews and tests do this based on their own choice. Thereforeall project members must treat these persons in a respectful way.
- The rights of the test subjects must be granted at all times by all persons working on the project. No actions should be taken that might harm or wrong-do the test subjects, neither direct nor as a consequence of their participation in a test or interview.
- Data protection has to be guaranteed throughout the project. Personal data must never be used or revealed outside of the project.
- Project members have to conduct and document their work in an exact, transparent and objective way.

3.2 Ethical Principles

The four principles of biomedical ethics, as composed by Beauchamp and Childress (Ref.2: Beauchamp et al 2008), have been chosen as the basic ethical principles for the RelaxedCare project.

Beauchamp and Childress' principles for research are some of the most widely used frameworks and they offer a broad consideration of medical ethics issues in general, not just for the use in a clinical setting.

The four principles are general guides that leave considerable room for judgement in specific cases.

The four principles are:

Respect for autonomy: respecting the decision-making capacities of autonomous persons; enabling individuals to make reasoned informed choices.

RelaxedCare: the project partners will fully respect all test subjects' decisions about participation / non participation in the project. The project will provide potential test subjects with information in an appropriate way, including information about risks and possibly arising problems.

Beneficence: this considers the balancing of benefits against risks and costs; with the aim to benefit the test subjects.

RelaxedCare: the project partners will only perform user tests at the stage where prototypes are considered as safe, while at the same time offering the test subjects as many benefits as possible.

Non maleficence: avoiding the causation of harm; the research trials should not harm the participating person. Research trials might involve some minor harm, but the harm should not be disproportionate to the benefits of the trials.

RelaxedCare: although the participation in field trials will demand a certain effort from the test subjects, the project partners should keep these efforts as minimal as possible.

Furthermore, the RelaxedCare project partners will try to make the user involvement as interesting and pleasurable as possible for the test subjects.

All prototypes that will be tested by the test subjects during the field trials (WP7) will initially undergo pilot trials in order to avoid any malfunctions and/or failures that could cause the test subjects physical harm.

Justice: distributing benefits, risks and costs fairly; the notion that participants in similar positions should be treated in a similar manner.

RelaxedCare: the project partners aim to make as much of the gained knowledge as possible available to the public.

The aim of the project's business model will be to bring the results of the project to as wide a market as possible, in order to offer benefits to all stakeholders, but in particular to realize products and services that will offer benefits to elderly people.

3.3 General Guidelines

The project, especially the field trials, must be executed in a legal, candid, honest and objective way, and it must also be organized and executed following academic principles.

The rights of the test subjects have to be considered at all times. The project partners must not be allowed to carry through anything that could harm the test subjects while they are taking part in the project and the associated field trials.

The execution of the project has to be carried through in a responsible way, and common ethical business rules must apply at all times.

The test phase has to be separated from non-research activities in a clear way, in particular all activities that are connected to exploitation and commercialisation.

3.3.1 Integrity

The test subject's confidence in the RelaxedCare project and its partners must not be affected, neither by the organization, the execution nor the interpretation of the tests and interviews. In particular, any assumptions as regards the ability, experience and activity among the target group that might lead to a negative view of the target group, must be avoided. Test situations, interviews, etc. have to be organized in such a way that they do not risk to collect negative data from the test subjects as a result of their limited experience and/or knowledge in/from the research domain.

3.3.2 Voluntary participation

All test subjects and interviewees will participate in the RelaxedCare project on a fully voluntary basis, and they must not be misled in any situation.

A person's decision to partake as a test subject or interviewee is not binding, and he/she can prematurely end the participation at any chosen time.

3.3.3 Safety

All project partners and persons involved in the RelaxedCare project must at all times take appropriate measures in order to ensure that the voluntary participants are not subject to apparent danger, physical harm or any wrong-doing as a result of their participation in the test and/or interview.

3.3.4 Transparency

The test situation and the scope of the research have to be explained at the beginning of each test/interview situation.

It must be simple for the test subject / interviewee to receive accurate information about the background, content and aim of the project.

If required, the test subjects / interviewees should be allowed to control the quality of the field trials through an external source (at their own cost). As far as required, any technical details have to be provided to the test subjects, without endangering any immaterial property rights.

The test leaders have to ensure that the test user involvement is organized, executed and documented in an exact, transparent and objective way.

3.3.5 Monitoring

Before the interview or test starts, the interviewees and test subjects must be informed about the type of monitoring and recording instruments that will be applied, except when the interview or test is carried out in a public area with no personal data being collected. The data and relevant part of any recordings have to be deleted / destroyed if the test subject so requests. If there is no special agreement about the contrary, the identity of the test subject must be protected at all times.

4 Participation & Informed Consent

4.1 Introduction

The RelaxedCare consortium guarantees that no participants, interviewees or test subjects will take part in the project without having signed an Informed Consent. The Informed Consent should include relevant project information that describes what an eventual participation will involve, and also a consent form to be signed by the participant who decides to take part.

Potential participants, interviewees and test subjects should in understandable terms be informed about potential benefits, risks, inconvenience or obligations associated with the project that might reasonably be expected to influence their willingness to participate.

After having been informed about the project, the potential participant must be given sufficient time in order to consider the decision to take part or not.

Where participants are involved in longer-term data collection, the use of procedures for the renewal of the consent at an appropriate interval should be considered.

No inducement to participate should be offered prior to seeking consent, either in the form of payments or of gifts. Reasonable recompense for inconvenience and time contributed to the research, and reimbursement of travelling expenses, can be offered.

4.2 The Right to Withdraw

Any participation as an interviewee and/or test subject is fully voluntary. Participants should be informed clearly that they at any time have the right to withdraw their consent, and withdraw from their participation, and that any data that they have provided will be destroyed if they so request and that there will be no resultant adverse consequences.

4.3 Informed Consent Document

Please see Appendix A.

5 Anonymity, Confidentiality & Data Protection

People participating in research have the right not to have their identities or personal data revealed. Data protection implies informing the participants about who has access to their data and what may be done with this data. It also implies that the project partners handle the collected data with great care and according to relevant laws and regulations.

Except where explicit written consent is given, researchers and project partners should respect and preserve the confidentiality* of participants' identities and data at all times. The procedures by which this is to be achieved should be specified in the project protocol.

*Note that the duty of confidentiality is not absolute in law and may in exceptional circumstances be overridden by more compelling duties such as the duty to protect individuals from harm. Where a significant risk of such issues arising is identified in the risk assessment, specific procedures to be followed should be specified in the protocol.

All data and information collected within the RelaxedCare project must be handled in accordance with the respective national data protection regulations of Austria, Sweden and Switzerland. In addition to these national data protection regulations, directive 95/46/EC of the European Parliament (Ref.3: Directive 95/46/EC) shall apply in its latest version. If any veritable changes in European and/or national legislation on data protection will occur during the duration of the project, these will apply. Interviewee, participating end users and test subjects shall, if they so request, be given access to the latest versions of both European directives and national acts on data protection.

5.1 National regulations

As the vast majority of the project's end user involvement and field trials will be conducted in Austria and Switzerland, respective national regulations on personal data protection will apply in order to protect the integrity of any end user, interviewee and/or test subject participating in the project.

5.1.1 Austrian Federal Act concerning the Protection of Personal Data

(Datenschutzgesetz 2000 – DSG 2000)

Any resident of Austria, participating in the RelaxedCare project as end user, interviewee and/or test subject, is granted personal integrity under the Austrian Federal Act concerning the Protection of Personal Data (Appendix B1.1).

5.1.2 Swiss Federal Act on Data Protection

(235.1 Bundesgesetz über den Datenschutz)

Any resident of Switzerland, participating in the RelaxedCare project as end user, interviewee and/or test subject, is granted personal integrity under the Swiss Federal Act on Data Protection (Appendix B.2).

5.1.3 Slovenian Act on Data Protection

PERSONAL DATA PROTECTION ACT OF THE REPUBLIC OF SLOVENIA (ZVOP-1) (2013)

5.1.4 Spanish Act on Data Protection

ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data

5.2 European regulations

In the event that any person not living in Austria, or Switzerland would participate in the RelaxedCare project, the following regulations on personal data protection will apply in order to protect the integrity of any end user, interviewee and/or test subject participating in the project.

5.2.1 Directive 95/46/EC of the European Council

(Directive 95/46/EC of the European Council)

Any resident of the EU, participating in the RelaxedCareproject as an end-user, interviewee and/or test subject, is granted personal integrity under Directive 95/46/EC of the European Council.

5.3 Data Protection Agreement

The Data Protection Agreement is a document that must be signed by all project partners in order to assure that the recorded data will only be used for the foreseen research objectives.

Please see Appendix C.

6 Protection from Harm & eventual Insurance

6.1 Protection from Harm

Researchers and project partners must make every effort to minimize the risks of any harm, either physical or psychological, arising for any participant, researcher, project partner, institution, funding body or other person.

The project should carry out a risk analysis and, where significant risks are identified, should specify a risk management and harm alleviation strategy.

Where harm does nevertheless arise in the course of research, researchers should take remedial steps.

Participants should be given information as to whom they may contact in the event of any issues arising in the course of the research that cannot be resolved with members of the project team.

6.2 Insurance

When concrete plans for the end user involvement have been created, these plans will be verified with the legal departments of the project partners in order to evaluate if any additional insurance for the test subjects is required.

All participants and test subjects should be informed about the status of insurance before they take part in the field trials.

References

1. Usability Professionals' Association (UPA): "What is User-Centered Design?" http://www.upassoc.org/usability_resources/about_usability/what_is_ucd.html
2. Tom L. Beauchamp and James F. Childress: "Principles of Biomedical Ethics" Sixth Edition; OUP USA 2008
3. EUR Lex 1: "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Appendix A Informed Consent

Please see document *"Appendix_A_Informed_Consent.pdf"*.

Appendix B National Acts on Data Protection

B.1. Austrian Federal Act concerning the Protection of Personal Data

(Datenschutzgesetz 2000 – DSG 2000)
Please see document *"AppB1_Austrian_Federal_Act_Protection_of_Personal_Data.pdf"*.

B.2. Swiss Federal Act on Data Protection

(SR 235.1)
Please see document *"AppB3_Swiss_Federal_Act_on_Data_Protection.pdf"*.

B.3. Slovenian Act on Data Protection

PERSONAL DATA PROTECTION ACT OF THE REPUBLIC OF SLOVENIA

Please see document *"AppB3_Slovenian_Act_on_Data_Protection.pdf"*.

B.4. Spanish Act on Data Protection

23750 ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data

Please see document *"AppB3_Spanisch_Act_on_Data_Protection.pdf"*.

Appendix C Data Protection Agreement

Please see document *"Appendix_C_Data_Protection_Agreement.pdf"*.

Fassung vom 01.01.2014 **Date of Version: 1 January 2014**

Disclaimer:

- This translation is an unofficial aid for our readers. It has been made with great care, but linguistic compromises were unavoidable. Only the original German version is valid in any legal dispute.
- The reader should bear in mind that this law does not exist alone, but is a part of the Austrian legal system. Some provisions of the DSG 2000 will remain unclear without a certain level of background knowledge.
- Please note that this law may be amended in the future, and check occasionally for updates.
- The German title "Datenschutzgesetz 2000" and the abbreviation "DSG 2000" should be used in English texts to avoid confusion.

DSG 2000

StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
(CELEX-Nr.: 395L0046)

← Original Version

Änderung

BGBl. I Nr. 136/2001 (NR: GP XXI RV 742 AB 824 S. 81. BR: 6458 AB 6459 S. 681.)
BGBl. I Nr. 13/2005 (NR: GP XXII IA 515/A AB 821 S. 96. BR: AB 7228 S. 719.)
BGBl. I Nr. 2/2008 (1. BVRBG) (NR: GP XXIII RV 314 AB 370 S. 41. BR: 7799 AB 7830 S. 751.)
BGBl. I Nr. 133/2009 (NR: GP XXIV RV 472 AB 531 S. 49. BR: 8220 AB 8225 S. 780.)
BGBl. I Nr. 135/2009 (NR: GP XXIV RV 485 AB 558 S. 49. BR: 8217 AB 8228 S. 780.)
BGBl. I Nr. 112/2011 (NR: GP XXIV RV 1494 AB 1500 S. 130. BR: 8602 AB 8603 S. 802.)
[CELEX-Nr.: 32009L0133, 32010L0024]
BGBl. I Nr. 51/2012 (NR: GP XXIV RV 1618 AB 1771 S. 155. BR: 8730 AB 8731 S. 809.)

as amended by:
(List of amendments published in the Federal Law Gazette (F. L. G. = BGBl.)

BGBl. I Nr. 57/2013 (NR: GP XXIV RV 2131 AB 2245 S. 194. BR: AB 8940 S. 819.)
BGBl. I Nr. 83/2013 (NR: GP XXIV RV 2168 AB 2268 S. 200. BR: AB 8968 S. 820.)
[CELEX-Nr.: 31995L0046]

← amendment entailing the latest update of the present translation
(mind later changes of the German original as highlighted in the left column)

Click here to check the up-to-date list of amendments in the Austrian Legal Information System.

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)

Federal Act concerning the Protection of Personal Data (DSG 2000)

Inhaltsverzeichnis

Table of Contents

4. Abschnitt: Publizität der Datenverarbeitungen

5. Abschnitt: Die Rechte des Betroffenen

6. Abschnitt: Rechtsschutz

7. Abschnitt: Kontrollorgane

Part 4: Publicity of Data Applications

Part 5: Rights of the Data Subject

Part 6: Legal Remedies

Part 7: Control Bodies

8. Abschnitt: Besondere Verwendungszwecke von Daten

9. Abschnitt: Besondere Verwendungsarten von Daten

9a. Abschnitt: Videoüberwachung

10. Abschnitt: Strafbestimmungen

11. Abschnitt: Übergangs- und Schlußbestimmungen

Part 8: Special Purposes of Data Use

Part 9: Special Uses of Data

Part 9a: Video surveillance

Part 10: Penal Provisions

Part 11: Transitional and Final Provisions

Artikel 1
(Verfassungsbestimmung)

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung

Article 1
(Constitutional Provision)

Fundamental Right to Data Protection

§ 1. (1) Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject [Betroffener].

(2) Insofar personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another, namely 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 of the European Convention on Human Rights (Federal Law Gazette No. 210/1958). Such laws may provide for the use of data [Verwendung von Daten] 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 the case of permitted restrictions the intervention with the fundamental right shall be carried out using only the least intrusive of all effective methods.

(3) Everybody shall have, insofar as personal data concerning him are destined for automated processing or manual processing, i.e. in filing systems [Dateien] without automated processing, as provided for by law,

1. the right to obtain information as to who processes what data concerning him, where the data originated, for which purpose they are used, as well as to whom the data are transmitted;
2. the right to rectification of incorrect data and the right to erasure of illegally

unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(5) (Anm.: aufgehoben durch BGBl. I Nr. 51/2012)

Zuständigkeit

§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzbehörde, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Räumlicher Anwendungsbereich

§ 3. (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.

(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

(3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden.

(4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

processed data.

(4) Restrictions of the rights according to para. 3 are only permitted under the conditions laid out in para. 2.

(5) *(Note: Repealed by Federal Law Gazette 1 No. 51/2012)*

Legislative Power and Enforcement

§ 2. (1) The Federation [Bund] shall have power to pass laws concerning the protection of personal data that are automatically processed.

(2) The Federation shall have power to execute such federal laws. Insofar as such data are used by a State [Land], on behalf of a State, by or on behalf of legal persons established by law within the powers of the States [Länder] these Federal Acts [Bundesgesetze] shall be executed by the States unless the execution has been entrusted by federal law to the Data Protection Authority [Daten¬schutz¬behörde], the Data Protection Council [Daten¬schutz¬rat] or the courts.

Territorial Jurisdiction

§ 3. (1) The provisions of this Federal Act [Bundesgesetz] shall be applied to the use of personal data in Austria. This Federal Act shall also be applied to the use of data [Verwendung von Daten] outside of Austria, insofar as the data is used in other Member States of the European Union for purposes of a main establishment or branch establishment (§ 4 sub-para. 15) in Austria of the controller [Auftraggeber] (§ 4 sub-para. 4).

(2) Deviating from para. 1 the law of the state where the controller has its seat applies, when a controller of the private sector (§ 5 para. 3), whose seat is in another Member State of the European Union, uses personal data in Austria for a purpose that cannot be ascribed to any of the controller's establishments in Austria.

(3) Furthermore, this law shall not be applied insofar as data are only transmitted through Austrian territory.

(4) Legal provisions deviating form paras. 1 to 3 shall be permissible only in matters not subject to the jurisdiction of the European Union.

Artikel 2
1. Abschnitt

Allgemeines

Definitionen

§ 4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

1. „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
2. „sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
3. „Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;
4. Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;
5. Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen

Article 2
Part 1

General Provisions

Definitions

§ 4. For the subsequent provisions of this Federal Act [Bundesgesetz] the terms listed below shall mean:

1. ”Data” (”Personal Data”) [Daten” (”personenbezogene Daten”)]: Information relating to data subjects (sub-para. 3) who are identified or identifiable; Data are ”only indirectly personal” for a controller (sub-para. 4), a processor (sub-para. 5) or recipient of a transmission (sub-para. 12) when the Data relate to the 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;
2. ”Sensitive Data” (”Data deserving special protection”) [”sensible Daten” (”besonders schutzwürdige Daten”)]: Data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life;
3. ”Data Subject” [”Betroffener”]: any natural or legal person or group of natural persons not identical with the controller, whose data are processed (sub-para. 8);
4. ”Controller” [”Auftraggeber”]: natural or legal person, group of persons or organ of a territorial corporate body [Gebietskörperschaft] or the offices of these organs, if they decide alone or jointly with others to use data (sub-para.8), without regard whether they use the data themselves (sub-para. 8) or have it done by a service provider (sub-para. 5). They are also deemed to be controllers when the service provider instructed to carry out an order (sub-para. 5) decides to use data for this purpose (sub-para. 8) except if this was expressly prohibited or if the contractor has to decide under his own responsibility, on the basis of rules of law or codes of conduct.
5. ”Processor” [”Dienstleister”]: natural or legal person, group of persons or organ of a federal, state and local authority [Gebietskörperschaft] or the offices of these organs, if they use data only for a commissioned work (sub-para. 8);

Werkes verwenden (Z 8);

6. „Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
7. „Datenanwendung“: die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);
8. Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;
9. Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten;
10. *(Anm.: aufgehoben durch BGBl. I Nr. 133/2009)*
11. Überlassen von Daten: die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (Z 5);
12. Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
13. „Informationsverbundsystem“: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;
14. „Zustimmung“: die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;
15. „Niederlassung“: jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.

6. ”Filing System ” [”Datei”]: structured set of personal data which are accessible according to at least one specific criterion;
7. ”Data Application” [”Datenanwendung”]: the sum of logically linked stages of data use (sub-para. 8) which are organised in order to reach a defined result (the purpose of the Data Application) and which are as a whole or partially performed automatically, that is, performed by machines and controlled through programs (automated data processing);
8. ”Use of Data” [”Verwenden von Daten”]: all kinds of operations with Data, meaning both processing of data (sub-para. 9) and transmission of Data (sub-para. 12);
9. ”Processing of Data” [”Verarbeiten von Daten”]: the collection, recording, storing, sorting, comparing, modification, interlinkeage, reproduction, consultation, output, utilisation, committing (No. 11), blocking, erasure or destruction or any other kind of operation with data except the transmission of Data (sub-para. 12);
10. *(Note: Repealed by Federal Law Gazette I No. 133/2009)*
11. ”Committing of Data” [”Überlassen von Daten”]: the transfer of data from the controller to a processor in the context of a commissioned work (sub-para. 5);
12. ”Transmission of Data” [”Übermitteln von Daten”]: the transfer of data to recipients other than the data subject, the controller or a processor, in particular publishing of data as well as the use of data for another application purpose [Aufgabengebiet] of the controller;
13. ”Joint Information System” [”Informationsverbundsystem”]: joint processing of data in a data application by several controllers and the joint utilisation of the data so that every controller has access even to those data in the system that have been made available to the system by other controllers;
14. ”Consent” [”Zustimmung”]: the valid declaration of intention of the data subject, given without constraint, that he agrees to the use of data relating to him in a given case, after having been informed about the prevalent circumstances;
15. ”Establishment” [”Niederlassung”]: any organisational unit set apart in terms of layout and function by fixed facilities at a specific place, with or without the status of a legal person, which carries out activities at the place where it is set up.

Öffentlicher und privater Bereich

§ 5. (1) Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Bundesgesetzes zuzurechnen, wenn sie für Zwecke eines Auftraggebers des öffentlichen Bereichs (Abs. 2) durchgeführt werden.

(2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

(3) Die dem Abs. 2 nicht unterliegenden Auftraggeber gelten als Auftraggeber des privaten Bereichs im Sinne dieses Bundesgesetzes.

(4) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzbehörde zur Entscheidung zuständig, es sei denn, dass Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.

Public and Private Sector

§ 5. (1) Data applications [Datenanwendungen] shall be imputed to the public sector according to this Federal Act [Bundesgesetz] if they are undertaken for purposes of a controller of the public sector (para. 2).

(2) Public sector controllers are all those controllers who

1. are established according to public law legal structures, in particular also as an organ of a territorial corporate body [Gebietskörperschaft], or
2. as far as they execute laws despite having been incorporated according to private law.

(3) Controllers not within the scope of para. 2 are considered controllers of the private sector according to this Federal Act [Bundesgesetz].

(4) The fundamental right to data protection, except the right to information [Auskunftsrecht], 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 Data Protection Authority [Datenschutzbehörde] shall be competent to render the decision, unless an act of legislation or a judicial decision is concerned.

2. Abschnitt
Verwendung von Daten

Grundsätze

§ 6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, daß sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die

Part 2
Use of Data

Principles

§ 6. (1) Data shall only

1. be used fairly and lawfully;
2. be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further uses for scientific and statistical purposes is permitted subject to § 46 and 47;
3. be used insofar as they are essential for the purpose of the data application [Datenanwendung] and are not excessive in relation to the purpose;
4. be used so that the results are factually correct with regard to the purpose of the application, and the data must be kept up to date when necessary;
5. be kept in a form which permits identification of data subjects [Betroffene] as

Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

(3) Der Auftraggeber einer diesem Bundesgesetz unterliegenden Datenanwendung hat, wenn er nicht im Gebiet der Europäischen Union niedergelassen ist, einen in Österreich ansässigen Vertreter zu benennen, der unbeschadet der Möglichkeit eines Vorgehens gegen den Auftraggeber selbst namens des Auftraggebers verantwortlich gemacht werden kann.

(4) Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben erachtet hat.

Zulässigkeit der Verwendung von Daten

§ 7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und
2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, daß die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und daß die Grundsätze des § 6 eingehalten werden.

long as this is necessary for the purpose for which the data were collected; a longer period of storage may be laid down in specific laws, particularly laws concerning archives.

(2) The controller [Auftraggeber] shall bear the responsibility that the principles of para. 1 are complied with in all his data applications; this also applies when he employs a processor [Dienstleister] to use the data.

(3) A controller responsible for a use of data [Datenverwendung] subject to this Federal Act [Bundesgesetz] who does not reside in the European Union has to name a representative residing in Austria who can be held responsible in place of the controller, without prejudice to the possibility of legal measures against the controller himself.

(4) To determine more closely what can be regarded as fair and lawful use of data [Datenverwendung] in a specific field, representations of interest established by law, other professional associations and comparable bodies may draw up codes of conduct for the private sector. These codes of conduct shall only be published after they have been submitted to the Federal Chancellor [Bundeskanzler] for evaluation, have been evaluated and have been found to be in compliance with the present law.

Legitimate Use of Data

§ 7. (1) Data shall be processed only insofar as the purpose and content of the data application [Datenanwendung] are covered by the statutory competencies or the legitimate authority of the respective controller and the data subjects' [Betroffener] interest in secrecy deserving protection is not infringed.

(2) Data shall only be transmitted if

1. they originate from a legal data application according to para. 1 and
2. the recipient has satisfactorily demonstrated to the transmitting party his statutory competence or legitimate authority with regard to the purpose of the transmission [Übermittlung], insofar as it is not beyond doubt, and
3. the interests in secrecy of the data subject deserving protection are not infringed by the purpose and content of the transmission.

(3) The legitimacy of a use of data [Datenverwendung] requires that the intervention be carried out only to the extent required, and using the least intrusive of all effective methods and that the principles of § 6 be respected.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

§ 8. (1) Schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder
4. überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung zulässigerweise veröffentlichter Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.

(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat oder
7. im Katastrophenfall, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist; im letztgenannten Fall gilt § 48a Abs. 3.

Interests in Secrecy Deserving Protection for the Use of Non-Sensitive Data

§ 8. (1) Interests in secrecy deserving protection are not infringed when using non-sensitive data if

1. an explicit legal authorisation or obligation to use the data exists; or
2. the data subject [Betroffener] has given his consent, which can be revoked at any time, the revocation making any further use of the data illegal; or
3. vital interests of the data subject require the use; or
4. overriding legitimate interests pursued by the controller [Auftraggeber] or by a third party require the use of data [Datenverwendung].

(2) The use of legitimately published data and only indirectly personal data shall not constitute an infringement of interests in secrecy deserving protection. The right to object to the use of data legitimately published pursuant to § 28 remains unaffected.

(3) Interests in secrecy deserving protection are not infringed according to para. 1 sub-para. 4, in particular if the use of data

1. is an essential requirement for a controller of the public sector to exercise a legally assigned function or
2. is performed by a controller of the public sector in fulfilment of his obligation to provide inter-authority assistance or
3. is required to protect the vital interests of a third party or
4. is necessary for the fulfilment of a contract between the controller and the data subject or
5. is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and if the data were collected legitimately or
6. concerns solely the exercise of a public office by the data subject.
7. in case of catastrophy, to the extent required to assist the persons directly affected by the catastrophy, to locate and identify persons missing or dead and to inform next of kin; in the very last case § 48a para. 3 applies.

(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder
2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder
3. sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Bundesgesetz gewährleistet oder
4. die Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlungen (Unterlassungen) zuständige Behörde erfolgt.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 9. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen

(4) The use of data concerning acts and omissions punishable by the courts or administrative authorities, and in particular concerning suspected criminal offences, as well as data concerning criminal convictions and preventive measures does not without prejudice to para. 2 infringe interests in secrecy deserving protection if

1. an explicit legal obligation or authorisation to use the data exists; or
2. the use of such data is an essential requirement for a controller of the public sector to exercise a legally assigned function;
3. the legitimacy of the data application [Daten¬anwendung] otherwise follows from statutory responsibilities or other legitimate interests of the controller that override the data subjects' interests in secrecy deserving protection and the manner of use safeguards the interests of the data subject according to this Federal Act [Bundesgesetz].or

4.the transmitting of data is made for a report to an institution in charge of prosecution of a reported criminal act (or criminal omission).

Interests in Secrecy Deserving Protection for the Use of Sensitive Data

§ 9. (1) The use of sensitive data does not infringe interests in secrecy deserving protection only and exclusively if

1. the data subject [Betroffener] has obviously made public the data himself or
2. the data are used only in indirectly personal form or
3. the obligation or authorisation to use the data is stipulated by laws, insofar as these serve an important public interest, or
4. the use is made by a controller of the public sector in fulfilment of his obligation to give inter-authority assistance or
5. data are used that concern solely the exercise of a public office by the data subject or
6. the data subject has unambiguously given his consent, which can be revoked at any time, the revocation making any further use of the data illegal, or
7. the processing or transmission [Über¬mittlung] is in the vital interest of the

des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder

8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46, zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 oder im Katastrophenfall gemäß § 48a verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hiebei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

§ 10. (1) Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister die hiefür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen

data subject and his consent cannot be obtained in time or

8. the use is in the vital interest of a third party or
9. the use is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and the data were collected legitimately or
10. data are used for private purposes pursuant to § 45 or for scientific research or statistics pursuant to § 46 for information or interviewing of the data subject pursuant to § 47 or in case of a catastrophy according to § 48a or
11. the use is required according to the rights and duties of the controller in the field of employment law and civil service regulations and, and is legitimate according to specific legal provisions; the rights of the labour councils according to the Arbeitsverfassungsgesetz with regard to the use of data [Datenverwendung] remain unaffected, or
12. the data are required for the purposes of preventive medicine, medical diagnosis, the provision of health care or treatment or the management of health-care services, and the use of data is performed by medical personnel or other persons subject to an equivalent duty of secrecy, or
13. non profit-organisations with a political, philosophical, religious or trade-union aim process data revealing the political opinion or philosophical beliefs of natural persons in the course of their legitimate activities, as long as these are data of members, sponsors or other persons who display an interest in the aim of the organisation on a regular basis; these data shall not be disclosed to a third party without the consent of the data subjects unless otherwise provided for by law.

Legitimate Committing of Data for Service Processing

§ 10. (1) Controllers [Auftraggeber] may employ processors [Dienstleister] for their data applications [Datenanwendungen] insofar as the latter sufficiently warrant the legitimate and secure use of data [Datenverwendung]. The controller shall enter into agreements with the processor necessary therefor and satisfy himself that the agreements are complied with by acquiring the necessary information about the actual

Maßnahmen zu überzeugen.

(2) Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegt, ist der Datenschutzbehörde mitzuteilen, es sei denn, daß die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht. Kommt die Datenschutzbehörde zur Auffassung, daß die geplante Inanspruchnahme eines Dienstleisters geeignet ist, schutzwürdige Geheimhaltungsinteressen der Betroffenen zu gefährden, so hat sie dies dem Auftraggeber unverzüglich mitzuteilen. Im übrigen gilt § 30 Abs. 6 Z 4.

Pflichten des Dienstleisters

§ 11. (1) Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber jedenfalls folgende Pflichten:

1. die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;
2. alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
3. weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, daß er dies allenfalls untersagen kann;
4. - sofern dies nach der Art der Dienstleistung in Frage kommt - im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;
5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;
6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen

measures implemented by the processor.

(2) A planned enlistment of a processor by a controller of the public sector for a data application subject to prior checking [Vorabkontrolle] pursuant to § 18 para. 2 shall be notified to the Data Protection Authority [Datenschutzbehörde] unless the enlistment of the processor is carried out on grounds of an explicit legal authorisation or the processor is an organisational unit that is superior or subordinate to the processor or one of his superior organs. The Data Protection Authority shall inform the controller without delay if it comes to the conclusion that the planned enlistment of a processor may endanger interest in secrecy of the data subject [Betroffener] deserving protection. § 30 para. 6 sub-para. 4 applies.

Obligations of the Processor

§ 11. (1) Irrespective of contractual obligations, all processors [Dienstleister] have the following obligations when using data for a controller [Auftraggeber]:

1. to use data only according to the instructions of the controller; in particular, the transmission [Übermittlung] of the data used is prohibited unless so instructed by the controller;
2. to take all required safety measures pursuant to § 14; in particular to employ only operatives who have committed themselves to confidentiality vis-á-vis the processor or are under a statutory obligation of confidentiality;
3. to enlist another processor only with the permission of the controller and therefore to inform the controller of this intended enlistment of another processor in such a timely fashion that the controller has the possibility to object;
4. insofar as this is possible given the nature of the service processing [Dienstleistung] to create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller’s obligation to grant the right of information, rectification and erasure;
5. to hand over to the controller after the end of the service processing all results of processing and documentation containing data or to keep or destroy them on his request;
6. to make available to the controller all information necessary to control the compliance with the obligations according to sub-paras. 1 to 5.

notwendig sind.

(2) Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der in Abs. 1 genannten Pflichten sind zum Zweck der Beweissicherung schriftlich festzuhalten.

Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

§ 12. (1) Die Übermittlung und Überlassung von Daten an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes ist keinen Beschränkungen im Sinne des § 13 unterworfen. Dies gilt nicht für den Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

(2) Keiner Genehmigung gemäß § 13 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird unter Beachtung des § 55 Z 1 durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des § 6 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

(3) Darüberhinaus ist der Datenverkehr ins Ausland dann genehmigungsfrei, wenn

1. die Daten im Inland zulässigerweise veröffentlicht wurden oder
2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden oder
3. die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder
4. Daten aus Datenanwendungen für private Zwecke (§ 45) oder für publizistische Tätigkeit (§ 48) übermittelt werden oder
5. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat oder
6. ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann oder
7. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden, oder
8. die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2

(2) Agreements between the controller and the processor concerning the details of the obligations according to para. 1 shall be laid down in writing to perpetuate the evidence.

Transborder Transmission and Committing of Data not Subject to Licensing

§ 12. (1) The transmission [Übermittlung] and committing [Überlassung] of data to recipients in signatory states of the European Economic Area is not subject to any restrictions in terms of § 13. This does not apply to data exchange between public sector controllers [Auftraggeber] in fields that are not subject to the law of the European Union.

(2) No authorisation pursuant to § 13 shall be required for data exchange with recipients in third countries with an adequate level of data protection. The countries that have an adequate level of data protection shall be enumerated in an ordinance [Verordnung] of the Federal Chancellor [Bundeskanzler] in accordance with § 55 sub-para. 1 . The decisive consideration as to the adequacy of the protection shall be the implementation of the principles of § 6 para. 1 in the foreign legal system as well as the existence of effective guarantees for their enforcement.

(3) Furthermore, transborder data exchange shall not require authorisation if

1. the data have been published legitimately in Austria or
2. data are transferred or committed that are only indirectly personal to the recipient or
3. the transborder transmission or committing is authorised by regulations that are equivalent to a statute in the Austrian legal system and are immediately applicable or
4. data from a data application [Daten¬anwendung] for private purposes (§ 45) or for journalistic purposes (§ 48) is transmitted or
5. the data subject [Betroffener] has without any doubt given his consent to the transborder transmission or committing or
6. a contract between the controller and the data subject or a third party that has been concluded clearly in the interest of the data subject cannot be fulfilled except by the transborder transmission of data or
7. the transmission is necessary for the establishment, exercise or defence of legal claims before a foreign authority and the data were collected legitimately or
8. the transmission or committing is expressly named in a standard ordinance

Z 6) oder Musterverordnung (§ 19 Abs. 2) ausdrücklich angeführt ist oder

9. es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt oder
10. Übermittlungen oder Überlassungen aus Datenanwendungen erfolgen, die gemäß § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

(4) Wenn eine Übermittlung oder Überlassung von Daten ins Ausland in Fällen, die von den vorstehenden Absätzen nicht erfaßt sind,

1. zur Wahrung eines wichtigen öffentlichen Interesses oder
2. zur Wahrung eines lebenswichtigen Interesses einer Person

notwendig und so dringlich ist, daß die gemäß § 13 erforderliche Genehmigung der Datenschutzbehörde nicht eingeholt werden kann, ohne die genannten Interessen zu gefährden, darf sie ohne Genehmigung vorgenommen werden, muß aber der Datenschutzbehörde umgehend mitgeteilt werden.

(5) Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung in das Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland gemäß § 7. Bei Überlassungen ins Ausland muß darüber hinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber - oder in den Fällen des § 13 Abs. 5 an den inländischen Dienstleister - vorliegen, daß er die Dienstleisterpflichten gemäß § 11 Abs. 1 einhalten werde. Dies entfällt, wenn die Dienstleistung im Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind.

Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

§ 13. (1) Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzbehörde (§§ 35 ff) einzuholen. Die Datenschutzbehörde kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden.

(2) Die Genehmigung ist unter Beachtung der gemäß § 55 Z 2 ergangenen Kundmachungen zu erteilen, wenn die Voraussetzungen des § 12 Abs. 5 vorliegen und wenn, ungeachtet des Fehlens eines im Empfängerstaat generell geltenden angemessenen Datenschutzniveaus,

1. für die im Genehmigungsantrag angeführte Übermittlung oder Überlassung im konkreten Einzelfall angemessener Datenschutz besteht; dies ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenverwendung

[Standardverordnung] (§ 17 para. 2 sub-para. 6) or model ordinance [Musterverordnung] (§ 19 para. 2) or

9. the data exchange is with Austrian governmental missions and offices in foreign countries or
10. the transmissions or committings are made from a data application that is exempted from notification according to § 17 para. 3.

(4) If the transborder transmission or committing in cases not covered by the preceding paragraphs is necessary

1. to safeguard an important public interest or
2. to safeguard a vital interest of a person

and of such urgency that the authorisation of the Data Protection Authority [Datenschutzbehörde] required according to § 13 cannot be obtained in time without risk to the above-mentioned interests, it may be performed without a permit, but must be notified to the Data Protection Authority immediately.

(5) The legality of a data application in Austria according to § 7 is a prerequisite for every transborder transmission or committing. Furthermore, transborder committings require the written promise of the processor [Dienstleister] abroad to the domestic controller - or in the case of § 13 para. 5 to the domestic processor - that he shall respect the obligations of a processor according to § 11 para 1. This is not applicable if the processing abroad is provided for in regulations that are equivalent to a law in the Austrian legal system and are immediately applicable.

Transborder Transmission and Committing of Data Subject to Licensing

§ 13. (1) Insofar as a case of transborder data exchange is not exempted from authorisation according to § 12, the controller has to apply for a permit by the Data Protection Authority [Datenschutzbehörde] (§ 35) before the transmission [Übermittlung] or committing [Überlassung]. The Data Protection Authority can issue the permit subject to conditions and obligations.

(2) The permit shall be given, taking into consideration the promulgations [Kundmachungen] pursuant to § 55 sub-para. 2, if the requirements of § 12 para. 5 are met, and despite the lack of an adequate general level of data protection in the recipient state

1. an adequate level of data protection exists for the transmission or committing outlined in the application for the permit in this specific case; this is then to be judged considering all circumstances relevant to the use of data

eine Rolle spielen, wie insbesondere die Art der verwendeten Daten, die Zweckbestimmung sowie die Dauer der geplanten Verwendung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen, Standesregeln und Sicherheitsstandards; oder

2. der Auftraggeber glaubhaft macht, daß die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers sowie einseitige Zusagen des Antragstellers (§ 19 Abs. 2) im Genehmigungsantrag über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein. Einseitige Zusagen des Antragstellers werden für diesen mit der Registrierung durch die Datenschutzbehörde verbindlich.

(3) Bei meldepflichtigen Datenanwendungen hat die Datenschutzbehörde eine Ausfertigung jedes Bescheides, mit dem eine Übermittlung oder Überlassung von Daten in das Ausland genehmigt wurde, zum Registrierungsakt zu nehmen und die Erteilung der Genehmigung im Datenverarbeitungsregister (§ 16) anzumerken.

(4) Abweichend von Abs. 1 kann auch ein inländischer Dienstleister die Genehmigung beantragen, wenn er zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber mehreren Auftraggebern jeweils einen bestimmten weiteren Dienstleister im Ausland heranziehen will. Die tatsächliche Überlassung darf jeweils nur mit Zustimmung des Auftraggebers erfolgen. Der Auftraggeber hat der Datenschutzbehörde mitzuteilen, aus welcher seiner meldepflichtigen Datenanwendungen die dem Dienstleister genehmigte Überlassung erfolgen soll; dies ist im Datenverarbeitungsregister anzumerken.

(5) Die Übermittlung von Daten an ausländische Vertretungsbehörden oder zwischenstaatliche Einrichtungen in Österreich gilt hinsichtlich der Pflicht zur Einholung von Genehmigungen nach Abs. 1 als Datenverkehr mit dem Ausland.

(6) Hat der Bundeskanzler trotz Fehlens eines im Empfängerstaat generell geltenden angemessenen Schutzniveaus durch Verordnung festgestellt, daß für bestimmte Kategorien des Datenverkehrs mit diesem Empfängerstaat die Voraussetzungen gemäß Abs. 2 Z 1 zutreffen, tritt an die Stelle der Verpflichtung zur Einholung einer Genehmigung die Pflicht zur Anzeige an die Datenschutzbehörde. Die Datenschutzbehörde hat binnen sechs Wochen ab Einlangen der Anzeige mit Bescheid den angezeigten Datenverkehr zu untersagen, wenn er keiner der in der Verordnung

[Datenverwendung], such as the type of data used, the purpose and duration of use, the country of origin and final destination as well as the general and sectoral legal provisions, professional rules and security standards applying in the third country; or

2. the controller can satisfactorily demonstrate that the interests in secrecy deserving protection of the data subject [Betroffener] of the planned data exchange will be respected outside of Austria. In particular, contractual guarantees by the recipient as well as unilateral declarations by the applicant (§ 19 para 2) in the application for permit about the more detailed circumstances of the use of data abroad are significant for the decision. Unilateral declarations by the applicant become legally binding for him upon registration by the Data Protection Authority.

(3) In the case of data applications subject to notification, the Data Protection Authority shall put a copy of each ruling [Bescheid] authorising the transborder transmission or committing of data on the notification file and enter the fact that authorisation has been granted into the Data Processing Register [Datenverarbeitungsregister] (§ 16).

(4) Deviating from para. 1, a domestic processors [Dienstleister] can apply for a permit if, in order to fulfil his contractual duties vis-á-vis multiple controllers, he wishes to enlist the service of a specific processor outside of Austria. The actual committing shall only be performed with the consent of the controller. The controller shall report to the Data Protection Authority from which of his data applications subject to notification the authorised committing to the processor shall take place; this is to be entered into the Data Processing Register .

(5) The transmission of data to representations of foreign governments or intergovernmental institutions in Austria shall be treated as transborder data exchange with regard to the requirement for authorisation according to para. 1.

(6) If the Federal Chancellor [Bundeskanzler] has decreed by ordinance [Verordnung] that, despite the lack of an adequate general level of data protection in the recipient state, the requirements according to para. 2 sub-para. 1 are met for specific categories of data exchange with this recipient state, the obligation to obtain a permit is replaced by an obligation to notify the Data Protection Authority. The Data Protection Authority shall prohibit the notified data exchange within six weeks after receiving the notification if it is not attributed to one of the categories regulated in the ordinance

geregelten Kategorien zuzurechnen ist oder den Voraussetzungen gemäß § 12 Abs. 5 nicht entspricht; andernfalls ist die Übermittlung oder Überlassung der Daten in das Ausland zulässig.

3. Abschnitt
Datensicherheit

Datensicherheitsmaßnahmen

§ 14. (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge,

[Verordnung] or if it does not fulfil the requirements according to sect. 12 para. 5; otherwise the transmission or committing is permitted.

Part 3
Data Security

Data Security Measures

§ 14. (1) Measures to ensure data security shall be taken by all organisational units of a controller [Auftraggeber] or processor [Dienstleister] that use data. Depending on the kind of data used as well as the extent and purpose of the use and considering the state of technical possibilities and economic justifiability it shall be ensured that the data are protected against accidental or intentional destruction or loss, that they are properly used and are not accessible to unauthorised persons.

(2) In particular, the following measures are to be taken insofar as this is necessary with regard to the last sentence of para. 1:

1. The distribution of functions between the organisational units as well as the operatives regarding the use of data [Datenverwendung] shall be laid down expressly,
2. The use of data must be tied to valid orders of the authorised organisational units or operatives,
3. every operative is to be instructed about his duties according to this Federal Act [Bundes¬gesetz] and the internal data protection regulations, including data security regulations,
4. The right of access to the premises of the data controller or processor is to be regulated,
5. The right of access to data and programs is to be regulated as well as the protection of storage media against access and use by unauthorised persons,
6. The right to operate the data processing equipment is to be laid down and every device is to be secured against unauthorised operation by taking precautions for the machines and programs used,
7. Logs shall be kept in order that the processing steps that were actually

wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,

8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(3) Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, daß dem Betroffenen Auskunft gemäß § 26 gegeben werden kann. In der Standardverordnung (§ 17 Abs. 2 Z 6) oder in der Musterverordnung (§ 19 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, daß es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.

(5) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

(6) Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, daß sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

Datengeheimnis

§ 15. (1) Auftraggeber, Dienstleister und ihre Mitarbeiter - das sind Arbeitnehmer

performed, in particular modifications, consultations and transmissions [Übermittlungen], can be traced to the extent necessary with regard to their permissibility,

8. A documentation shall be kept on the measures taken pursuant to sub-paras. 1 to 7 to facilitate control and conservation of evidence.

These measures must, taking into account the technological state of the art and the cost incurred in their execution, safeguard a level of data protection appropriate with regard to the risks arising from the use and the type of data to be protected.

(3) Unregistered transmissions from data applications [Datenanwendungen] subject to an obligation to grant information pursuant to § 26 shall be logged in such a manner that the right of information [Auskunftsrecht] can be granted to the subject pursuant to § 26. Transmissions provided for in the standard ordinance [Standardverordnung] (§ 17 para. 2 lit. 6) and the model ordinance [Musterverordnung] (§ 19 para. 2) do not require logging.

(4) Logs and documentation data may not be used for purposes that are incompatible with the purpose of the collection [Ermittlung] - viz., monitoring the legitimacy of the use of the logged and documented data files [Datenbestand]. In particular, any further use for the purpose of supervising the data subjects [Betroffener] whose data is contained in the logged data files, as well as for the purpose of monitoring the persons who have accessed the logged data files, or for any purpose other than checking access rights shall be considered incompatible, unless the data is used is for the purpose of preventing or prosecuting a crime according to § 278a StGB (criminal organisation) or a crime punishable with a maximum sentence of more than five years imprisonment.

(5) Unless expressly provided for otherwise by law, logs and documentation data shall be kept for three years. Deviations from this rule shall be permitted to the same extent that the logged or documented data files [Datenbestand] may legitimately be erased earlier or kept longer.

(6) Data security regulations are to be issued and kept available in such a manner that the operatives can inform themselves about the regulations to which they are subject at any time.

Confidentiality of Data

§ 15. (1) Controllers [Auftraggeber], processors [Dienstleister] and their

(Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis - haben Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, daß sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeits(Dienst)verhältnisses zum Auftraggeber oder Dienstleister einhalten werden.

(3) Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen die Bestimmungen dieses Bundesgesetzes kein Nachteil erwachsen.

operatives these being the employees and persons comparable to employees shall keep data from uses of data [Datenanwendungen] confidential that have been entrusted or made accessible to them solely for professional reasons, without prejudice to other professional obligations of confidentiality, unless a legitimate reason exists for the transmission [Übermittlung] of the entrusted or accessed data (confidentiality of data [Datengeheimnis]).

(2) Operatives shall transmit data only if expressly ordered to do so by their employer. controllers and processors shall oblige their operatives by contract, insofar as they are not already obliged by law, to transmit data from uses of data only if so ordered and to adhere to the confidentiality of data even after the end of their professional relationship with the controller or processor.

(3) Controllers and processors may only issue orders for the transmission of data if this is permitted pursuant to the provisions of this Federal Act [Bundesgesetz]. They shall inform the operatives affected by these orders about the transmission orders in force and about the consequences of a violation of data confidentiality.

(4) Without prejudice to the constitutional right to issue instructions [Weisungen] , a refusal to follow an order to transmit data on the grounds that it violates the provisions of this Federal Act shall not be to the operatives detriment.

4. Abschnitt
Publizität der Datenanwendungen

Datenverarbeitungsregister

§ 16. (1) Die Datenschutzbehörde hat ein Register der Auftraggeber mit den von ihnen betriebenen Datenanwendungen zum Zweck der Information der Betroffenen zu führen.

(2) Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, daß er Betroffener ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Auftraggebers oder anderer Personen entgegenstehen.

Part 4
Publicity of Data Applications

Data Processing Register

§ 16. (1 The Data Protection Authority [Datenschutzbehörde] shall operate a register of controllers and their data applications [Datenanwendungen] for the purpose information of the data subjects [Betroffene].

(2) Any person may inspect the register. Access to the registration file including the licences contained therein shall be granted if the person applying for inspection can satisfactorily demonstrate that he is a data subject, and as far as no overriding interest in secrecy on part of the controller deserving protection is an obstacle to access.

(3) Der Bundeskanzler hat die näheren Bestimmungen über die Führung des Registers durch Verordnung zu erlassen. Dabei ist auf die Richtigkeit und Vollständigkeit des Registers, die Übersichtlichkeit und Aussagekraft der Eintragungen und die Einfachheit der Einsichtnahme Bedacht zu nehmen.

Meldepflicht des Auftraggebers

§ 17. (1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzbehörde mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken (Änderungsmeldung). Für manuelle Dateien besteht eine Meldepflicht nur, soweit die Inhalte zumindest einen der Tatbestände des § 18 Abs. 2 Z 1 bis 3 erfüllen.

(1a) Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte (§ 2 Z 10 des E Government-Gesetzes, BGBl. I Nr. 10/2004) erfolgen. Nähere Bestimmungen über die Identifizierung und Authentifizierung sind in die gemäß § 16 Abs. 3 zu erlassende Verordnung aufzunehmen. Eine Meldung in Form von E-Mail oder in nicht-elektronischer Form ist für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.

(2) Nicht meldepflichtig sind Datenanwendungen, die

1. ausschließlich veröffentlichte Daten enthalten oder
2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses oder
3. nur indirekt personenbezogene Daten enthalten oder
4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) oder
5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden oder
6. einer Standardanwendung entsprechen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts

(3) The Federal Chancellor [Bundeskanzler] shall lay down more specific regulations about the management of the register in an ordinance [Verordnung]. This is to be done with due regard to the correctness and completeness of the register, the clarity and expressiveness of the entries and the ease of access.

Duty of the Controller to Notify

§ 17. (1) Every controller [Auftraggeber] shall, unless provided for otherwise in paras. 2 and 3, before commencing a data application [Datenanwendung], file a notification whose contents are laid down in § 19 with the Data Protection Authority [Datenschutzbehörde] for the purpose of registration in the Data Processing Register [Datenverarbeitungsregister]. The duty to notify also applies to all circumstances that subsequently lead to the incorrectness or incompleteness of the notification (notification of change). Such duty of notification applies to manual filing systems only to the extent its contents match at least one of the elements of § 18 para 2 sub-para. 1 to 3.

(1a) The notification is to be filed electronically through a web application to be provided by the Federal Chancellor. Identification and authentication can be performed by using the citizen´s card [Bürgerkarte] (§ 2 para 10 of the E Government Act, Federal Law Gazette I No. 10/2004). Detailed instructions on the identification and authentication procedure shall be contained in the ordinance to be rendered according to § 16 para 3. Notification by e-mail or in non-electronic form is admissible for manual filing systems, or in case of a longer lasting technical blackout of the web application.

(2) Data applications are not subject to notification

1. which solely contain published data or
2. whose subject is the management of registers and catalogues that are by law open to inspection by the public, even if a legitimate interest for doing so must be demonstrated or
3. which contain only indirectly personal data or
4. which are carried out by natural persons for activities that are entirely personal or concern just the person’s family life (§ 45) or
5. which are carried out for journalistic purposes according to § 48 or
6. correspond to a standard application [Standardanwendung]. The Federal Chancellor [Bundeskanzler] can lay down in an ordinance [Verordnung] that some types of data applications and transmissions [Übermittlung] are standard applications, if they are carried out by a large number of controllers in similar

des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

(3) Weiters sind Datenanwendungen für Zwecke

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherstellung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten

von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist.

Aufnahme der Verarbeitung

§ 18. (1) Der Vollbetrieb einer meldepflichtigen Datenanwendung darf - außer in den Fällen des Abs. 2 - unmittelbar nach Abgabe der Meldung aufgenommen werden.

(2) Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in § 48a Abs. 1 genannten Zwecke betreffen, dürfen, wenn sie

1. sensible Daten enthalten oder
2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder
3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder
4. in Form eines Informationsverbundsystems durchgeführt werden sollen,

erst nach ihrer Prüfung (Vorabkontrolle) durch die Datenschutzbehörde nach den näheren Bestimmungen des § 20 aufgenommen werden.

Notwendiger Inhalt der Meldung

§ 19. (1) Eine Meldung im Sinne des § 17 hat zu enthalten:

fashion and if a risk to the data subjects' [Betroffener] interest in secrecy deserving protection is unlikely considering the purpose of the use and the processed categories of data [Datenarten]. The ordinance shall list for every Standard Application the authorised categories of data, the categories of data subjects [Betroffenenkreise] and recipients [Empfängerkreise] as well as the maximum period of time during which the data may be stored .

(3) Furthermore, data applications for the purpose of

1. protecting the constitutional institutions of the Republic of Austria or
2. safeguarding the operational readiness of the federal army or
3. safeguarding the interests of comprehensive national defence or
4. protecting important foreign policy, economic or financial interests of the Republic of Austria or the European Union
5. preventing and prosecuting of crimes

shall be exempt from the duty to notify, insofar as this is necessary to achieve the purpose of the data application.

Commencement of Processing

§ 18. (1) A data application [Daten¬anwendung] subject to notification may - except as laid down in para. 2 - take up full operation immediately after the notification has been submitted.

(2) Data applications subject to notification which neither correspond to a Model Application [Musteranwendung] pursuant to § 19 para. 2 nor concern the internal affairs of the churches and religious communities recognised by the state or the processing of data in case of a catastrophy for the purposes named in § 48a al 1 and

1. which involve sensitive data or
2. which involve data about offences according to § 8 para. 4 or
3. whose purpose is to give information on the data subjects [Betroffener] creditworthiness or
4. which are carried out in the form of a joint information system [Informationsverbundsystem],

shall be initiated only after an examination (prior checking) [Vorabkontrolle] by the Data Protection Authority [Datenschutzbehörde] in accordance with § 20.

Required Content of the Notification

§ 19. (1) A notification pursuant to § 17 must contain

1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 3 oder eines Betreibers gemäß § 50 Abs. 1, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben, und

3a. die Erklärung, ob die Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 oder § 50c Abs. 1 zweiter Satz genannten Tatbestände für die Vorabkontrollpflicht erfüllt, und

4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und
5. die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise - einschließlich allfälliger ausländischer Empfängerstaaten - sowie die Rechtsgrundlagen der Übermittlung und
6. - soweit eine Genehmigung der Datenschutzbehörde notwendig ist - die Geschäftszahl der Genehmigung durch die Datenschutzbehörde sowie
7. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

(2) Der Auftrageber kann bei Einbringung der Meldung oder danach bis zum Abschluss des Registrierungsverfahrens zusagen, dass er sich beim Betrieb der Datenanwendung bestimmten Auflagen oder Bedingungen unterwerfen oder die Datenanwendung nur befristet betreiben wird. Eine derartige Zusage wird für den Auftraggeber mit der Registrierung durch die Datenschutzbehörde rechtsverbindlich. Eine Registrierung darf nur erfolgen, wenn die zugesagte Auflage, Bedingung oder Befristung derart bestimmt ist, dass sie auch von der Datenschutzbehörde nach § 21 Abs. 2 ausgesprochen werden könnte.

(3) Wenn eine größere Anzahl von Auftraggebern gleichartige Datenanwendungen vorzunehmen hat und die Voraussetzungen für die Erklärung zur Standardanwendung

1. the name (or other designation) and address of the controller [Auftraggeber] and of his representative according to § 6 para. 3 or of the operator pursuant to § 50 para. 1; furthermore the registration number of the controller, insofar as one has been already assigned to him, and
2. the proof of statutory competence or of the legitimate authority that the controller's activities are permitted, if so required and
3. the purpose of the data application [Datenanwendung] to be registered and the legal basis, as long as this is not included in the information according to sub-para. 2 and

3a. a statement, whether the data application matches one or more of the cases for prior checking named in § 18 para 2 sub-para 1 to 4 or § 50c para 1 second sentence and

4. the categories of data subjects [Betroffenenkreise] and the categories of data [Datenarten] about them that are processed and
5. the categories of data subjects [Betroffenenkreise] affected by intended transmissions [Übermittlungen], the categories of data [Datenarten] to be transmitted and the matching categories of recipients [Empfängerkreise] - including possible recipient states abroad - as well as the legal basis for the transmission and
6. insofar as a permit by the Data Protection Authority [Datenschutzbehörde] is required the file number of the permit of the Data Protection Authority as well as
7. a general description of data security measures taken pursuant to § 14, which enable a preliminary assessment of the appropriateness of the security measures.

(2) The controller may at from time the notification is submitted until the end of the registration procedure promise to respect certain requirements or conditions when operating a data application or to operate the data application only for a limited period of time. A declaration of this type becomes legally binding for the controller upon registration by the Data Protection Authority. A registration may only be made if a promised requirement, the condition or time limit is equally specific to a requirement that could be imposed by the Data Protection Authority according to § 21 para 2.

(3) If a large number of controllers has to carry out data applications in similar fashion and the prerequisites for a Standard Application [Standardanwendung] do not

nicht vorliegen, kann der Bundeskanzler durch Verordnung Musteranwendungen festlegen. Meldungen über Datenanwendungen, die inhaltlich einer Musteranwendung entsprechen, müssen nur folgendes enthalten:

1. die Bezeichnung der Datenanwendung gemäß der Musterverordnung und
2. die Bezeichnung und Anschrift des Auftraggebers sowie den Nachweis seiner gesetzlichen Zuständigkeit oder seiner rechtlichen Befugnis, soweit dies erforderlich ist, und
3. die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde.

(4) Eine Meldung ist mangelhaft, wenn Angaben fehlen, offenbar unrichtig, unstimmig oder so unzureichend sind, daß Einsichtnehmer im Hinblick auf die Wahrnehmung ihrer Rechte nach diesem Bundesgesetz keine hinreichende Information darüber gewinnen können, ob durch die Datenanwendung ihre schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer gemeldeten Datenanwendung durch die gemeldeten Rechtsgrundlagen nicht gedeckt ist.

Prüfungs- und Verbesserungsverfahren

§ 20. (1) Meldungen von Datenanwendungen, die nach Angabe des Auftraggebers nicht einen der Tatbestände des § 18 Abs. 2 Z 1 bis 4 erfüllen, sind nur automationsunterstützt auf ihre Vollständigkeit und Plausibilität zu prüfen. Ist demnach die Meldung nicht fehlerhaft, so ist sie sofort zu registrieren.

(2) Wird bei der automationsunterstützten Prüfung ein Fehler der Meldung festgestellt, so ist dem Auftraggeber die Möglichkeit zur Verbesserung einzuräumen. Gleichzeitig ist er darauf hinzuweisen, dass die Meldung als nicht eingebracht gilt, wenn keine Verbesserung erfolgt oder er auf der Einbringung der unverbesserten Meldung besteht. Im letztgenannten Fall kann der Einbringer die Meldung schriftlich unter Anschluss der ausgedruckten Fehlermeldung der Datenschutzbehörde übermitteln, welche die Meldung auf Mangelhaftigkeit im Sinn des § 19 Abs. 4 zu prüfen hat.

(3) Meldungen, die der Auftraggeber als vorabkontrollpflichtig bezeichnet hat oder von diesem zulässigerweise nicht im Wege der Internetanwendung (§ 17 Abs. 1a) eingebracht wurden, sind auf Mangelhaftigkeit im Sinn des § 19 Abs. 4 zu prüfen.

(4) Ergibt die Prüfung nach § 19 Abs. 4 eine Mangelhaftigkeit der Meldung, so ist

apply, the Federal Chancellor can designate Model Applications [Musteranwendung] by ordinance [Verordnung]. Notifications of data applications whose content corresponds to a Model Application need to contain only the following:

1. the designation of the model application [Musteranwendung] according to the model ordinance [Musterverordnung] and
2. the designation and address of the controller as well as proof of statutory competencies or of legitimate authority, as far as this is required, and
3. the registration number of the controller, insofar as one has been already assigned to him.

(4) 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 this Federal Act [Bundesgesetz] cannot obtain sufficient information as to the issue whether their interests in secrecy deserving protection could be infringed by the data application. In particular, inconsistency is given in case of a deviation of the notified content from the notified legal basis.

Examination and Correction Procedure

§ 20. (1) Notifications of data applications, which according to the information provided by the controller, do not match one of the cases of § 18 para 2 No. 1 to 4, are to be examined only through automatic examination for completeness and plausibility. If, accordingly, the notification is not faulty, it is to be registered immediately.

(2) In case it is determined in the course of the automatic examination that the notification is faulty, the controller is to be granted the opportunity for correction. Simultaneously he is to be informed that the notification shall be regarded as not have been submitted if no correction is made or if he insists on the submitting the uncorrected notification. In the latter case the filing person may transmit the notification in writing, attaching the printed error report, to the Data Protection Authority, which has to examine the notification for defectiveness in the sense of § 19 para 4.

(3) Notifications which the controller has marked as subject to prior checking or which have been filed not by web application in an admissible manner (§ 17 para 1a) are to be examined for defectiveness in the sense of § 19 para 4.

(4) If the examination according to § 19 para 4 shows the defectiveness of a

dem Auftraggeber innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung unter Setzung einer angemessenen Frist aufzutragen. Im Verbesserungsauftrag ist auf die Rechtsfolgen einer Nichtbefolgung nach Abs. 5 hinzuweisen.

(5) Wird dem Verbesserungsauftrag nicht entsprochen, ist die Registrierung der Meldung durch eine schriftliche Mitteilung abzulehnen. In die Mitteilung sind aufzunehmen:

1. die Punkte, in denen der Verbesserungsauftrag nicht erfüllt wurde und
2. der Hinweis, dass innerhalb von zwei Wochen ab Zustellung bei der Datenschutzbehörde ein Antrag gestellt werden kann, über die Ablehnung mit Bescheid abzusprechen.

Nach Absendung der Mitteilung erstattete Verbesserungen sind nicht zu berücksichtigen.

Registrierung

§ 21. (1) Meldungen gemäß § 19 sind in das Datenverarbeitungsregister einzutragen, wenn

1. das Prüfungsverfahren nach § 20 Abs. 1 keinen Fehler ergeben hat oder
2. das Prüfungsverfahren nach § 20 Abs. 2 und 3 keine Mangelhaftigkeit der Meldung ergeben hat oder
3. nach Einlangen einer auf Mangelhaftigkeit zu prüfenden Meldung bei der Datenschutzbehörde zwei Monate verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 4 erteilt wurde oder
4. der Auftraggeber die aufgetragenen Verbesserungen (§ 20 Abs. 2 und 4) vorgenommen hat.

Die in der Meldung enthaltenen Angaben über Datensicherheitsmaßnahmen sind im Register nicht ersichtlich zu machen.

(2) Bei Datenanwendungen, die gemäß § 18 der Vorabkontrolle unterliegen, können auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen, Bedingungen oder Befristungen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit dies zur Wahrung der durch dieses Bundesgesetz geschützten Interessen der Betroffenen notwendig ist.

(3) Der Auftraggeber ist von der Durchführung und vom Inhalt der Registrierung

notification, the controller is to it be instructed within two months after the notification has been received, to correct it within an adequate time period. The instruction for correction has to contain information on the legal consequences of non-compliance according to para 5.

(5) If the instruction for correction [Verbesserungsauftrag] is not fulfilled the registration of the notification is to be denied by written information. This information must contain:

1. the points in which the instruction for correction was not fulfilled and
2. the information, that within two weeks after delivery a motion can be filed with the Data Protection Authority to render a ruling on the refusal.

Corrections filed after sending of the information are not to be taken into consideration.

Registration

§ 21. (1) Notifications pursuant to § 19 are to be entered into the Data Processing Register [Datenverarbeitungsregister] if

1. the examination procedure according to § 20 para 1 has shown no defect or
2. the examination procedure according to § 20 paras 2 and 3 has shown no deficiency of the notification or
3. two months have passed since a notification meant to be examined for deficiency was submitted to the Data Protection Authority without a request for correction having been issued pursuant to § 20 para 4 or
4. the controller has made the corrections which were requested (§ 20 para 2 and 4).

The information on data security measures contained in the notification shall not be entered into the register.

(2) For data applications subject to prior checking [Vorabkontrolle] pursuant to § 18 the execution of the data application may be permitted subject to conditions, requirements and deadlines based on the findings of the checking procedure, insofar as this is necessary to safeguard interests of the data subject [Betroffener] that are protected by this Federal Act [Bundesgesetz].

(3) The controller is to be informed on the registration and its content in an

in geeigneter Weise zu verständigen.

(4) Jedem Auftraggeber ist bei der erstmaligen Registrierung eine Registernummer zuzuteilen.

(5) Hat die automationsunterstützte Prüfung nach § 20 Abs. 1 keine Fehlerhaftigkeit der Meldung ergeben, so ist in die Registrierung ein Vermerk aufzunehmen, dass der Meldungsinhalt nur automationsunterstützt geprüft wurde.

Richtigstellung des Registers und Rechtsnachfolge

§ 22. (1) Streichungen aus dem Register und sonstige Änderungen des Registers sind auf Grund einer Änderungsmeldung des registrierten Auftraggebers oder von Amts wegen in den Fällen des Abs. 2, des § 22a Abs. 2 und des § 30 Abs. 6a vorzunehmen. Derartige Änderungen sind für die Dauer von sieben Jahren ersichtlich zu machen.

(2) Gelangen der Datenschutzbehörde aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist dieser von Amts wegen aus dem Register zu streichen. Außerdem ist eine registrierte Datenanwendung zu streichen, wenn eine Befristung des Betriebes (§ 19 Abs. 2, § 21 Abs. 2) abgelaufen ist oder der Datenschutzbehörde zur Kenntnis gelangt, dass die Datenanwendung dauerhaft nicht mehr betrieben wird.

(3) Berichtigungen oder Streichungen nach Abs. 2 sind ohne weiteres Ermittlungsverfahren durch Mandatsbescheid (§ 57 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51) zu verfügen.

(4) Der Rechtsnachfolger eines registrierten Auftraggebers kann einzelne oder alle registrierten Meldungen des Rechtsvorgängers übernehmen, wenn er innerhalb von sechs Monaten nach Wirksamkeit der Rechtsnachfolge eine entsprechend glaubhaft gemachte Erklärung gegenüber der Datenschutzbehörde abgibt. Dem Rechtsnachfolger kann auf Antrag auch die Registernummer des Rechtsvorgängers übertragen werden, wenn der Rechtsvorgänger jegliche Verarbeitung personenbezogener Daten in Auftraggebereigenschaft eingestellt hat.

Verfahren zur Überprüfung der Erfüllung der Meldepflicht

§ 22a. (1) Die Datenschutzbehörde kann jederzeit die Erfüllung der Meldepflicht durch einen Auftraggeber prüfen. Dies gilt sowohl für die Mangelhaftigkeit einer registrierten Meldung im Sinn des § 19 Abs. 4 als auch für die rechtswidrige

appropriate manner.

(4) A registration number shall be assigned to each controller upon first registration.

(5) If the automatically processed examination according to § 20 para 1 has shown no deficiency of the notification a note is to be made in the registration that the content of the notification was only examined through automatic processing.

Rectification of the Register and Legal Succession

§ 22. (1) Deletions from the register and other amendments of the register are to be made on the basis of an amendment notification by the registered controller or ex officio in the cases of para 2, § 22a para 2 and of § 30 para 6a. Such amendments are to be made visible for the duration of seven years.

(2) If the Data Protection Authority [Daten¬schutz¬behörde] learns through official publications about changes in the designation or address of the controller [Auftraggeber], the entry shall be corrected ex officio. If an official publication states that the legal basis of the controller [Auftraggeber] is no longer valid, the he/she shall be deleted from the register shall ex officio. Also a registered data-application is to be deleted if a time limit for its operation has expired (§19 para 2, § 21 para 2) or the Data Protection Authority learns that the data application is no longer in operation.

(3) Corrections or deletions pursuant to para. 2 are to be ordered without further investigation by provisional rulings [Mandatsbescheid] (§ 57 of the General Administrative Procedure Act 1991 – AVG, Federal Law Gazette No. 51/1991).

(4) The legal successor of a registered controller may take over individual or all registered notifications of the predecessor, if he/she, within six months after the effectiveness of the legal succession, makes a plausible statement to the Data Protection Authority. Upon request, the legal successor may also be granted the register number of the predecessor, if the predecessor has discontinued any processing of personal data in the function of a controller.

Procedure for the control of the fulfilment of the registration obligation

§ 22a. (1) The Data Protection Authority may at any time examine whether a controller has fulfilled the registration obligation. This applies to the deficiency of a registered notification and the sense of § 19 para 4 as well as to the unlawful omission

Unterlassung von Meldungen.

(2) Bei Vorliegen des Verdachtes der Nichterfüllung der Meldepflicht infolge Mangelhaftigkeit einer registrierten Meldung (Abs. 1) oder Unterlassung der Meldung, die über die Fälle des § 22 Abs. 2 hinausgeht, ist ein Verfahren zur Berichtigung des Datenverarbeitungsregisters durchzuführen. Das Verfahren wird durch begründete Verfahrensanordnung eingeleitet, die dem meldepflichtigen Auftraggeber mit einem Auftrag zur Verbesserung (§ 20 Abs. 4) oder einer Aufforderung zur Nachmeldung (§ 17 Abs. 1) innerhalb gesetzter Frist zuzustellen ist.

(3) Wird einem im Verfahren nach Abs. 2 erteilten Verbesserungsauftrag nicht entsprochen, so ist die Streichung der Meldung mit Bescheid der Datenschutzbehörde zu verfügen. Die Streichung kann sich, wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Herstellung des rechtmäßigen Zustandes ausreichend ist, auch nur auf Teile der Meldung beschränken.

(4) Wird einer im Verfahren nach Abs. 2 erteilten Aufforderung zur Nachmeldung nicht entsprochen und die Unterlassung einer Meldung entgegen § 17 Abs. 1 erwiesen, so ist mit Bescheid der Datenschutzbehörde der weitere Betrieb der Datenanwendung, soweit er vom Registerstand abweicht, zu untersagen und gleichzeitig Anzeige nach § 52 Abs. 2 Z 1 an die zuständige Behörde zu erstatten.

(5) Ergibt das Verfahren nach Abs. 2 alleine die Unangemessenheit oder die Nichteinhaltung von nach § 19 Abs. 1 Z 7 erklärten Datensicherheitsmaßnahmen, so ist dies mit Bescheid festzustellen und gleichzeitig eine angemessene Frist zur Herstellung ausreichender Datensicherheit zu setzen. Der Auftraggeber hat innerhalb dieser Frist der Datenschutzbehörde die getroffenen Maßnahmen mitzuteilen. Sind diese nicht ausreichend, so ist die Streichung der Datenanwendung zu verfügen.

(6) Die Einleitung und der Stand eines Berichtigungsverfahrens nach Abs. 2 ist bei registrierten Meldungen im Datenverarbeitungsregister bis zur Einstellung oder bis zur Herstellung eines rechtmäßigen Zustandes durch Maßnahmen nach den Abs. 3 bis 6 geeignet anzumerken.

Pflicht zur Offenlegung nicht-meldepflichtiger Datenanwendungen

§ 23. (1) Auftraggeber einer Standardanwendung haben jedermann auf Anfrage mitzuteilen, welche Standardanwendungen sie tatsächlich vornehmen.

(2) Nicht-meldepflichtige Datenanwendungen sind der Datenschutzbehörde bei

of notifications.

(2) In case it is suspected that the registration obligation has not been fulfilled because of deficiency of a registered notification (para 1) or omission of the notification beyond the cases of § 22 para 2, a procedure to correct the data processing register is to be performed. The procedure is to be instituted by reasoned procedural order to be served to the controller obliged to the notification with the instruction for correction (§ 20 para 4) or with summons for subsequent notification (§ 17 para 1) within a deadline set.

(3) If in a procedure an order for correction under para 2 is not complied with, the Data Protection Authority shall order the deletion of the notification by ruling. The deletion may be restricted only to parts of the notification, if this technically possible, gives a meaningful result with regard to the purpose of the data application and is sufficient to create the lawful situation.

(4) If in a procedure according to para 2 a request for subsequent notification is not complied with and the omission of a notification contrary to § 17 para 1 is proven, the Data Protection Authority shall prohibit any further operation of the data application, to the extent deviating from the situation in the register, by a ruling and simultaneously a report is to be made according to § 52 para 2 sub-para. 1 to the authority in charge.

(5) In case the procedure according to para 2 shows only that data safety measures declared in accordance with § 19 para 1 sub-para. 7 are unsuitable or not observed, this is to be stated in a ruling and simultaneously an adequate deadline to be set to provide sufficient data security. The controller shall within such deadline inform the data protection Authority about the measures taken. If such are insufficient, the deletion of the data application shall be ordered.

(6) The beginning and the current status of the correction procedure according to para 2 for registered notifications in the data processing register is to be marked in adequate manner till the termination or till a lawful situation has been created by measures according para 3 to 6.

Obligation to Provide Information on Data Applications not Subject to Notification

§ 23. (1) Controllers [Auftraggeber] of a standard application [Standardanwendung] shall inform anyone on request which standard applications they actually carry out.

(2) Data applications not subject to notification shall be disclosed to the Data

Ausübung ihrer Kontrollaufgaben gemäß § 30 offenzulegen.

Informationspflicht des Auftraggebers

§ 24. (1) Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und
2. über Namen und Adresse des Auftraggebers,

zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.

(2) Über Abs. 1 hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist; dies gilt insbesondere dann, wenn

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder
2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder
3. Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne daß dies gesetzlich vorgesehen ist.

(2a) Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert.

(3) Werden Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt, darf die Information gemäß Abs. 1 entfallen, wenn

1. die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist oder
2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder

Protection Authority [Daten¬schutz¬behörde] in pursuit of its supervisory duties according to § 30.

The Controller's Duty to Provide Information

§ 24. (1) The controller [Auftraggeber] of a data application [Datenanwendung] shall inform the data subjects when collecting data in an appropriate manner about

1. the purpose of the data application for which for which the data are collected, and
2. the name and address of the controller,

insofar as this as this information is not already available to the data subject [Betroffener], with regard to the particular circumstances of the case.

(2) Information beyond the scope of para. 1 shall be given if this is necessary for fair and lawful processing, in particular if

1. the data subject has a right to object to intended processing or transmission of data pursuant to § 28 or
2. it is not clear for the data subject under the circumstances whether he is required by law to reply to the questions posed, or
3. data are to be processed in a joint information system [Informationsverbundsystem] that is not authorised by law.

(2a) If the controller learns that data from his data application are systematically and seriously misused and the data subject may suffer damages, he shall immediately inform the data subject in appropriate manner. Such obligation does not exist if the information – taking into consideration that only minor damage to the data subject is likely and the cost of the information to all persons concerned - .would require an inappropriate effort

(3) Where data have not been collected by asking the data subject, but through transmission [Übermittlung] from another application purpose [Aufgabengebiet] of the same controller or from a data application of another controller, the information according to para. 1 may be omitted

1. if the use of data [Datenverwendung] is provided for by law or an ordinance [Verordnung] or
2. if it is impossible to provide the information because the data subjects cannot be reached or

3. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 46 oder Adreßdaten im Rahmen des § 47 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Der Bundeskanzler kann durch Verordnung weitere Fälle festlegen, in welchen die Pflicht zur Information entfällt.

(4) Keine Informationspflicht nach Abs. 1 besteht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 und 3 nicht meldepflichtig sind.

Pflicht zur Offenlegung der Identität des Auftraggebers

§ 25. (1) Bei Übermittlungen und bei Mitteilungen an Betroffene hat der Auftraggeber seine Identität in geeigneter Weise offenzulegen, sodaß den Betroffenen die Verfolgung ihrer Rechte möglich ist. Bei meldepflichtigen Datenanwendungen ist in Mitteilungen an Betroffene die Registernummer des Auftraggebers anzuführen.

(2) Werden Daten aus einer Datenanwendung für Zwecke einer vom Auftraggeber verschiedenen Person verwendet, ohne daß diese ihrerseits ein Verfügungsrecht über die verwendeten Daten und damit die Eigenschaft eines Auftraggebers in Bezug auf die Daten erlangt, dann ist bei Mitteilungen an den Betroffenen neben der Identität der Person, für deren Zwecke die Daten verwendet werden, auch die Identität des Auftraggebers anzugeben, aus dessen Datenanwendung die Daten stammen. Handelt es sich hiebei um eine meldepflichtige Datenanwendung, ist die Registernummer des Auftraggebers beizufügen. Diese Pflicht trifft sowohl den Auftraggeber als auch denjenigen, in dessen Namen die Mitteilung an den Betroffenen erfolgt.

5. Abschnitt
Die Rechte des Betroffenen

Auskunftsrecht

§ 26. (1) Ein Auftraggeber hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist, Auskunft über die zu dieser Person oder Personengemeinschaft verarbeiteten Daten zu geben. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt

3. if, considering the improbability of infringements of the data subjects' rights and the expense involved in reaching the data subjects, an unreasonable effort would be required. In particular, this applies if data are collected for purposes of scientific research or statistics pursuant to § 46 or address data pursuant to § 47 and the requirement to inform the data subject is not explicitly stipulated. The Federal Chancellor may determine further cases by ordinance [Verordnung] in which the duty to give information does not apply.

(4) There shall be no duty to provide information according to para 1 regarding such data applications that are not subject to notification pursuant to § 17 para. 2 and 3.

Obligation to Disclose the Identity of the Controller

§ 25. (1) In the case of transmissions [Übermittlungen] and communications to data subjects [Betroffene], the controller [Auftraggeber] shall disclose his identity in an appropriate manner, so that the data subjects can pursue their rights. In the case of data application [Datenanwendung] subject to notification, communications to the data subject shall carry the controllers registration number.

(2) Where data from a data application are used for purposes of a person other than the controller, without said person receiving a right of disposal and thereby the status of a controller over the used data , the communication to the data subject shall give the identity of the person for whose purposes the data are used as well as the identity of the controller from whose data application the data originate. If this concerns a data application subject to notification, the controller's registration number shall be included in the correspondence. This obligation applies to both the controller and the person in whose name the correspondence to the data subject is communicated.

Part 5
Rights of the Data Subject

Right to Information

§ 26. (1) A controller [Auftraggeber] shall provide any person or group of persons with information about the data being processed about the person or the group of persons who so request in writing and prove his/her identity in an appropriate manner. Subject to the agreement of the controller, the request for information can be made

werden. Die Auskunft hat die verarbeiteten Daten, die Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form anzuführen. Auf Verlangen eines Betroffenen sind auch Namen und Adressen von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft). Mit Zustimmung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des Auskunftswerbers aus besonderen Gründen notwendig ist oder soweit überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten

ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzbehörde nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzbehörde gemäß § 31 Abs. 4.

(3) Der Auskunftswerber hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Auskunftswerber am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z

orally. The information shall contain the processed data, the information about their origin, the recipients or categories of recipients [Empfängerkreise] of transmissions [Übermittlungen], the purpose of the use of data [Datenverwendung] as well as its legal basis in intelligible form. Upon request of a data subject, the names and addresses of processors [Dienstleister] shall be disclosed in case they are charged with processing data relating to him. If no data of the person requesting information exist it is sufficient to disclose this fact (negative information). With the consent of the person requesting information, the information may be provided orally alongside with the possibility to inspect and make duplicates or photocopies instead of being provided in writing.

(2) The information shall not be given insofar as this is essential for the protection of the person requesting information for special reasons or insofar as overriding legitimate interests pursued by the controller or by a third party, especially overriding public interests, are an obstacle to furnishing the information. Overriding public interests can arise out of the necessity

1. to protect of the constitutional institutions of the Republic of Austria or
2. to safeguard of the operational readiness of the federal army or
3. to safeguard the interests of comprehensive national defence or
4. to protect important foreign policy, economic or financial interests of the Republic of Austria or the European Union or
5. to prevent and prosecute crimes.

The right to refuse information for the reasons stated in sub-paras. 1 to 5 is subject to control by the Data Protection Authority [Datenschutzbehörde] pursuant to § 30 para. 3 and the special complaint proceeding before the Data Protection Authority pursuant to § 31 para. 4.

(3) Upon inquiry, the person requesting information has to cooperate in the information procedure to a reasonable extent to prevent an unwarranted and disproportionate effort on the part of the controller.

(4) Within eight weeks of the receipt of the request, the information shall be provided or a reason given in writing why the information is not or not completely provided. The information may be refused if the person requesting information has failed to cooperate in the procedure according to para. 3 or has not reimbursed the cost.

(5) In the areas of the executive responsible for the fields described in para. 2 sub-

1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen:

Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, daß keine der Auskunftspflicht unterliegenden Daten über den Auskunftswerber verwendet werden. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzbehörde nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzbehörde nach § 31 Abs. 4.

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Auskunftswerber im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzbehörde bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten. Diese Frist gilt nicht, wenn einem Löschungsantrag des Auskunftswerbers nach § 27 Abs. 1 Z 2 oder § 28 zu entsprechen ist.

(8) In dem Umfang, in dem eine Datenanwendung für eine Person oder Personengemeinschaft hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, hat diese das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen. Für das Verfahren der Einsichtnahme (einschließlich deren Verweigerung) gelten die näheren Regelungen des Gesetzes, das das Einsichtsrecht vorsieht. In Abs. 1 genannte Bestandteile einer Auskunft, die vom Einsichtsrecht nicht umfasst sind, können dennoch nach diesem Bundesgesetz geltend gemacht werden.

(9) Für Auskünfte aus dem Strafregister gelten die besonderen Bestimmungen des Strafregistergesetzes 1968 über Strafregisterbescheinigungen.

(10) Ergibt sich eine Auftraggeberstellung auf Grund von Rechtsvorschriften, obwohl die Datenverarbeitung für Zwecke der Auftragserfüllung für einen Dritten

para. 1 to 5, the procedure in a case where public interests require that no information be given shall be as follows:

In all cases where no information is given even when in fact no data on the person requesting information is used instead of giving a reason in substance, an indication shall be given that no data are being used which are subject to the right to information. The legality of such course of action is subject to review by the Data Protection Authority [Datenschutzbehörde] pursuant to § 30 para. 3 and the special complaint proceeding before the Data Protection Authority pursuant to § 31 para. 4.

(6) The information shall be given free of charge if it concerns the current data files [Daten¬bestand] of a use of data and if the person requesting information has not yet made a request for information to the same controller regarding the same application purpose [Aufgabengebiet] in the current year. In all other cases a flat rate compensation of 18,89 Euro may be charged; deviations are permitted to cover actually incurred higher expenses. A compensation already paid shall be refunded, irrespective of any claims for damages, if data have been used illegally or if the information has otherwise led to a correction.

(7) As of the moment the controller has knowledge of a request for information, the controller shall not erase the data relating to the person requesting information until four months have passed or in case a complaint is lodged with the Data Protection Authority pursuant to § 31, until the final conclusion of the proceedings. This deadline does not apply if a request for deletion by the person requesting information according to § 27 para 1 sub-para. 2 or § 28 is to be complied with.

(8) To the extent a data application [Daten¬anwendung] is by law open to inspection by a person or group of persons with regard to data processed on them they shall have the right to information in accordance with the provisions providing the right to inspect. To the procedure of inspection (and its refusal) the regulations of the law providing the right of inspection are to be applied. Parts of an information according ton para 1 that are not covered by the right of inspection may, however, be asserted according to this federal law.

(9) For information on Criminal Records [Strafregister], the special regulations of the Criminal Records Act 1968 [Strafregistergesetz 1968] shall apply.

(10) In case legal provisions lead to a qualification as controller, though the data are processed for a third party in order to carry out a job (§ 4 para 1 sub-para. 4 last

erfolgt (§ 4 Abs. 1 Z 4 letzter Satz), kann der Auskunftswerber sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Auskunftswerber, soweit ihm dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des tatsächlichen Auftraggebers mitzuteilen, damit der Auskunftswerber sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann. Wird ein Auskunftsbegehren an einen Dienstleister gerichtet und lässt dieses erkennen, dass der Auskunftswerber ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Dienstleister das Auskunftsbegehren unverzüglich an den Auftraggeber weiterzuleiten und dem Auskunftswerber mitzuteilen, dass in seinem Auftrag keine Daten verwendet werden. Der Auftraggeber hat innerhalb von acht Wochen ab Einlangen des Auskunftsbegehrens beim Dienstleister dem Auskunftswerber Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, von einer Auskunftserteilung abzusehen. Wird jedoch in weiterer Folge das Ersuchen direkt an den Auftraggeber gestellt, so hat dieser nach Abs. 5 vorzugehen. Für Betreiber von Informationsverbundsystemen gilt jedoch ausschließlich § 50 Abs. 1.

Recht auf Richtigstellung oder Löschung

§ 27. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder
2. auf begründeten Antrag des Betroffenen.

Der Pflicht zur Richtigstellung nach Z 1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§ 46 und 47.

sentence), the person requesting information may also first direct the request for information to the entity that ordered the job. This entity has to provide the person requesting information, to the extent the one does not know already, with the name and address of the effective controller within two weeks, free of costs, so that the person requesting information may assert his right of information according to para 1 against him. In case a request for information is directed to a service provider and is obvious that the person requesting information mistakes him for the controller of the data application operated by him, the service provider shall forward the request for information immediately to the controller and to inform the person requesting information, that no data are processed by him as controller. Within eight weeks after the request for information has been received by the service provider the controller has to grant information to the person requesting information or argue in writing, for which reason it is not granted or not completely. In those sectors of public administration what are charged to implement the functions named in para 2 sub-para. 1 to 5, information shall not be given to the extent necessary for the protection of public interests. If, subsequently, the request is directed to the controller, such has to act according to para 5. To operators of joint information systems § 50 para 1 is to be applied exclusively.

Right to Rectification and Erasure

§ 27. (1) Every controller shall rectify or erase data that are incorrect or have been processed contrary to the provisions of this Federal Act [Bundesgesetz]

1. on his own, as soon the incorrectness of the data or the inadmissibility of the processing becomes know to him, or
2. on a well founded application by the data subject [Betroffener].

The obligation to rectify data according to sub-para. 1 shall apply only to those data whose correctness is significant for the purpose of the data application [Datenanwendung]. The incompleteness of data shall only justify a claim to rectification if the incorrectness, with regard to the purpose of the data application, results in the entire information being incorrect. As soon as data are no longer needed for the purpose of the data application, they shall be regarded as illegally processed data and shall be erased unless their archiving is legally permitted and unless the access to these data is specially secured. Any further use for another purpose shall be legitimate only if a transmission [Übermittlung] of the data for this purpose is legitimate; the legitimacy of further uses for scientific or statistical purposes is laid down in sects. 46 and 47.

(2) Der Beweis der Richtigkeit der Daten obliegt - sofern gesetzlich nicht ausdrücklich anderes angeordnet ist - dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

(3) Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zuläßt. Die erforderlichen Richtigstellungen sind diesfalls durch entsprechende zusätzliche Anmerkungen zu bewirken.

(4) Innerhalb von acht Wochen nach Einlangen eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in § 26 Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Geheimhaltung erfordern, mit einem Richtigstellungs- oder Löschungsantrag folgendermaßen zu verfahren: Die Richtigstellung oder Löschung ist vorzunehmen, wenn das Begehren des Betroffenen nach Auffassung des Auftraggebers berechtigt ist. Die gemäß Abs. 4 erforderliche Mitteilung an den Betroffenen hat in allen Fällen dahingehend zu lauten, daß die Überprüfung der Datenbestände des Auftraggebers im Hinblick auf das Richtigstellungs- oder Löschungsbegehren durchgeführt wurde. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzbehörde nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzbehörde nach § 31 Abs. 4.

(6) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

(7) Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet, und läßt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzbehörde gelöscht werden.

(8) Wurden im Sinne des Abs. 1 richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Auftraggeber die Empfänger

(2) It shall be the obligation of the controller to prove that the data are correct unless specifically provided otherwise by law insofar as the data have not been collected exclusively based on statements made by the data subject.

(3) No rectification or erasure of data is possible insofar as the documentation purpose of a data application does not permit later changes. In such case, the necessary rectifications shall be effected by means of additional comments.

(4) The application for rectification or erasure shall be complied with within eight weeks after receipt and the applicant shall be informed thereof, or a reason in writing shall be given why the requested erasure or rectification was not carried out.

(5) In the areas of the executive responsible for the fields described in § 26 para. 2 sub paras. 1 to 5, the following procedure shall be applied to applications for rectification or erasure, insofar as this is required to safeguard those public interests that require secrecy: The rectification or erasure shall be carried out if the demands of the data subject are justified in the opinion of the controller. The required information pursuant to para. 4 shall in all cases be that a check of the data files [Datenbestand] of the controller with regard to the application for rectification or erasure has been performed. The legality of this course of action is subject to review by the Data Protection Authority [Datenschutzbehörde] according to § 30 para. 3 and the special complaint proceeding before the Data Protection Authority pursuant to § 31 para. 4.

(6) If the erasure or rectification of data kept solely on media readable by means of automatic processing systems can be carried out only at specific times for economic reasons, the data to be erased shall be kept inaccessible and a correcting remark shall be attached the data that are to be corrected.

(7) If data are used whose correctness is disputed by the data subject, and if neither their correctness or incorrectness can be established, an entry about the dispute [Bestreitungsvermerk] shall be attached upon request by the data subject. The entry about the dispute shall be erased only with the consent of the data subject or on grounds of a decision of the competent court of law or of the Data Protection Authority.

(8) If data that were rectified or erased in terms of para. 1 were transmitted before having been rectified or erased, the controller shall inform the recipient of the data by

dieser Daten hievon in geeigneter Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere im Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.

(9) Die Regelungen der Abs. 1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für öffentliche Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für

1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder
2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschungsanträge von Betroffenen

durch Bundesgesetz nicht anderes bestimmt ist.

Widerspruchsrecht

§ 28. (1) Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen.

(2) Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datenanwendung kann der Betroffene jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben. Die Daten sind binnen acht Wochen zu löschen.

(3) § 27 Abs. 4 bis 6 gelten auch in den Fällen der Abs. 1 und 2.

Die Rechte des Betroffenen bei der Verwendung nur indirekt personenbezogener Daten

§ 29. Die durch die §§ 26 bis 28 gewährten Rechte können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.

appropriate means, insofar as this does not constitute an unreasonable effort, in particular with regard to a legitimate interest in the information, and that the recipient can still be determined.

(9) The provisions of para. 1 to 8 shall be applied to the criminal records [Strafregister], kept according to the Criminal Records Act 1968 [Strafregistergesetz 1968] as well as to public books and registers kept by public sector controllers only insofar as

1. the obligation to rectification and erasure ex officio or
2. the procedure to assert and the competence to decide applications to rectification and erasure of data subjects

is not regulated otherwise by federal law.

Right to Object

§ 28. (1) Insofar as a use of data [Datenverwendung] is not authorised by law, every data subject [Betroffener] shall have the right to raise an objection with the controller [Auftraggeber] of the data application [Datenanwendung] against the use of data because of an infringement of an overriding interest in secrecy deserving protection arising from his special situation. If the requirements are met, the controller shall erase the data relating to the data subject within eight weeks from his data application and shall refrain from transmitting the data.

(2) If the inclusion of data in a data application open to inspection by the public is not mandated by law, the data subject can object at any time and without any need to give reasons for his desire. The data shall be erased within eight weeks.

(3) § 27 para 4 to 6 shall also be applied in the cases of paras 1 and 2.

Rights of the Data Subject concerning the Use of only Indirectly Personal Data

§ 29. The rights granted in sects. 26 to 28 cannot be exercised insofar as only indirectly personal data are used.

6. Abschnitt
Rechtsschutz

Kontrollbefugnisse der Datenschutzbehörde

§ 30. (1) Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzbehörde wenden.

(2) Die Datenschutzbehörde kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hiebei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.

(2a) Sofern sich eine zulässige Eingabe nach Abs. 1 oder ein begründeter Verdacht nach Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzbehörde die Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorgehen.

(3) Datenanwendungen, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dies gilt auch für jene Bereiche der Vollziehung, in welchen ein Auftraggeber des öffentlichen Bereichs die grundsätzliche Anwendbarkeit der §§ 26 Abs. 5 und 27 Abs. 5 in Anspruch nimmt.

(4) Zum Zweck der Einschau ist die Datenschutzbehörde nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen. Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

(5) Informationen, die der Datenschutzbehörde oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der

Part 6
Legal Remedies

Duties of Supervision of the Data Protection Authority

§ 30. (1) Anyone shall have the right to lodge an application with the Data Protection Authority [Daten¬schutz¬behörde] because of an alleged infringement of his rights or obligations concerning him pursuant to this Federal Act [Bundesgesetz] by a controller [Auftraggeber] or processor [Dienstleister].

(2) The Data Protection Authority shall have the right to examine data applications [Daten¬anwendungen] in case of reasonable suspicion of an infringement of the rights and obligations mentioned in para. 1. 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 relevant documents.

(2a) In case an application admissible according to para 1 or a reasonable suspicion according to para 2 refers to a data application (filing system) subject to the obligation of notification, the Data Protection Authority may examine whether the notification obligation has been fulfilled and eventually proceed according to §§ 22 and 22a.

(3) Data applications subject to prior checking [Vorabkontrolle] pursuant to § 18 para. 2 may be examined without a suspicion of illegal data use. The same applies to those fields of the government where a public sector controller claims that sects. 26 para. 5 and 27 para. 5 are to be applied.

(4) For purposes of the inspection, the Data Protection Authority shall have the right, after having informed the owner of said rooms and the controller (processor), to enter rooms where data applications are carried out, operate data processing equipment, run the processing to be examined and to make copies of the storage media to the extent absolutely required for the exercise of the right to examination. The controller (processor) shall render the assistance necessary for the examination. The supervisory rights are to be exercised in a way that least interferes with the rights of the controller (processor) and third parties.

(5) Information acquired by the Data Protection Authority or its representatives during any examination shall be used only for supervisory purposes in the context of

Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Dazu zählt auch die Verwendung für Zwecke der gerichtlichen Rechtsverfolgung durch den Einschreiter oder die Datenschutzbehörde nach § 32. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes, einer strafbaren Handlung nach den §§ 118a, 119, 119a, 126a bis 126c, 148a oder § 278a des Strafgesetzbuches, BGBl. Nr. 60/1974, oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozessordnung, BGBl. Nr. 631/1975, zu entsprechen ist.

(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzbehörde, sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach Abs. 6a zu treffen sind, Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzbehörde je nach der Art des Verstoßes von Amts wegen insbesondere

1. Strafanzeige nach §§ 51 oder 52 erstatten, oder
2. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder
3. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzbehörde entsprochen wird, oder der Datenschutzbehörde mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzbehörde der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.

(6a) Liegt durch den Betrieb einer Datenanwendung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51, untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Wird einer Untersagung nicht sogleich Folge geleistet, ist Strafanzeige nach § 52 Abs. 1 Z 3 zu erstatten. Nach Rechtskraft einer Untersagung nach diesem Absatz ist ein

the execution of data protection regulations. This includes the use for purposes of litigation at courts by the person involved or the Data Protection Authority according to § 22. Incidentally, the obligation to confidentiality also exists before courts and administrative authorities, in particular fiscal authorities, with the reservation that, if the examination leads to probable cause to believe that a crime according to sects. 51 and 52 of this Federal Act [Bundesgesetz] or a criminal act according to §§ 118a, 119, 119a, 126a to 126c, 148a or §278a of the Criminal Code, Federal Law Gazette No. 60/1974, or any crime punishable with more than five years of imprisonment has been committed, a report shall be made and requests for assistance according to § 76 Code of Criminal Procedure, Federal Law Gazette No. 631/1974 regarding such crimes and offences shall be complied with.

(6) To establish the rightful state, the Data Protection Authority can issue recommendations, unless measures according to §§ 22 and 22a or para 6a are to be taken an appropriate period for compliance shall be set if required. If a recommendation is not obeyed within the set period, the Data Protection Authority shall, depending on the kind of transgression and ex officio,

1. bring a criminal charge pursuant to sects. 51 or 52, or
2. in case of severe transgressions by a private sector controller file a lawsuit before the competent court of law pursuant to § 32 para. 5, or
3. in case of a transgression by an organ of a territorial corporate body [Gebietskörperschaft], involve the competent highest authority. This authority shall within an appropriate period, not exceeding twelve weeks, take measures to ensure that the recommendation of the Data Protection Authority is complied with or inform the Data Protection Authority why the recommendation is not complied with. The reason may be publicised by the Data Protection Commission in an appropriate manner as far as not contrary to official secrecy.

(6a) In case the operation of a data application causes an serious and immediate danger to interests of secrecy of the data subject deserving protection (imminent danger) the Data Protection Authority may prohibit the continuation of the data application by ruling in accordance with § 57 para. 1 of the General Administrative Act 1991 - AVG, Federal Law Gazette No. 51/1991. The continuation may also be prohibited only partially if this technically possible, gives a meaningful result with regard to the purpose of the data application and is sufficient to eliminate the risk. If the ban is not complied with the offence is to be reported according to § 52 para 1 sub-para 3. If a ban under this para has become final, any running procedure for correction according to

Berichtigungsverfahren nach § 22a Abs. 2 formlos einzustellen. Die Datenanwendung ist im Umfang der Untersagung aus dem Register zu streichen.

(7) Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde.

Beschwerde an die Datenschutzbehörde

§ 31. (1) Die Datenschutzbehörde erkennt über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Auskunft nach § 26 oder nach § 50 Abs. 1 dritter Satz oder in ihrem Recht auf Darlegung einer automatisierten Einzelentscheidung nach § 49 Abs. 3 verletzt zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Die Datenschutzbehörde erkennt weiters über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Geheimhaltung (§ 1 Abs. 1) oder in ihrem Recht auf Richtigstellung oder auf Löschung (§§ 27 und 28) verletzt zu sein, sofern der Anspruch nicht nach § 32 Abs. 1 vor einem Gericht geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet.

(3) Die Beschwerde hat zu enthalten:

1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner),
3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,
4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

(4) Einer Beschwerde nach Abs. 1 sind außerdem das zu Grunde liegende Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) und eine allfällige Antwort des Beschwerdegegners anzuschließen. Einer Beschwerde nach Abs. 2 sind außerdem der zu Grunde liegende Antrag auf Richtigstellung oder Löschung und eine allfällige Antwort des Beschwerdegegners anzuschließen.

§ 22a para 2 is to be discontinued informally. According to the extent of the ban the data application is to be deleted from the register.

(7) The intervening party shall be informed as to how his intervention was dealt with.

Complaint before the Data Protection Authority

§ 31. (1) The Data Protection Authority [Datenschutzbehörde] shall decide on complaints of persons or group of persons who allege to have been infringed in their right for information according to § 26 or § 50 para 1 third phrase or in their right to be informed about an automatically processed individual decision according to § 49 para 3 insofar as the request for information (the application for information or disclosure) does not concern the use of data [Datenverwendung] for acts in the service of legislation or jurisdiction.

(2) Furthermore, the Data Protection Authority shall decide on complaints of persons or groups of persons who allege to have been infringed in their right to secrecy (§ 1 para 1) or in their right to correction or deletion (§§ 27 and 28), to the extent the right is not to be asserted under § 32 para 1 before a court or is not directed against an organ in the service of legislation or jurisdiction.

(3) The complaint must contain:

1. the description of the right considered to be infringed,
2. to the extent reasonable, the description of the legal entity or the organ, which is deemed to be responsible for the alleged infringement (opponent of the complaint),
3. the facts from which the infringement is derived,
4. the reasons for which the unlawfulness is alleged,
5. the request to determine the alleged infringement and
6. the details which are necessary in order to decide whether the complaint has been filed in due time.

(4) A complaint according to para 1 must be accompanied by the pertinent request for information (the application for information or presentation) and an reply by the opponent to the complaint, if any. A complaint according to para 2 must be accompanied by the pertinent request for correction or deletion and an answer of the opponent to the complaint, if any.

(5) Die der Datenschutzbehörde durch § 30 Abs. 2 bis 4 eingeräumten Kontrollbefugnisse kommen ihr auch in Beschwerdeverfahren nach Abs. 1 und 2 gegenüber dem Beschwerdegegner zu. Ebenso besteht auch hinsichtlich dieser Verfahren die Verschwiegenheitspflicht nach § 30 Abs. 5.

(6) Im Fall der Einbringung einer zulässigen Beschwerde nach Abs. 1 oder 2 ist ein auf Grund einer Eingabe nach § 30 Abs. 1 über denselben Gegenstand eingeleitetes Kontrollverfahren durch eine entsprechende Information (§ 30 Abs. 7) zu beenden. Die Datenschutzbehörde kann aber dennoch auch während der Anhängigkeit des Beschwerdeverfahrens von Amts wegen nach § 30 Abs. 2 vorgehen, wenn ein begründeter Verdacht einer über den Beschwerdefall hinausgehenden Verletzung datenschutzrechtlicher Verpflichtungen besteht. § 30 Abs. 3 bleibt unberührt.

(7) Soweit sich eine Beschwerde nach Abs. 1 oder 2 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte Verletzung im Recht auf Auskunft (Abs. 1) einem Auftraggeber des privaten Bereichs zuzurechnen, so ist diesem auf Antrag zusätzlich die – allenfalls erneute – Reaktion auf das Auskunftsbegehren nach § 26 Abs. 4, 5 oder 10 in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen.

(8) Ein Beschwerdegegner, gegen den wegen Verletzung in Rechten nach den §§ 26 bis 28 Beschwerde erhoben wurde, kann bis zum Abschluss des Verfahrens vor der Datenschutzbehörde durch Reaktionen gegenüber dem Beschwerdeführer gemäß § 26 Abs. 4 oder § 27 Abs. 4 die behauptete Rechtsverletzung nachträglich beseitigen. Erscheint der Datenschutzbehörde durch derartige Reaktionen des Beschwerdegegners die Beschwerde als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzbehörde das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 13 Abs. 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen. Auch diesfalls ist das ursprüngliche Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen.

Begleitende Maßnahmen im Beschwerdeverfahren

§ 31a. (1) Sofern sich eine zulässige Beschwerde nach § 31 Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzbehörde die

(5) The control rights granted to the Data Protection Authority according to § 30 paras 2 to 4 also apply to the complaint procedure according to para 1 and 2 vis-a-vis the opponent to the complaint. Also, the duty of confidentiality according to § 30 para 5 applies to this procedure.

(6) In case of filing of an admissible complaint according to paras 1 or 2 a control procedure instituted on an application based on § 30 para 1 on the same issue is to be discontinued merely by giving information (§ 30 para 7). Nevertheless, the Data Protection Authority may proceed even when the complaint procedure is pending ex officio according to § 30 para 2, if reasonable suspicion exists on an infringement of obligations under the data protection provisions beyond the case of complaint. § 30 para 3 remains unaffected.

(7) To the extent a complaint according to paras 1 or 2 is shown to be justified, it is to be granted and the infringement to be stated. If a stated infringement of the right of information (para 1) falls under the responsibility of a controller in the private sector, he/she, upon request, in addition, is to be instructed to give - again - an answer to the request for information according to § 26 para 4, 5 or 10, in the extent required, to eliminate the infringement having been stated. To the extent the complaint is not found to be justified, it is to be rejected.

(8) An opponent against whom a complaint has been filed for infringement of rights according to §§ 26 to 28, may, till the end of the proceedings before the data protection commission, by communicating with the complaining person according to § 26 para 4 or § 27 para 5, subsequently eliminate the alleged infringement. If the data protection commission deems the complaint to be settled by such reactions of the opponent to the complaint, it shall hear the person complaining on this. Simultaneously he/she is to be informed, that the Data Protection Authority will informally end the procedure, if he/she does not establish within an adequate period, for which reason he/she still does not consider the originally alleged infringement to be eliminated at least partially. If such answer of the person complaining modifies the merits of the case (§ 13 para 8 General Administrative Act) the original complaint is to be deemed withdrawn and simultaneously a new complaint to be deemed filed. In this case the original complaint procedure is also to be ended informally and the person complaining to be informed correspondingly. Belated answers are to be ignored.

Accompanying measures in the complaint procedure

§ 31a. (1) In so far an admissible complaint according to § 31 para 2 refers to a data application subject to the obligation of notification, the Data Protection Authority

Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorgehen.

(2) Macht der Beschwerdeführer im Rahmen einer Beschwerde nach § 31 Abs. 2 eine wesentliche Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen durch die Verwendung seiner Daten glaubhaft, so kann die Datenschutzbehörde nach § 30 Abs. 6a vorgehen.

(3) Ist in einem Verfahren nach § 31 Abs. 2 die Richtigkeit von Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen. Erforderlichenfalls hat dies die Datenschutzbehörde auf Antrag des Beschwerdeführers mit Mandatsbescheid anzuordnen.

(4) Beruft sich ein Auftraggeber des öffentlichen Bereichs bei einer Beschwerde wegen Verletzung des Auskunfts-, Richtigstellungs- oder Löschungsrechts gegenüber der Datenschutzbehörde auf die §§ 26 Abs. 5 oder 27 Abs. 5, so hat diese nach Überprüfung der Notwendigkeit der Geheimhaltung die geschützten öffentlichen Interessen in ihrem Verfahren zu wahren. Kommt sie zur Auffassung, dass die Geheimhaltung von verarbeiteten Daten gegenüber dem Betroffenen nicht gerechtfertigt war, ist die Offenlegung der Daten mit Bescheid aufzutragen. Wurde keine Beschwerde erhoben und wird dem Bescheid der Datenschutzbehörde binnen acht Wochen nicht entsprochen, so hat die Datenschutzbehörde die Offenlegung der Daten gegenüber dem Betroffenen selbst vorzunehmen und ihm die verlangte Auskunft zu erteilen oder ihm mitzuteilen, welche Daten bereits berichtigt oder gelöscht wurden. Die ersten beiden Sätze gelten in Verfahren nach § 30 sinngemäß.

Anrufung der Gerichte

§ 32. (1) Ansprüche wegen Verletzung der Rechte einer Person oder Personengemeinschaft auf Geheimhaltung, auf Richtigstellung oder auf Löschung gegen natürliche Personen, Personengemeinschaften oder Rechtsträger, die in Formen des Privatrechts eingerichtet sind, sind, soweit diese Rechtsträger bei der behaupteten Verletzung nicht in Vollziehung der Gesetze tätig geworden sind, auf dem Zivilrechtsweg geltend zu machen.

(2) Sind Daten entgegen den Bestimmungen dieses Bundesgesetzes verwendet worden, so hat der Betroffene Anspruch auf Unterlassung und Beseitigung des diesem Bundesgesetz widerstreitenden Zustandes.

(3) Zur Sicherung der auf dieses Bundesgesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die in

may examine whether the obligation for notification has been fulfilled and eventually proceed according to §§ 22 and 22a.

(2) If the person complaining establishes a prima facie case of serious infringement to his/her interests for confidentiality deserving protection within the frame of a complaint according ot § 31 para 2 by use of his/her data, the Data Protection Authority may proceed according to § 30 para 6a.

(3) If in a proceeding according to § 31 para 2 the correctness of data is controversial, the opponent to the complaint shall place a note of the dispute [Bestreitungsvermerk] till the proceedings are terminated. If necessary, upon request of the person complaining, the Data Protection Authority shall order this done by provisional rulings.

(4) If a public sector controller invokes sects. 26 para. 5 or 27 para. 5 before the Data Protection Authority concerning a complaint because of an infringement of the rights to information, rectification and erasure, the Data Protection Authority shall, after having examined the necessity of confidentiality, safeguard the protected public interests during the proceedings. If the Data Protection Authority comes to the conclusion that it was not justified to keep the processed data secret from the data subject, the disclosure of the data shall be ordered by a ruling [Bescheid]. If no appeal is made and the ruling [Bescheid] of the Data Protection Authority is not complied within eight weeks, the Data Protection Authority itself shall carry out the disclosure to the data subject and shall communicate to him the desired information or inform him which data have been rectified or erased. In proceedings according to § 30 the first two sentences are to be applied accordingly.

Court Action

§ 32. (1) Claims for infringement of the rights of a person or a group of persons to secrecy, rectification and erasure against natural persons, groups of persons or legal entities established in forms of private law, are, as long as such legal entities were not acing to enforce laws when their rights were infringed, shall be brought before the civil courts.

(2) If data have been used contrary to the provisions of this Federal Act [Bundesgesetz], the data subject shall have the right to sue for an end to such unlawful condition.

(3) In order to safeguard the legal right to put an end to an unlawful state an injunction may be issued even if the requirements mentioned in § 381 Foreclosure Act

§ 381 EO bezeichneten Voraussetzungen nicht zutreffen. Dies gilt auch für Verfügungen über die Verpflichtung zur Anbringung eines Bestreitungsvermerks.

(4) Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.

(5) Die Datenschutzbehörde hat in Fällen, in welchen der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, gegen diesen eine Feststellungsklage (§ 228 ZPO) bei dem gemäß Abs. 4 zweiter Satz zuständigen Gericht zu erheben.

(6) Die Datenschutzbehörde hat, wenn ein Einschreiter (§ 30 Abs. 1) es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von natürlichen Personen geboten ist, einem Rechtsstreit auf Seiten des Einschreiters als Nebenintervenient (§§ 17 ff ZPO) beizutreten.

(7) Anlässlich einer zulässigen Klage nach Abs. 1, die sich auf eine nach Ansicht des Gerichts meldepflichtige Datenanwendung bezieht, kann das Gericht die Datenschutzbehörde um Überprüfung nach den §§ 22 und 22a ersuchen. Die Datenschutzbehörde hat das Gericht vom Ergebnis der Überprüfung zu verständigen. Dieses ist sodann vom Gericht auch den Parteien bekannt zu geben, sofern das Verfahren noch nicht rechtskräftig beendet ist.

Schadenersatz

§ 33. (1) Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Werden durch die öffentlich zugängliche Verwendung der in § 18 Abs. 2 Z 1 bis 3 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs. 1 des Mediengesetzes, BGBl. Nr. 314/1981, gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen.

are not fulfilled. This also applies to orders to make a note about the dispute [Bestreitungsvermerk].

(4) Complaints and applications for injunctions pursuant to this Federal Act shall in the first instance be lodged with the regional civil court [Landesgericht] in whose district the plaintiff (applicant) has his domicile or seat. Actions (applications) may, however, also be brought before the regional civil court in whose district the defendant has his domicile or seat or branch office.

(5) The Data Protection Authority [Datenschutzbehörde] shall, in a case where there is probable cause to believe that a serious data protection infringement has been committed by a private sector controller, file an action for a declaratory judgement (§ 228 Code of Civil Procedure) [Feststellungsklage] in the court that is competent pursuant to para. 4 second sentence.

(6) On request of an intervening party (§ 30 para 1) the Data Protection Authority shall, if such action appears necessary to safeguard the protected interests of a large number of natural persons pursuant to this Federal Act, intervene in the proceedings in support of the intervening party as an intervening third party [Nebenintervenient] (§§ 17 et seq. of the Code of Civil Procedure).

(7) At the occasion of an admissible claim according to para 1 referring to a data application subject to the obligation of notification according to the view of the court, the court may request the Data Protection Authority for a review according to §§ 22 and 22a. The Data Protection Authority shall inform the court about the result of the review. The result is then to be notified by the court also to the parties, insofar as the proceedings have not been decided finally.

Damages

§ 33. (1) A controller [Auftraggeber] or processor [Dienstleister] who has culpably used data contrary to the provisions of this Federal Act [Bundesgesetz], shall indemnify the data subject [Betroffener] pursuant to the general provisions of civil law. If data falling under the categories listed in § 18 para. 2 no. 1 to 3 are publicly used in a manner that violates a data subjects' interests in secrecy deserving protection that is suitable to expose that person in a like manner to § 7 para. 1 of the Media Act, Federal Law Gazette No. 314/1981, that provision shall be applied even if the public use of data [Datenverwendung] is not committed by publication in the media. The claim for appropriate compensation for the defamation suffered shall be brought against the controller of the data used.

(2) Der Auftraggeber und der Dienstleister haften auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

(3) Der Auftraggeber kann sich von seiner Haftung befreien, wenn er nachweist, daß der Umstand, durch den der Schaden eingetreten ist, ihm und seinen Leuten (Abs. 2) nicht zur Last gelegt werden kann. Dasselbe gilt für die Haftungsbefreiung des Dienstleisters. Für den Fall eines Mitverschuldens des Geschädigten oder einer Person, deren Verhalten er zu vertreten hat, gilt § 1304 ABGB.

(4) Die Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 32 Abs. 4.

Gemeinsame Bestimmungen

§ 34. (1) Der Anspruch auf Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32 erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist dem Einschreiter im Falle einer verspäteten Eingabe gemäß § 30 mitzuteilen; verspätete Beschwerden nach § 31 und Klagen nach § 32 sind zurückzuweisen.

(2) Eingaben nach § 30, Beschwerden nach § 31, Klagen nach § 32 sowie Schadenersatzansprüche nach § 33 können nicht nur auf die Verletzung der Vorschriften dieses Bundesgesetzes, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaates der Europäischen Union gegründet werden, soweit solche Vorschriften gemäß § 3 im Inland anzuwenden sind.

(3) Ist ein von der Datenschutzbehörde zu prüfender Sachverhalt gemäß § 3 nach der Rechtsordnung eines anderen Vertragsstaates des Europäischen Wirtschaftsraumes zu beurteilen, so kann die Datenschutzbehörde die zuständige ausländische Datenschutzkontrollstelle um Unterstützung ersuchen.

(4) Die Datenschutzbehörde hat den Unabhängigen Datenschutzkontrollstellen der anderen Vertragsstaaten des Europäischen Wirtschaftsraumes über Ersuchen Amtshilfe zu leisten.

(2) The controller or processor shall also be liable for damage caused by their staff, insofar as their action was casual for the damage.

(3) The controller shall be free from liability if he can prove that the circumstances which caused the damage cannot be attributed to him or his staff (para. 2). This also applies to the exclusion of the processors' liability. In the case of contributory negligence on the part of the injured party or a person for whose conduct the injured party is responsible, § 1304 ABGB [Note: The AGBG is the basic Austrian codex on civil law.] shall apply.

(4) Lawsuits according to para. 1 shall be brought before the court that is competent according to § 32 para. 4.

Common Provisions

§ 34. (1) The right to lodge an application according to § 30, a complaint according to § 31 or legal action according to § 32 and claims for damages according to § 33 shall apply only if the charge is filed by the intervening party within a year after having gained knowledge of the incident that gave rise to the complaint and no later than three years after the alleged incident. This is to be communicated to the intervening party in the case of a late application according to § 30; late complaints according to § 31 or legal actions according to § 32 shall be rejected.

(2) Applications according to § 30, complaints according to § 31 or legal action according to § 32 and claims for damages according to § 33 can be filed not only because of an alleged infringement of this Federal Act [Bundesgesetz], but also based on an infringement of data protection provisions of another member state of the European Union, insofar as these provisions are applicable in Austria according to § 3.

(3) If a case to be adjudicated by the Data Protection Authority by applying the national provisions of another member state of the European Economic Area pursuant to § 3, the Data Protection Authority [Datenschutzbehörde] shall ask the competent foreign supervisory authority for assistance.

(4) The Data Protection Authority shall render inter-authority assistance [Amtshilfe] to the independent supervisory authorities of the signatory states of the European Economic Area upon request.

7. Abschnitt
Kontrollorgane

Datenschutzbehörde und Datenschutzrat

§ 35. (1) Zur Wahrung des Datenschutzes sind nach den näheren Bestimmungen dieses Bundesgesetzes – unbeschadet der Zuständigkeit des Bundeskanzlers und der ordentlichen Gerichte – die Datenschutzbehörde und der Datenschutzrat berufen.

(2) **(Verfassungsbestimmung)** Die Datenschutzbehörde übt ihre Befugnisse auch gegenüber den in Art. 19 B VG bezeichneten obersten Organen der Vollziehung aus.

Einrichtung der Datenschutzbehörde

§ 36. (1) Der Datenschutzbehörde steht ein Leiter vor. Dieser wird vom Bundespräsidenten auf Vorschlag der Bundesregierung für eine Dauer von fünf Jahren bestellt; die Wiederbestellung ist zulässig. Dem Vorschlag hat eine Ausschreibung zur allgemeinen Bewerbung voranzugehen. Die Ausschreibung ist vom Bundeskanzler zu veranlassen. Die Funktion des Leiters der Datenschutzbehörde ist auf der beim Bundeskanzleramt eingerichteten Website „Karriere Öffentlicher Dienst“ auszuschreiben. Die Ausschreibung ist zusätzlich im „Amtsblatt zur Wiener Zeitung“ kundzumachen.

(2) Der Leiter der Datenschutzbehörde hat

1. das Studium der Rechtswissenschaften oder die rechts- und staatswissenschaftlichen Studien abgeschlossen zu haben,
2. die persönliche und fachliche Eignung durch eine entsprechende Vorbildung und einschlägige Berufserfahrung in den von der Datenschutzbehörde zu besorgenden Angelegenheiten aufzuweisen,
3. überausgezeichnete Kenntnisse des österreichischen Datenschutzrechtes, des Unionsrechtes und der Grundrechte zu verfügen und
4. übereine mindestens fünfjährige juristische Berufserfahrung zu verfügen.

(3) Zum Leiter der Datenschutzbehörde dürfen nicht bestellt werden:

Part 7
Control Bodies

Data Protection Authority and Data Protection Council

§ 35. (1) The Data Protection Authority [Datenschutzbehörde] and the Data Protection Council [Datenschutzrat] shall safeguard data protection in accordance with the regulations of this Federal Act [Bundesgesetz] without prejudice to the competence of the Federal Chancellor [Bundeskanzler] and the courts of law.

(2) **(Constitutional provision)** The Data Protection Authority shall exercise its functions vis-á-vis the highest executive authorities enumerated in Art. 19 B-VG.

Establishment of the Data Protection Authority

§ 36. (1) The Data Protection Autority [Datenschutzbehörde] is managed by its head. He is appointed for a term of five years by the Federal President [Bundespräsident] on a proposal of the Federal Government [Bundesregierung]; re-appointments are permitted. The proposal is to be preceded by an advertisment for the position, which permits general applications. The advertisement for the position falls under the responsibility of the Federal Chancellor. The position of the head of the data protection authority shall be advertised on the public career website of the Federal Chancellery [Bundeskanzleramt]. The position shall also be advertised in the official journal “Wiener Zeitung”[1].

(2) The head of the data protection authority [Datenschutzbehörde] must

1. have completed his study of law and political science,
2. have the necessary personal and professional aptitude through prior education and appropriate professional experience in the matters to be handled by the Data Protection Authority,
3. possess excellent knowledge of Austrian data protection law, European Union law and fundamental rights and
4. have at least five years of professional experience in the legal field.

(3) The following persons may not be appointed head of the Data Protection

1 The "Wiener Zeitung" is a regular newspaper which also serves as the official journal of the Austrian Federal government.

1. Mitglieder der Bundesregierung, Staatssekretäre, Mitglieder einer Landesregierung, Mitglieder des Nationalrates, des Bundesrates oder sonst eines allgemeinen Vertretungskörpers oder des Europäischen Parlaments, ferner Volksanwälte und der Präsident des Rechnungshofes,

2. Personen, die eine der in der Z 1 genannten Funktionen innerhalb der letzten zwei Jahre ausgeübt haben, und

3. Personen, die von der Wählbarkeit in den Nationalrat ausgeschlossen sind.

(4) Der Leiter der Datenschutzbehörde darf für die Dauer seines Amtes keine Tätigkeit ausüben, die Zweifel an der unabhängigen Ausübung seines Amtes oder die Vermutung einer Befangenheit hervorrufen könnte oder die ihn an der Erfüllung seiner dienstlichen Aufgaben behindert oder wesentliche dienstliche Interessen gefährdet. Er ist verpflichtet, Tätigkeiten, die er neben seiner Tätigkeit als Leiter der Datenschutzbehörde ausübt, unverzüglich dem Bundeskanzler zur Kenntnis zu bringen.

(5) Die Funktion des Leiters der Datenschutzbehörde endet durch Zeitablauf, Tod, Verzicht oder bei Verlust der Wählbarkeit zum Nationalrat.

(6) Bei Beendigung der Funktion des Leiters der Datenschutzbehörde ist nach Maßgabe der Abs. 1 bis 3 unverzüglich ein neuer Leiter zu bestellen.

(7) Vom Bundespräsidenten wird auf Vorschlag der Bundesregierung ein Stellvertreter des Leiters der Datenschutzbehörde nach Maßgabe der Abs. 1 bis 3 bestellt. Für den Stellvertreter des Leiters der Datenschutzbehörde gelten die Abs. 4 bis 6 sinngemäß. Er vertritt den Leiter der Datenschutzbehörde in dessen Abwesenheit.

Organisation und Unabhängigkeit der Datenschutzbehörde

§ 37. (1) Der Leiter der Datenschutzbehörde ist in Ausübung seines Amtes unabhängig und an keine Weisungen gebunden.

(2) Die Datenschutzbehörde ist eine Dienstbehörde und Personalstelle. Im Bundesfinanzgesetz ist die notwendige Sach- und Personalausstattung sicherzustellen. Die Bediensteten der Datenschutzbehörde unterstehen nur den Weisungen des Leiters

Authority [Datenschutzbehörde]

1. Members of the Federal Government [Bundesregierung], State Secretaries [Staatssekretäre], Members of a Land Government [Landesregierung], National Council [Nationalrat], Federal Council [Bundesrat] or any other General Representative Body [allgemeiner Vertretungskörper] or of the European Parliament, as well as a member of the Ombudsman Board [Volksanwalt] and the president of the Public Audit Office [Rechnungshof]

2. Anybody who held one of the positions listed in sub-para. 1 in the last two years

3. Anybody who may not be elected for the National Council.

(4) The head of the Data Protection Authority may not exercise any function that casts doubt on his professional independence or creates the impression of partiality or that keeps him from performing his duties or endangers essential official interests. He is required to report functions that he exercises beside his office as head of the Data Protection Authority to the Federal Chancellor [Bundeskanzler] without delay.

(5) The function of the head of the Data Protection Authority ends with the expiry of the period of office, death, abdication and loss of eligibility to the national Council.

(6) Once the function of the herad of the Data Protection Authority ends, a new head shall be appointed according to the rules of para. 1 to 3.

(7) The Federal President [Bundespräsident] shall appoint a deputy head of the Data Protection Authority on a proposal of the Federal Government [Bundesregierung] according to the rules of para. 1 to 3. Para. 4 to 6 shall be applied to the deputy head of the Data Protection Authority in equal measure. He shall represent the head of the Data Protection Authority during his absence.

Organisation and Indepence of the Data Protection Authority

§ 37. (1) The head of the Data Protection Authority [Leiter der Datenschutzbehörde] is independent and not bound by instructions [Weisungen] in the exercise of his office.

(2) The Data Protection Authority [Datenschutzbehörde] is an administrative authority [Dienstbehörde] und human resource department [Personalstelle]. The Federal Finance Act [Bundesfinanzgesetz] shall provide for the necessary expenditures

der Datenschutzbehörde. Der Leiter der Datenschutzbehörde übt die Diensthoheit über die Bediensteten der Datenschutzbehörde aus.

(3) Der Bundeskanzler kann sich beim Leiter der Datenschutzbehörde über die Gegenstände der Geschäftsführung unterrichten. Dem ist vom Leiter der Datenschutzbehörde nur insoweit zu entsprechen, als dies nicht der völligen Unabhängigkeit der Kontrollstelle im Sinne von Art. 28 Abs. 1 UAbs. 2 der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23.11.1995 S. 31, widerspricht.

(4) Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen, die wesentliche Fragen des Datenschutzes unmittelbar betreffen, sowie von Verordnungen des Bundes, die auf der Grundlage dieses Bundesgesetzes ergehen oder sonstige wesentliche Fragen des Datenschutzes unmittelbar betreffen, anzuhören.

(5) Die Datenschutzbehörde hat bis zum 31. März eines jeden Jahres einen Bericht über ihre Tätigkeit im vorangegangenen Kalenderjahr zu erstellen, dem Bundeskanzler vorzulegen und in geeigneter Weise zu veröffentlichen. Der Bericht ist vom Bundeskanzler dem Nationalrat und dem Bundesrat vorzulegen.

(6) Entscheidungen der Datenschutzbehörde von grundsätzlicher Bedeutung für die Allgemeinheit sind von der Datenschutzbehörde unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.

Bescheide der Datenschutzbehörde

§ 38. (1) Partei in Verfahren vor der Datenschutzbehörde sind auch die Auftraggeber des öffentlichen Bereichs.

(2) Bescheide, mit denen gemäß § 13 Übermittlungen oder Überlassungen von Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen oder tatsächlichen Voraussetzungen für die Erteilung der Genehmigung, insbesondere auch infolge einer gemäß § 55 ergangenen Kundmachung des Bundeskanzlers, nicht mehr bestehen.

(3) Parteien gemäß Abs. 1 können Beschwerde an das Bundesverwaltungsgericht erheben.

Verfahren vor dem Bundesverwaltungsgericht

§ 39. (1) Das Bundesverwaltungsgericht entscheidet in Verfahren über

for staff and equipment. The officials of the Data Protection Authority shall be bound only by the instructions of the head. The head shall have the service prerogative [Diensthoheit] over the officials of the Data Protection Authority.

(3) The Federal Chancellor [Bundeskanzler] can request information from the head of the Data Protection Authority about the operations of the authority. The head of the Data Protection Authority shall honor shuch requests only insofar as this does not compromise the independence of the supervisory authority as laid down in Article 28 paragraph 1 sub-paragraph 2 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995, p. 31.

(4) The Data Protection Authority shall be heard before laws concerning essential issues of data protection and federal ordinances based on this Federal Act [Bundesgesetz] or which otherwise directly concerns important issues of data protection are enacted.

(5) The Data Protection Authority shall formulate until 31 March every year a report about its activicties in the preceding calendar year, submit it to the Federal Chancellor [Bundeskanzler] and publish it in an appropriate manner. The report shall be submitted to the National Council [Nationalrat] and the Federal Council [Bundesrat] by the Federal Chancellor [Bundeskanzler].

(6) Decisions of the Data Protection Authority of fundamental importance to the general public shall be published by the Data Protection Authority in a suitable manner while respecting official secrecy rules [Amtsverschwiegenheit].

Rulings of the Data Protection Authority

§ 38. (1) Controllers in the public sector always have a position as party in proceedings before the Data Protection Authority.

(2) Rulings that permit transborder transmission and committing of data according to section 13, shall be revoked once the legal or factual prerequisites under which the permit was issued, especially pursuant to a promulgation [Kundmachung] of the Federal Chancellor [Bundeskanzler] according to section 55 no longer apply.

(3) Parties according to para. 1 may file a complaint with the Federal Administrative Court [Bundesverwaltungsgericht]

Procedure before the Federal Administrative Court

§ 39. (1) The Federal Administrative Court [Bundesverwaltungsgericht] shall

Beschwerden gegen Bescheide sowie wegen Verletzung der Entscheidungspflicht in den Angelegenheiten dieses Bundesgesetzes durch Senat.

(2) Der Senat besteht aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer. Die fachkundigen Laienrichter werden auf Vorschlag der Wirtschaftskammer Österreich und der Bundeskammer für Arbeiter und Angestellte bestellt. Es sind entsprechende Vorkehrungen zu treffen, dass zeitgerecht eine hinreichende Anzahl von fachkundigen Laienrichtern zur Verfügung steht.

(3) Die fachkundigen Laienrichter müssen eine mindestens fünfjährige einschlägige Berufserfahrung und besondere Kenntnisse des Datenschutzrechtes besitzen.

(4) Der Vorsitzende hat den fachkundigen Laienrichtern alle entscheidungsrelevanten Dokumente unverzüglich zu übermitteln bzw., wenn dies untunlich oder zur Wahrung der Vertraulichkeit von Dokumenten unbedingt erforderlich ist, zur Verfügung zu stellen.

Revision beim Verwaltungsgerichtshof

§ 40. Revision beim Verwaltungsgerichtshof können auch Parteien gemäß § 38 Abs. 1 erheben.

Einrichtung und Aufgaben des Datenschutzrates

§ 41. (1) Beim Bundeskanzleramt ist ein Datenschutzrat eingerichtet.

(2) Der Datenschutzrat berät die Bundesregierung und die Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe

1. kann der Datenschutzrat Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen und dazu Gutachten erstellen oder in Auftrag geben;
2. ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind;
3. haben Auftraggeber des öffentlichen Bereichs ihre Vorhaben dem Datenschutzrat zur Stellungnahme zuzuleiten, soweit diese datenschutzrechtlich von Bedeutung sind;

decide on complaints against rulings as well as complaints regarding the obligation to decide in due time regarding matters of this Federal Act by chamber.

(2) The chamber shall consist of a chairman und one professionally experienced lay judge [Laienrichter] from the domain of the employers and from the domain of employees each. The professionally experienced lay judges shall be appointed on a proposal by the Austrian Federal Economic Chamber [Wirtschaftskammer Österreich] and the Federal Chamber of Labour [Bundeskammer für Arbeiter und Angestellte]. Appropriate arrangements shall be made so that a sufficient number of professionally experienced lay judges can be nominated at the right time.

(3) The professionally experienced lay judges must have at least five years of relevant professional experience and special knowledge of data protection law.

(4) The chairman shall transmit all documents relevant to the decision to the professionally experienced lay judges without delay, or, if this is impractical or absolutely necessary to safeguard the confidentitality of the documents, make them available in some other way.

Appeal before the Administrative Court

§ 40. An appeal before the Administrative Court [Verwaltungsgerichtshof] may be brought by any party according to section 38 para. 1.

Establishment and Duties of the Data Protection Council

§ 41. (1) A Data Protection Council [Datenschutzrat] is established at the Federal Chancellery [Bundes¬kanzler¬amt].

(2) The Data Protection Council shall advise the Federal Government [Bundesregierung] and the State Governments [Landesregierungen] on requests in political matters of data protection. For this purpose,

1. the Data Protection Council can deliberate on questions of fundamental importance for data protection and may issue opinions by itself or commission an expert to deliver an opinion;
2. the Data Protection Council shall be given opportunity to give its opinion on draft bills of Federal Ministries [Bundesministerien], insofar as these are significant for data protection;
3. public sector controllers shall present their projects to the Data Protection Council for evaluation, insofar as these are significant for data protection;

4. hat der Datenschutzrat das Recht, von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;

4a. *(Anm.: aufgehoben durch BGBl. I Nr. 83/2013)*

5. kann der Datenschutzrat Auftraggeber des privaten Bereichs oder auch ihre gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung auffordern, die aus datenschutzrechtlicher Sicht Anlaß zu Bedenken, zumindest aber Anlaß zur Beobachtung geben;

6. kann der Datenschutzrat seine Beobachtungen, Bedenken und allfälligen Anregungen zur Verbesserung des Datenschutzes in Österreich der Bundesregierung und den Landesregierungen mitteilen, sowie über Vermittlung dieser Organe den gesetzgebenden Körperschaften zur Kenntnis bringen.

(3) Abs. 2 Z 3 und 4 gilt nicht, soweit innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betroffen sind.

Zusammensetzung des Datenschutzrates

§ 42. (1) Dem Datenschutzrat gehören an:

1. Vertreter der politischen Parteien: Von der im Hauptausschuss des Nationalrates am stärksten vertretenen Partei sind vier Vertreter, von der am zweitstärksten vertretenen Partei sind drei Vertreter und von jeder anderen im Hauptausschuss des Nationalrates vertretenen Partei ist ein Vertreter in den Datenschutzrat zu entsenden, wobei es allein auf die Stärke im Zeitpunkt der Entsendung ankommt. Bei Mandatsgleichheit zweier Parteien im Hauptausschuss ist die Stimmenstärke bei der letzten Wahl zum Nationalrat ausschlaggebend;
2. je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;
3. zwei Vertreter der Länder;
4. je ein Vertreter des Gemeindebundes und des Städtebundes;
5. ein vom Bundeskanzler zu ernennender Vertreter des Bundes.

4. the Data Protection Council shall have 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 in Austria;

4a. *(Note: Repealed by Federal Law Gazette I Nr. 83/2013)*

5. the Data Protection Council may ask private sector controllers or their representations of interest established by law to give their opinion on developments of general importance that give cause for concern or at least call for attention from a data protection perspective;

6. the Data Protection Council may transmit its observations, concerns and suggestions for improvements of data protection in Austria to the Federal Government and the State Governments, as well as to the legislative bodies by way of these organs.

(3) Para. 2 sub-paras. 3 and 4 shall not apply insofar as the internal affairs of the churches and religious communities recognised by law are concerned.

Composition of the Data Protection Council

§ 42. (1) The Data Protection Council [Datenschutzrat] shall have the following members:

1. representatives of the political parties: The party that is most strongly represented in the Main Committee of the National Council [Hauptausschuß des Nationalrates] shall delegate four representatives, the second strongest shall delegate three members and all other parties represented in the Main Committee of the National Council shall delegate one member each, to be determined by the strength of representation at the time of delegation. In case of equal number of deputies of two parties in the Main Committee the number of votes cast in the most recent election to the Federal Parliament is decisive;
2. one representative each from Federal Chamber of Labour [Bundeskammer für Arbeiter und Angestellte] and the Austrian Federal Economic Chamber [Wirtschaftskammer Österreich];
3. two representatives of the States [Länder];
4. one representative each of the Association of Austrian Municipalities [Gemeindebund] and the Austrian Association of Towns [Städtebund];
5. a member of the Federation [Bund] appointed by the Federal Chancellor [Bundeskanzler].

(2) Die in Abs. 1 Z 3, 4 und 5 genannten Vertreter sollen berufliche Erfahrung auf dem Gebiet der Informatik und des Datenschutzes haben.

(3) Für jedes Mitglied ist ein Ersatzmitglied namhaft zu machen.

(4) Dem Datenschutzrat können Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre und weiters Personen, die zum Nationalrat nicht wählbar sind, nicht angehören.

(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis sie dem Bundeskanzler schriftlich ihr Ausscheiden mitteilen oder, mangels einer solchen Mitteilung, von der entsendenden Stelle (Abs. 1) dem Bundeskanzler ein anderer Vertreter namhaft gemacht wird. Mitglieder nach Abs. 1 Z 1 scheiden außerdem aus, sobald der Hauptausschuss nach den §§ 29 und 30 des Geschäftsordnungsgesetzes 1975, BGBl. Nr. 410, neu gewählt wurde, und sie nicht neuerlich entsendet werden.

(6) Die Tätigkeit der Mitglieder des Datenschutzrates ist ehrenamtlich. Mitglieder des Datenschutzrates, die außerhalb von Wien wohnen, haben im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) nach Maßgabe der für Bundesbeamte geltenden Rechtsvorschriften.

Vorsitz und Geschäftsführung des Datenschutzrates

§ 43. (1) Der Datenschutzrat gibt sich mit Beschluß eine Geschäftsordnung.

(2) Der Datenschutzrat hat aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu wählen. Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden dauert - unbeschadet des § 42 Abs. 5 - fünf Jahre. Wiederbestellungen sind zulässig.

(3) Die Geschäftsführung des Datenschutzrates obliegt dem Bundeskanzleramt. Der Bundeskanzler hat das hiefür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind die Bediensteten des Bundeskanzleramtes fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.

Sitzungen und Beschlußfassung des Datenschutzrates

§ 44. (1) Die Sitzungen des Datenschutzrates werden vom Vorsitzenden nach Bedarf einberufen. Begehrt ein Mitglied die Einberufung einer Sitzung, so hat der Vorsitzende die Sitzung so einzuberufen, daß sie binnen vier Wochen stattfinden kann.

(2) The representatives mentioned in para. 1 sub-para. 3, 4 and 5 should have professional experience in the field of computer science and data protection.

(3) An alternate representative shall be nominated for every representative.

(4) Members of the Federal Government [Bundesregierung] or of a State Government [Landesregierung] or Secretaries of State [Staatssekretäre] as well as persons who may not be elected for the National Council [Nationalrat] shall not be members of the Data Protection Council [Datenschutzrat].

(5) The representatives shall be members of the Data Protection Council until they announce their resignation in writing to the Federal Chancellor [Bundeskanzler], or, if no resignation is announced, until the nominating body (para. 1) has named another representative to the Federal Chancellor. Members according to para 1 sub-para 1 retire also, as soon as the Main Committee has been newly elected according to § 29 and 30 of the Parlamentary Rules of Procedure 1975, Federal Law Gazette No. 410, and they have not been delegated again.

(6) The members of the Data Protection Council shall serve in an honorary capacity. Members of the Data Protection Council living outside of Vienna shall be entitled to receive compensation for travel expenses (category 3) according to the regulations for federal officials, if they attend meetings of the Data Protection Council.

Chairmanship and Operation of the Data Protection Council

§ 43. (1) The Data Protection Council shall decide on its rules of procedure.

(2) The Data Protection Council [Datenschutzrat] shall elect a chairman and two vice chairmen. The term of office of the chairman and the vice chairmen shall be five years, without prejudice to § 42 para. 5. Reappointments shall be permitted.

(3) The Federal Chancellery [Bundeskanzleramt] shall be responsible for the operation of the Data Protection Council. The Federal Chancellor [Bundeskanzler] shall supply the necessary personnel. While working for the Data Protection Council, the officials of the Federal Chancellery shall be bound only by instructions [Weisungen] of the chairman of the Data Protection Council with regard to their professional work.

Meetings and Decisions of the Data Protection Council

§ 44. (1) The meeting of the Data Protection Council [Datenschutzrat] shall be convened by the chairman whenever the need arises. If a member requests that a meeting be convened, the chairman shall convene the meeting so that it can take place

(2) Zu den Sitzungen kann der Vorsitzende nach Bedarf Sachverständige zuziehen.

(3) Für Beratungen und Beschlußfassungen im Datenschutzrat ist die Anwesenheit von mehr als der Hälfte seiner Mitglieder erforderlich. Zur Beschlußfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Die Beifügung von Minderheitenvoten ist zulässig.

(4) Der Datenschutzrat kann aus seiner Mitte ständige oder nichtständige Arbeitsausschüsse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten übertragen kann. Er ist auch berechtigt, die Geschäftsführung, Vorbegutachtung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatter) zu übertragen.

(5) Jedes Mitglied des Datenschutzrates ist verpflichtet, an den Sitzungen - außer im Fall der gerechtfertigten Verhinderung - teilzunehmen. Ist ein Mitglied an der Teilnahme verhindert, hat es hievon unverzüglich das Ersatzmitglied zu verständigen.

(6) Der Leiter der Datenschutzbehörde ist berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse teilzunehmen. Ein Stimmrecht steht ihm nicht zu.

(7) Die Beratungen in der Sitzung des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, vertraulich.

(8) Die Mitglieder des Datenschutzrates, der Leiter der Datenschutzbehörde und die zur Sitzung gemäß Abs. 2 zugezogenen Sachverständigen sind zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet, sofern die Geheimhaltung im öffentlichen Interesse oder im Interesse einer Partei geboten ist.

8. Abschnitt

Besondere Verwendungszwecke von Daten

Private Zwecke

§ 45. (1) Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten verarbeiten, wenn sie ihnen vom Betroffenen selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise, insbesondere in

within four weeks.

(2) The chairman can bring experts into the meeting whenever the need arises.

(3) Deliberations and decisions of the Data Protection Council shall require the presence of at least half of its members. Decisions shall be passed by a simple majority of votes cast. In the case of a parity of votes, the vote of the chairman shall decide the issue. An abstention from the vote is not permitted. A dissenting opinion may be given.

(4) The Data Protection Council may create permanent or ad hoc working groups which it may entrust with the preparation, appraisal and handling of specific issues. An individual member (rapporteur) may be entrusted with executive work, the first appraisal and handling of specific issues.

(5) Every member of the Data Protection Council must - unless justifiably being prevented - attend the meetings of the Council. A member who is unable to attend shall inform his alternate member without delay.

(6) The head of the Data Protection Authority shall have the right to attend meetings of the Data Protection Council or its working groups. He shall have no right to vote.

(7) The deliberations of the Data Protection Council shall be confidential as long as the Council itself does not decide otherwise.

(8) The members of the Data Protection Council, the head of the Data Protection Authority and experts brought into the meeting according to para. 2 shall be obliged to keep all information confidential of which they have learned solely due to their activities for the Data Protection Council, insofar as secrecy is required in the public interest or in the interest of a party.

Part 8

Special Purposes of Data Use

Private Purposes

§ 45.(1) Natural persons shall be permitted to process data for purely personal or family matters that have been disclosed to them by the data subject [Betroffener] himself or that they have received in a lawful manner, in particular in accordance with

Übereinstimmung mit § 7 Abs. 2, zugekommen sind.

(2) Daten, die eine natürliche Person für ausschließlich persönliche oder familiäre Tätigkeiten verarbeitet, dürfen, soweit gesetzlich nicht ausdrücklich anderes vorgesehen ist, für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.

Wissenschaftliche Forschung und Statistik

§ 46. (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die

1. öffentlich zugänglich sind oder
2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für ihn nur indirekt personenbezogen sind.

Andere Daten dürfen nur unter den Voraussetzungen des Abs. 2 Z 1 bis 3 verwendet werden.

(2) Bei Datenanwendungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs. 1 fallen, dürfen Daten nur

1. gemäß besonderen gesetzlichen Vorschriften oder
2. mit Zustimmung des Betroffenen oder
3. mit Genehmigung der Datenschutzbehörde gemäß Abs. 3 verwendet werden.

(3) Eine Genehmigung der Datenschutzbehörde für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik ist auf Antrag des Auftraggebers der Untersuchung zu erteilen, wenn

1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und
2. ein öffentliches Interesse an der beantragten Verwendung besteht und
3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird.

Sollen sensible Daten ermittelt werden, muß ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muß gewährleistet sein, daß die Daten beim Auftraggeber der Untersuchung nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verläßlichkeit sonst glaubhaft ist. Die Datenschutzbehörde kann die Genehmigung an die Erfüllung von Bedingungen und

§ 7 para. 2.

(2) Data that are processed by a natural person for purely personal or family matters shall be transmitted for another purpose only with the consent of the data subject, unless expressly provided for otherwise by law.

Scientific Research and Statistics

§ 46. (1) For the purpose of scientific or statistical research projects whose goal is not to obtain results in a form relating to specific data subjects [Betroffene], the controller [Auftraggeber] shall have the right to use all data that

1. are publicly accessible or
2. he has lawfully collected for other research projects or other purposes or
3. are only indirectly personal for him/her.

Other data shall only be used under the conditions specified in para. 2 sub-paras. 1 to 3.

(2) In case of the use of data [Datenverwendung] for purposes of scientific research or statistics that do not fall under para. 1 shall be used only

1. pursuant to specific legal provisions or
2. with the consent of the data subject [Betroffener] or
3. with a permit of the Data Protection Authority [Datenschutzbehörde] pursuant to para. 3.

(3) A permit of the Data Protection Authorityfor the use of data for purposes of scientific research or statistics shall be granted upon request of the controller ordering the research project, if

1. the consent of the data subjects is impossible to obtain because they cannot be reached or the effort would otherwise be unreasonable and
2. there is a public interest in the use of data for which a permit is sought and
3. the professional aptitude of the applicant has satisfactorily been demonstrated.

If sensitive data are to be collected an important public interest in the research must exist; furthermore, it must be ensured that the data at the controller ordering the research project the data shall only be used by persons who are subject to a statutory duty to confidentiality or whose reliability in this respect is otherwise credible. The Data Protection Authoritymay issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests deserving protection, in

Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

(3a) Einem Antrag nach Abs. 3 ist jedenfalls eine vom Verfügungsbefugten über die Datenbestände, aus denen die Daten ermittelt werden sollen, oder einem sonst darüber Verfügungsbefugten unterfertigte Erklärung anzuschließen, dass er dem Auftraggeber die Datenbestände für die Untersuchung zur Verfügung stellt. Anstelle dieser Erklärung kann auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 der Exekutionsordnung – EO, RGBl. Nr. 79/1896) vorgelegt werden.

(4) Rechtliche Beschränkungen der Zulässigkeit der Benützung von Daten aus anderen, insbesondere urheberrechtlichen Gründen bleiben unberührt.

(5) Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personsbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personsbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

§ 47. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adreßdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung der Zustimmung der Betroffenen.

(2) Wenn allerdings angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung eine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist, bedarf es keiner Zustimmung, wenn

1. Daten desselben Auftraggebers verwendet werden oder
2. bei einer beabsichtigten Übermittlung der Adreßdaten an Dritte
   a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
   b) der Betroffene nach entsprechender Information über Anlaß und Inhalt der Übermittlung innerhalb angemessener Frist keinen Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der

particular, with regard to the use of sensitive data.

(3a) An application according to para. 3 must, however, be accompanied by a statement signed by the person authorized to dispose of the collection of information from which the data shall be collected or by another authorized person that he/she makes available the collection of information for the research. Such statement may be replaced by a writ of execution (§ 367 para. 1 Foreclosure Act, RGBl No. 79/1896) replacing such statement.

(4) Legal restrictions on the right to make use of data [Datenverwendung] for other reasons, in particular copyright, shall not be affected.

(5) Even in those cases where the use of data in a form which permits identification of data subjects is legal for purposes of scientific research or statistics, the data shall be coded without delay so that the data subjects are no longer identifiable if specific phases of scientific or statistic work can be performed with indirectly personal data only. Unless expressly laid down otherwise, data in a form which permits identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistic work to keep them identifiable.

Transmission of Addresses to Inform or Interview Data Subjects

§ 47. (1) Unless provided for otherwise by law, the transmission [Übermittlung] of address data of a certain group of data subjects [Betroffene] in order to inform or interview them shall require the consent of the data subjects.

(2) If an infringement of the data subject's interests in secrecy is unlikely, considering the selection criteria for the category of data subjects [Betroffenenkreis] and the subject of the information or interviews, no consent shall be required if

1. data from the same controller are used or
2. in case of an intended transmission of address data to third parties
   a. there is an additional public interest in the information or interviewing or
   b. the data subject, having received an adequate information about the cause for and content of the transmission, has not objected to the transmission within a reasonable period of time.

(3) If the prerequisites of para. 2 are not met and if obtaining the consent of the

Zustimmung der Betroffenen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adreßdaten mit Genehmigung der Datenschutzbehörde gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst oder
2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder
3. zur Befragung der Betroffenen für wissenschaftliche oder statistische Zwecke

erfolgen soll.

(4) Die Datenschutzbehörde hat auf Antrag eines Auftraggebers, der Adressdaten verarbeitet, die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Die Datenschutzbehörde kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.

(5) Die übermittelten Adreßdaten dürfen ausschließlich für den genehmigten Zweck verwendet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) In jenen Fällen, in welchen es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adreßdaten notwendigen Verarbeitungen vorgenommen werden.

Publizistische Tätigkeit

§ 48. (1) Soweit Medienunternehmen, Mediendienste oder ihre Mitarbeiter Daten unmittelbar für ihre publizistische Tätigkeit im Sinne des Mediengesetzes verwenden, sind von den einfachgesetzlichen Bestimmungen des vorliegenden Bundesgesetzes nur die §§ 4 bis 6, 10, 11, 14 und 15 anzuwenden.

(2) Die Verwendung von Daten für Tätigkeiten nach Abs. 1 ist insoweit zulässig, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihrer Mitarbeiter in Ausübung des Grundrechtes auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK erforderlich ist.

data subjects' pursuant to para. 1 would require an unreasonable effort, the transmission of the address data shall be permissible with a permit of the Data Protection Authority [Datenschutzbehörde] pursuant to para. 4, in case the transmission to third parties shall be performed for

1. the purpose of information or an interview due to an important interest of the data subject himself
2. an important public interest in the information or interviews or
3. an interview of the data subjects for reasons of scientific research and statistics.

(4) Upon request of a controller processing address data the Data Protection Authorityshall grant the permit for the transmission if the controller has satisfactorily demonstrated that one of the requirements in para. 3 applies and no overriding interests in secrecy deserving protection on the part of the data subject are an obstacle to the transmission. The Data Protection Authoritymay issue the permit subject to terms and conditions, insofar s this is necessary to safeguard the data subjects' interests deserving protection, in particular, with regard to the use of sensitive data as selection criterion.

(5) The transmitted address data shall only be used for the permitted purpose and shall be erased as soon as they are no longer needed for information or interviews.

(6) In those cases where it is lawful to transmit the names and addresses of persons belonging to a certain category of data subjects pursuant to the aforementioned provisions, the processing required for selecting the address data to be transmitted shall also be permitted.

Journalistic Purposes

§ 48. (1) Insofar as media companies, media services and their operatives use data directly for journalistic purposes according to the Media Act [Mediengesetz], only sects. 4 to 6, 10, 11, 14 and 15 of the non-constitutional provisions of this Federal Act [Bundesgesetz] shall apply.

(2) The use of data [Datenverwendung] for activities pursuant to para. 1 shall be legal insofar as this is required to fulfil the information requirements of the media companies, media services and their operatives in exercise of the right to free speech pursuant to art. 10 para. 1 of the European Convention on Human Rights.

(3) Im übrigen gelten die Bestimmungen des Mediengesetzes, insbesondere seines dritten Abschnitts über den Persönlichkeitsschutz.

Verwendung von Daten im Katastrophenfall

§ 48a. (1) Auftraggeber des öffentlichen Bereiches sind im Katastrophenfall ermächtigt, Daten zu verwenden, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist. Zu diesem Zweck sind auch Hilfsorganisationen (Abs. 6) nach Maßgabe der ihnen zukommenden Aufgaben und rechtlichen Befugnis ermächtigt, Daten zu verwenden. Wenn dies zur raschen Bewältigung der Katastrophe notwendig ist, darf eine Datenverwendung in Form der Teilnahme an einem Informationsverbundsystem erfolgen. Wer rechtmäßig über Daten verfügt, darf diese an Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen übermitteln, sofern diese die Daten zur Bewältigung der Katastrophe für die genannten Zwecke benötigen. Die Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.

(2) Eine Überlassung oder Übermittlung von Daten in das Ausland ist zulässig, soweit dies für die Erfüllung der in Abs. 1 genannten Zwecke notwendig ist. Wenn dies zur raschen Bewältigung der Katastrophe notwendig ist, darf eine Datenverwendung durch Auftraggeber des öffentlichen Bereichs und Hilfsorganisationen in Form der Teilnahme an einem Informationsverbundsystem, an dem auch ausländische Auftraggeber beteiligt sind, erfolgen. Die Übermittlung erkennungsdienstlicher und sensibler Daten zu Identifizierungszwecken an ein derartiges System darf erst stattfinden, wenn auf Grund von Erhebungen konkrete Anhaltspunkte dafür vorliegen, dass die vermisste Person verstorben sein dürfte. Daten, die für sich allein den Betroffenen strafrechtlich belasten, dürfen nicht übermittelt werden, es sei denn, dass diese zur Identifizierung im Einzelfall unbedingt notwendig sind. Die Übermittlung von Daten Angehöriger darf nur in pseudonymisierter Form erfolgen. Daten dürfen in Staaten ohne angemessenes Datenschutzniveau nur übermittelt oder überlassen werden, wenn der Auftraggeber auf Grund schriftlicher Vereinbarungen mit dem Empfänger oder auf Grund schriftlicher Zusagen des Empfängers oder, wenn dies nach den Umständen nicht oder nicht in angemessener Zeit möglich ist, durch Erteilung von Auflagen an den Empfänger davon ausgehen kann, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Eine Übermittlung oder Überlassung hat dann zu unterbleiben, wenn Grund zur Annahme besteht, dass der Empfänger nicht für den

(3) In all other respects the Media Act [Mediengesetz] shall apply, especially the third part about the protection of personality rights.

Use of data in case of a catastrophe

§ 48a. (1) Controllers of the public sector shall be authorised to use data in case of a catastrophe to assist persons affected directly by the catastrophe, to locate and identify missing or deceased persons and to provide information to the relatives. Relief organisations (para. 6) shall be authorised to use data for this purpose in accordance with their duties and legitimate authority. If this is necessary to cope with the catastrophe swiftly, the use of data may be carried out by participating in a joint information system. Anybody who lawfully possesses data shall be permitted to transmit these data to controllers of the public sector and relief organisations, if these organisations need this data to manage the catastrophe for the purposes specified. The data are to be deleted immediately if they are not any longer required for the fulfilment of the specific purpose.

(2) The data shall be committed or transmitted to recipients in third countries insofar as this is necessary to fulfil the purposes mentioned in para. 1. If this is necessary to rapidly cope with the catastrophe, data may be used by public sector controllers and relief organisations in the form of a joint information system with the participation of foreign controllers. A transfer of police records and sensitive data for the purpose of identification to a system of this kind shall only take place if investigations have yielded tangible evidence that the missing person is presumably deceased. Data that by itself would implicate the data subject in a crime shall not be transferred unless it is absolutely necessary for identification in a particular case. The data of relatives shall only be transferred in pseudonymous form. Data shall be transmitted or committed to states lacking an adequate general level of data protection only if the controller can assume, based on a written agreement with the recipient or, if such cannot be obtained under the circumstances in due time, by specifying conditions for the recipient, that the interests in secrecy deserving protection of the data subjects of the intended transfer shall be sufficiently respected in the recipient country. A transmission or committing shall not take place if there is cause for concern that the recipient will not devote attention to the interests in secrecy deserving protection of the data subjects or that he will ignore data protection conditions imposed by the controller. While the catastrophic event continues, the requirement to obtain a permit shall not apply pursuant to § 12 para. 3 sub-para. 3. The Data Protection Authorityshall be

gebotenen Schutz der Geheimhaltungsinteressen der Betroffenen Sorge tragen oder ausdrückliche datenschutzrechtliche Auflagen des Auftraggebers missachten werde. Während der Dauer der Katastrophensituation entfällt im Hinblick auf § 12 Abs. 3 Z 3 die Genehmigungspflicht. Die Datenschutzbehörde ist von den veranlassten Übermittlungen und Überlassungen und den näheren Umständen des Anlass gebenden Sachverhaltes jedoch unverzüglich zu verständigen. Die Datenschutzbehörde kann zum Schutz der Betroffenenrechte Datenübermittlungen oder -überlassungen untersagen, wenn der durch die Datenweitergabe bewirkte Eingriff in das Grundrecht auf Datenschutz durch die besonderen Umstände der Katastrophensituation nicht gerechtfertigt ist.

informed immediately about the data transfers and committings performed and about the circumstances of the motivating incident. The Data Protection Authorityis authorized to prohibit data transfers and committings if the intervention into the civil right to data protection is not justified by special circumstances caused by the catastrophe.

(3) Auf Grund einer konkreten Anfrage eines nahen Angehörigen einer tatsächlich oder vermutlich von der Katastrophe unmittelbar betroffenen Person sind Auftraggeber ermächtigt, dem Anfragenden Daten über die Reise in das und aus dem Katastrophengebiet, Aufenthaltsdaten im Katastrophengebiet sowie Daten über den Stand der Ausforschung von betroffenen Personen zu übermitteln, wenn der Angehörige folgende Daten bekannt gibt:

(3) Based on a specific inquiry of a close relative of a person who is actually or presumably affected by a catastrophe, controllers of the public sector shall be authorised to transmit data to the inquiring person regarding the journey to an from the disaster area, data on the data subjects whereabouts in the disaster area as well as data on the search for the involved persons, if the relative can name the following data:

1. Vor- und Zuname, Geburtsdatum sowie Wohnadresse der tatsächlich oder vermutlich von der Katastrophe betroffenen Person und

1. First name and surname, date of birth as well as the place of residence of a person who is actually or presumably affected by the catastrophe person and

2. seinen Vor- und Zunamen, sein Geburtsdatum, seine Wohnadresse und sonstige Erreichbarkeit sowie seine Angehörigeneigenschaft zur betroffenen Person.

2. then relatives own first name and surname, his date of birth, place of residence, contact details as well as his relation to the person involved.

Bestehen Zweifel an der Angehörigeneigenschaft und können diese durch Überprüfungen nicht ausgeräumt werden, ist ein Nachweis der Identität und Angehörigeneigenschaft notwendig.

If doubts remain about the relation to the person involved which cannot be eliminated by examination, a proof of identity and relation shall be required.

(4) Über Abs. 3 hinaus dürfen nahen Angehörigen von Auftraggebern des öffentlichen Bereiches und Hilfsorganisationen Daten einschließlich sensibler Daten über tatsächlich oder vermutlich unmittelbar von der Katastrophe betroffene Personen nur übermittelt werden, wenn sie ihre Identität und ihre Angehörigeneigenschaft nachweisen und die Auskunft zur Wahrung ihrer Rechte oder jener der betroffenen Person erforderlich ist. Die Sozialversicherungsträger sind verpflichtet, die Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen bei der Überprüfung der Daten gemäß Abs. 3 und der Angehörigenbeziehung zu unterstützen. Behörden sind ermächtigt, die zur Überprüfung dieser Angaben notwendigen Daten im Wege der Amtshilfe zu ermitteln und für diesen Zweck zu verwenden.

(4) Data, including sensitive data, on persons actually or presumably affected by the catastrophe may be transmitted beyond the scope of para. 3 to close relatives by public sector controllers and relief organisations if they prove their identity and relation and the information is necessary to safeguard their rights or those of the affected person. The social insurance agencies shall be obliged to assist the public sector controllers and relief organisations with the verification of the data pursuant to para. 3 and the family relation. The authorities are authorized to collect the necessary data by administrative assistance and to use them for this purpose.

(5) Als nahe Angehörige im Sinne dieser Bestimmung sind Eltern, Kinder, Ehegatten, eingetragene Partner und Lebensgefährten der Betroffenen zu verstehen.

(5) Close relatives pursuant to this regulation are parents, children, spouses and companions in life of the data subjects. Other relatives shall receive the mentioned

Andere Angehörige dürfen die erwähnten Auskünfte unter denselben Voraussetzungen wie nahe Angehörige dann erhalten, wenn sie eine besondere Nahebeziehung zu der von der Katastrophe tatsächlich oder vermutlich unmittelbar betroffenen Person glaubhaft machen.

(6) Eine Hilfsorganisation im Sinne dieser Bestimmung ist eine allgemein anerkannte gemeinnützige Organisation, die statuten- oder satzungsgemäß das Ziel hat, Menschen in Notsituationen zu unterstützen und von der angenommen werden kann, dass sie in wesentlichem Ausmaß eine Hilfeleistung im Katastrophenfall erbringen kann.

(7) Alle Datenverwendungen sind im Sinne des § 14 Abs. 2 Z 7 zu protokollieren.

(8) Die Zulässigkeit von Datenverwendungen auf der Grundlage anderer in den §§ 8 und 9 genannter Tatbestände bleibt unberührt.

9. Abschnitt
Besondere Verwendungsarten von Daten

Automatisierte Einzelentscheidungen

§ 49. (1) Niemand darf einer für ihn rechtliche Folgen nach sich ziehenden oder einer ihn erheblich beeinträchtigenden Entscheidung unterworfen werden, die ausschließlich auf Grund einer automationsunterstützten Verarbeitung von Daten zum Zweck der Bewertung einzelner Aspekte seiner Person ergeht, wie beispielsweise seiner beruflichen Leistungsfähigkeit, seiner Kreditwürdigkeit, seiner Zuverlässigkeit oder seines Verhaltens.

(2) Abweichend von Abs. 1 darf eine Person einer ausschließlich automationsunterstützt erzeugten Entscheidung unterworfen werden, wenn

1. dies gesetzlich ausdrücklich vorgesehen ist oder
2. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages ergeht und dem Ersuchen des Betroffenen auf Abschluß oder Erfüllung des Vertrages stattgegeben wurde oder
3. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen - beispielsweise die Möglichkeit, seinen Standpunkt geltend zu machen - garantiert wird.

(3) Dem Betroffenen ist bei automatisierten Einzelentscheidungen auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen. § 26 Abs. 2 bis 10 gilt sinngemäß.

information under the same conditions as close relatives if they can satisfactorily demonstrate a special relationship to the person actually or presumably affected by the catastrophe.

(6) A relief organization in terms of this regulation is a generally recognized non-profit organisation with designated to assist people in emergencies as laid down in its charter or articles of association and which can be expected to deliver substantial aid in case of a catastrophe.

(7) all uses of data shall be logged pursuant to § 14 para. 2 sub-para 7.

(8) The legitimacy of any use of data based on any other case -outlined in § 8 and 9 shall not be affected.

Part 9
Special Uses of Data

Automated Individual Decisions

§ 49. (1) Nobody shall be subjected to a decision that produces legal effects concerning him or adversely affects him in a significant manner which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, for example his performance at work, creditworthiness, reliability and conduct.

(2) Deviating from para. 1, a person may be subjected to a decision based solely on auto¬mated processing if

1. this is expressly authorised by law or
2. the decision is taken in the course of the entering into or performance of a contract, and the request of the data subject [Betroffener] for the entering into or the performance of the contract has been satisfied or
3. the legitimate interests of the data subject are safeguarded by appropriate means such as arrangements allowing him to assert his point of view.

(3) Upon request, the data subject shall in case of automated decisions be informed of the logical procedure of the automated decision in an intelligible form. § 26 paras 2 to 10 are to be applied accordingly.

Informationsverbundsysteme

§ 50. (1) Die Auftraggeber eines Informationsverbundsystems haben, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen. Name (Bezeichnung) und Anschrift des Betreibers sind in der Meldung zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet des Rechtes des Betroffenen auf Auskunft nach § 26 hat der Betreiber jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen; in Fällen, in welchen der Auftraggeber gemäß § 26 Abs. 5 vorzugehen hätte, hat der Betreiber mitzuteilen, daß kein der Pflicht zur Auskunftserteilung unterliegender Auftraggeber benannt werden kann. Abgesehen von der abweichenden Frist gilt § 26 Abs. 3 bis 10 sinngemäß. Die Unterstützungspflicht des Betreibers gilt auch bei Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber unter den gleichen Voraussetzungen, wie sie in § 33 Abs. 3 vorgesehen sind, befreien. Wird ein Informationsverbundsystem geführt, ohne daß eine entsprechende Meldung an die Datenschutzbehörde unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.

(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten, insbesondere auch die Vornahme der Meldung des Informationsverbundsystems, auf den Betreiber übertragen werden. Allein für die Übertragung der Meldepflicht ist die Vorlage von Vollmachten nach § 10 AVG nicht erforderlich. Soweit der Pflichtenübergang nicht durch Gesetz angeordnet ist, ist er gegenüber Dritten nur wirksam, wenn er – auf Grund einer entsprechenden Meldung an die Datenschutzbehörde – aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.

(2a) Wird ein Informationsverbundsystem auf Grund einer Meldung von zumindest zwei Auftraggebern registriert, so können Auftraggeber, die in der Folge die Teilnahme an dem Informationsverbundsystem anstreben, die Meldung im Umfang des § 19 Abs. 1 Z 3 bis 7 auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken, wenn sie eine Teilnahme im genau gleichen Umfang anstreben.

(3) Die Bestimmungen der Abs. 1 und 2 gelten nicht, soweit infolge der besonderen, insbesondere internationalen Struktur eines bestimmten Informationsverbundsystems gesetzlich ausdrücklich anderes vorgesehen ist.

Joint Information Systems

§ 50. (1) The controllers [Auftraggeber] of a joint information system [Informationsverbundsystem] shall, unless already regulated by law, appoint a suitable operator [Betreiber] for the system. The name (designation) and address of the operator shall be included in the notification for registration in the Data Processing Register [Datenverarbeitungsregister]. Without prejudice to the data subject's rights pursuant to § 26, the operator shall give to the data subject [Betroffener] upon request within twelve weeks all information necessary to identify the controller who is responsible for the data processed in the system concerning him; in cases where the controller would have to apply § 26 para. 5, the operator shall inform the data subject that no controller obligated to give the information can be named. Notwithstanding the different deadline § 26 paras 3 to 10 applies accordingly. The operator's obligation to assist shall also apply in case of requests by public authorities. The operator shall also be responsible for the necessary data security measures (§ 14) in the joint information system. The operator can free himself of liability under the conditions laid down in § 33 para. 3. If a joint information system is operated and no appropriate notification with an appointed operator is filed with the Data Protection Authority, each controller shall have to bear the obligations of the Operator.

(2) Further controller duties may be assigned to the operator by an appropriate legal instrument especially the duty of notification of the joint information system. Merely for the assignment of the notification obligation the presentation of powers according to § 10 General Administrative Act shall not be required. To the extent such assignment of duties is not provided by law it is only valid vis-á-vis third parties if the assignment is recorded in the Data Processing Register [Datenverarbeitungsregister] following an appropriate communication to the Data Protection Authority [Datenschutzbehörde].

(2a) If a joint information system is registered based on the notification of at least two controllers, other controllers who subsequently wish to join the joint information system, may limit the registration in the extent of § 19 para 1 sub-para 3 to 7 to a reference to the content of the notification of an already registred controller, provided they intend to participate in exactly the same manner.

(3) The provisions of para. 1 and 2 shall not apply if provided for otherwise by law due to the special, in particular, international structure of a specific joint information system.

9a. Abschnitt
Videoüberwachung

Allgemeines

§ 50a. (1) Videoüberwachung im Sinne dieses Abschnittes bezeichnet die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte. Für derartige Überwachungen gelten die folgenden Absätze, sofern nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Für Videoüberwachung gelten die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3). Rechtmäßige Zwecke einer Videoüberwachung, insbesondere der Auswertung und Übermittlung der dabei ermittelten Daten, sind jedoch vorbehaltlich des Abs. 5 nur der Schutz des überwachten Objekts oder der überwachten Person oder die Erfüllung rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, im Hinblick auf Ereignisse nach Abs. 1. Persönlichkeitsrechte nach § 16 ABGB bleiben unberührt.

(3) Ein Betroffener ist durch eine Videoüberwachung dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn

1. diese im lebenswichtigen Interesse einer Person erfolgt, oder
2. Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder
3. er der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.

(4) Ein Betroffener ist darüber hinaus durch eine Videoüberwachung ausschließlich dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn sie nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgt und

1. bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden, oder
2. unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche

Part 9a.
Video surveillance

General

§ 50a. (1) Video surveillance in the sense of this part means the systematic, most of all continuous observation of occurrences concerning a certain object (observed object) or a certain person (observed person) by technical –devices designed to make or transmit images. The following paragraphs apply to such surveillance unless provided differently by other laws.

(2) §§ 6 and 7 apply to video surveillance, especially the principle of proportionality (§ 7 para 3). Lawful purposes for video surveillance, especially analysis and transmission of the data obtained such way, under reservation of para 5 only are the protection of the object or the person observed or the fulfilment of legal duties of diligence, including securing of evidence, with regard to occurrences according to para 1. Personal rights according to § 16 General Civil Code remain unaffected.

(3) A data subject concerned by video surveillance is not infringed in his/her interests for secrecy deserving protection (§ 7 para 2 sub-para 3) if,

1. it is made in the vital interest of a person, or
2. data on behaviour are processed which, without any doubt, has been intended to be publicly noticed, or
3. he/she has expressly consented to the use of his/her data in the context of the surveillance operation.

(4) A data subject concerned is exclusively not infringed in his/her interests for secrecy deserving protection (§ 7 para 2 sub-para 3), if the video-surveillance is not made in the performance of official executive tasks and

1. certain facts justify the presumption, that the object or person surveyed could become the target or the location of a dangerous attack, or
2. directly applicable legal rules of the international or EU-Law, laws, ordinances, orders or judicial decisions oblige the controller to special duties of

Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der überwachten Person auferlegen, oder

3. sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden (Echtzeitüberwachung), und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

(5) Mit einer Videoüberwachung nach Abs. 4 dürfen nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen. Weiters ist die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt.

(6) Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 bis 4 hinaus in folgenden Fällen übermittelt werden:

1. an die zuständige Behörde oder das zuständige Gericht, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder
2. an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs. 5 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, eingeräumten Befugnisse,

auch wenn sich die Handlung oder der Angriff nicht gegen das überwachte Objekt oder die überwachte Person richtet. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Auftraggebers bleiben unberührt.

(7) Mit einer Videoüberwachung gewonnene Daten von Betroffenen dürfen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.

Besondere Protokollierungs- und Löschungspflicht

§ 50b. (1) Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren. Dies gilt nicht für Fälle der Echtzeitüberwachung.

(2) Aufgezeichnete Daten sind, sofern sie nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- oder Beweissicherungszwecke oder für Zwecke nach § 50a Abs. 6 benötigt werden, spätestens nach 72 Stunden zu löschen. § 33 Abs. 2 AVG gilt. Eine beabsichtigte längere Aufbewahrungsdauer ist in der

diligence the for protection of the object or the person surveyed or

3. the surveillance is restricted to a mere real time reproduction of occurrences concerning the surveyed object/the surveyed person which, therefore, are neither recorded nor processed in any other way (real time surveillance) and is performed for the purpose of the protection of health, life or property of the controller.

(5) Video surveillance according to para 4 must not observe occurrences at locations that are part of the most personal area of life of a data subject. Furthermore, video surveillance for staff-control at places of work is prohibited.

(6) Interests for secrecy of data subjects concerned deserving protection are also not infringed if data recorded by video surveillance, in cases exceeding a use in accordance with paras 2 to 4, are transmitted:

1. to the competent authority or the court, because the controller has reasonable ground for suspicion that the data could document a criminal act punishable by the courts to be prosecuted ex officio or
2. to police authorities in order to carry out their function granted under the Police Act (SPG) Federal Law Gazette No. 566/1991,

even if the action or attack is not directed against the object or the person surveyed. The rights of authorities and courts to enforce the submission of documented evidence and to secure means of evidence and the corresponding obligations of the controller remain unaffected.

(7) Data collected of data subjects concerned by video surveillance may not be analyzed by comparison with other picture data and not be searched using sensitive data as selection criteria.

Special duty of documentation and deletion

§ 50b. (1) Any use of video surveillance is to be documented. This does not apply to real time observation.

(2) Data recorded are to be deleted the latest after 72 hours, unless needed on a specific occasion for the intended purposes of protection or securing evidence or for purposes according to § 50a para 6. § 33 para 2 General Administrative Act is to be applied. An intended longer duration of storage is to be indicated in the notification and

Meldung anzuführen und zu begründen. In diesem Fall darf die Datenschutzbehörde die Videoüberwachung nur registrieren, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist.

Meldepflicht und Registrierungsverfahren

§ 50c. (1) Videoüberwachungen unterliegen der Meldepflicht gemäß den §§ 17 ff. Sofern der Auftraggeber nicht in der Meldung zusagt, die Videoüberwachungsdaten zu verschlüsseln und unter Hinterlegung des einzigen Schlüssels bei der Datenschutzbehörde sicherzustellen, dass eine Auswertung der Videoaufzeichnungen nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet, unterliegen sie der Vorabkontrolle (§ 18 Abs. 2). Bestimmte Tatsachen im Sinn von § 50a Abs. 4 Z 1 müssen bei Erstattung der Meldung glaubhaft gemacht werden. Soweit gemäß § 96a des Arbeitsverfassungsgesetzes 1974 – ArbVG, BGBl. Nr. 22, Betriebsvereinbarungen abzuschließen sind, sind diese im Registrierungsverfahren vorzulegen.

(2) Eine Videoüberwachung ist über § 17 Abs. 2 und 3 hinaus von der Meldepflicht ausgenommen

1. in Fällen der Echtzeitüberwachung oder
2. wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.

(3) Mehrere überwachte Objekte oder überwachte Personen, für deren Videoüberwachung derselbe Auftraggeber eine gesetzliche Zuständigkeit oder rechtliche Befugnis (§ 7 Abs. 1) hat, können auf Grund ihrer gleichartigen Beschaffenheit oder ihrer räumlichen Verbundenheit in einer Meldung zusammengefasst werden, wenn sich diese auf die gleiche Rechtsgrundlage stützt.

Information durch Kennzeichnung

§ 50d. (1) Der Auftraggeber einer Videoüberwachung hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Auftraggeber eindeutig hervorzugehen, es sei denn, dieser ist den Betroffenen nach den Umständen des Falles bereits bekannt. Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

(2) Keine Kennzeichnungsverpflichtung besteht bei Videoüberwachungen im Rahmen der Vollziehung hoheitlicher Aufgaben, die nach § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

must be explained. In such case the Data Protection Authoritymay register the video surveillance only if this is regularly necessary for specific reasons to serve the purposes.

Obligation of notification and procedure of registration

§ 50c. (1) Video surveillances are subject to the obligation of notification according to §§ 17 et seq. If the controller does not specify in the notification that the video surveillance data are to be encrypted and does not ensure that an analysis of the video surveillance data may only take place through a certain institution in a specific case by depositing the sole code key with the Data Protection Authority, they are subject to prior checking (§ 18 para. 2). When filing the notification prima facie evidence must be given for facts in the sense of § 50a para. 4 sub-para 1. To the extent agreements between the works committee and the management are to be concluded according to § 96a of the Labour Constitution Act 1974 - ArbVG, Federal Law Gazette No. 22, such are to be submitted in the registration procedure.

(2) Beyond § 17 para 2 and 3, video surveillance is exempted from the notification obligation

1. in cases of real-time observation or
2. if the recording is only made on a analog video recording system.

(3) If the same controller has the statutory competence or legitimate authority (§ 7 para 1) for video surveillance of several objects or persons, he may submit a combined notification based on their similar quality or local connection, if the legal basis is identical.

Information by signs

§ 50d. (1) The controller of a video surveillance shall put up appropriate signs. The sign shall specify who the controller is, unless already known to the data subjects based on the circumstances of the case. The information sign has to be fixed in places in a way, that any potential data subject approaching the surveyed object or person has the possibility to bypass the video surveillance.

(2) Video surveillances within the frame of implementation of official executive tasks, being exempted from the obligation of notification according to § 17 para 3, need not be marked with signs.

Auskunftsrecht

§ 50e. (1) Abweichend von § 26 Abs. 1 ist dem Auskunftswerber, nachdem dieser den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, und den Ort möglichst genau benannt und seine Identität in geeigneter Form nachgewiesen hat, Auskunft über die zu seiner Person verarbeiteten Daten durch Übersendung einer Kopie der zu seiner Person verarbeiteten Daten in einem üblichen technischen Format zu gewähren. Alternativ kann der Auskunftswerber eine Einsichtnahme auf Lesegeräten des Auftraggebers verlangen, wobei ihm auch in diesem Fall die Ausfolgung einer Kopie zusteht. Die übrigen Bestandteile der Auskunft (verfügbare Informationen über die Herkunft, Empfänger oder Empfängerkreise von Übermittlungen, Zweck, Rechtsgrundlagen sowie allenfalls Dienstleister) sind auch im Fall der Überwachung schriftlich zu erteilen, wenn nicht der Auskunftswerber einer mündlichen Auskunftserteilung zustimmt.

(2) § 26 Abs. 2 ist mit der Maßgabe anzuwenden, dass in dem Fall, dass eine Auskunft wegen überwiegender berechtigter Interessen Dritter oder des Auftraggebers nicht in der in Abs. 1 geregelten Form erteilt werden kann, der Auskunftswerber Anspruch auf eine schriftliche Beschreibung seines von der Überwachung verarbeiteten Verhaltens oder auf eine Auskunft unter Unkenntlichmachung der anderen Personen hat.

(3) In Fällen der Echtzeitüberwachung ist ein Auskunftsrecht ausgeschlossen.

10. Abschnitt

Strafbestimmungen

Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

Right of information

§ 50e. (1) Deviating from § 26 para 1, the person requesting information, after having indicated the timeframe during which he/she might have been captured by the surveillance and after having indicated the location as precisely as possible and after having proven his/her identity in adequate manner, is to be granted information on the data processed on his/her person, by sending of a copy on the data processed to his/her person in a common technical format. Alternately, the person requesting information may request inspection on a reading device of the controller and is also entitled to be handed over a copy in such case. The other elements of the information (available data on the origin, recipient or circles of recipients of data transmitted, purpose, legal basis and eventually service providers) are to be given in writing also in case of surveillance, unless the person requesting information agrees to oral information.

(2) § 26 para 2 is to be applied with the proviso, that in case, that an information cannot be disclosed because of overriding legitimate interests of third parties or of the controller in a manner as described in para 1, the person requesting information is entitled to a written description of his/her behaviour processed by the surveillance or to an information, in which other persons have been made unrecognizable.

(3) In cases of real time surveillance there is no right for information.

Part 10

Penal Provisions

Use of Data with the Intention to make a Profit or to Cause Harm

§ 51. (1) Whoever with the intention to enrich himself or a third person unlawfully or to harm someone in his entitlement guaranteed according to § 1 para 1 deliberately uses personal data that have been entrusted to or made accessible to him solely because of professional reasons, or that he has acquired illegally, for himself or makes such data available to others or publishes such data with the intention to make a profit or to harm others, despite the data subject’s interest in secrecy deserving protection, shall be punished by a court with imprisonment up to a year, unless the offence shall be subject to a more severe punishment pursuant to another provision.

Verwaltungsstrafbestimmung

§ 52. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 25 000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder
4. Daten vorsätzlich entgegen § 26 Abs. 7 löscht;
5. sich unter Vortäuschung falscher Tatsachen vorsätzlich Daten gemäß § 48a verschafft.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 10 000 Euro zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß den §§ 17 oder 50c erfüllt zu haben oder eine Datenanwendung auf eine von der Meldung abweichende Weise betreibt oder
2. Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Datenschutzbehörde gemäß § 13 Abs. 1 eingeholt zu haben oder
3. gegen gemäß § 13 Abs. 2 Z 2, § 19 oder § 50c Abs. 1 abgegebene Zusagen oder von der Datenschutzbehörde gemäß § 13 Abs. 1 oder § 21 Abs. 2 erteilte Auflagen verstößt oder
4. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24, 25 oder 50d verletzt oder
5. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht lässt oder
6. die gemäß § 50a Abs. 7 und § 50b Abs. 1 erforderlichen Sicherheitsmaßnahmen außer Acht lässt oder
7. Daten nach Ablauf der in § 50b Abs. 2 vorgesehene Löschungsfrist nicht löscht.

Administrative Penalties

§ 52. (1) Insofar as the act does not realise the legal elements of a criminal offence subject to the jurisdiction of the courts of law and is not subject to more severe penalties according to another administrative provision, an administrative offence punishable by a fine of up to 25 000 Euro is committed by anyone who

1. intentionally and illegally gains access to a data application [Datenanwendung] or maintains an obviously illegal means of access or
2. transmits data intentionally in violation of the rules on confidentiality (§ 15), and in particular anybody who uses data entrusted to him according to § 46 and 47 for other purposes or
3. uses or fails to grant information, to rectify or erase data in violation of a final judicial decision or ruling [Bescheid],
4. intentionally erases data in violation of § 26 para. 7;
5. by pretending incorrect facts intentionally obtains data according to § 48a.

(2) Insofar as the act does not realise the legal elements of a criminal offence subject to the jurisdiction of the courts of law, an administrative offence punishable by a fine of up to 10 000 Euro is committed by anyone who

1. collects, processes and transmits data without having fulfilled his obligation to notification according to §§ 17 or 50c or operates a data application in a manner deviating from the notification.
2. engages in transborder data transmissions [Übermittlungen] or committings [Überlassungen] without the necessary permit of the Data Protection Authority [Datenschutzbehörde] according to § 13 para 1or
3. violates declarations given according to § 13 para 2 sub-para. 2, § 19 or 50c para 1 or conditions imposed by the Data Protection Authorityaccording to § 13 para 1 or § 21 para 2 or
4. violates his obligations of disclosure and information according to sects. 23, 24, 25 and 50d or
5. grossly neglects the required data security measures according to § 14 or
6. disregards the safety measures required according to § 50a para 7 and § 50b para 1 or
7. does not delete data after expiring of the period provided for in § 50b para 2 for deletion.

(2a) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit einer Strafe bis zu 500 Euro zu ahnden ist, wer Daten entgegen den §§ 26, 27 oder 28 nicht fristgerecht beauskunftet, richtigstellt oder löscht.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

(5) Zuständig für Entscheidungen nach Abs. 1 bis 4 ist die Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat. Falls ein solcher im Inland nicht gegeben ist, ist die am Sitz der Datenschutzbehörde eingerichtete Bezirksverwaltungsbehörde zuständig.

11. Abschnitt
Übergangs- und Schlußbestimmungen

Befreiung von Gebühren, Abgaben und vom Kostenersatz

§ 53. (1) Die durch dieses Bundesgesetz unmittelbar veranlaßten Eingaben der Betroffenen zur Wahrung ihrer Interessen sowie die Eingaben im Registrierungsverfahren und die gemäß § 21 Abs. 3 zu erstellenden Registerauszüge sind von den Stempelgebühren und von den Verwaltungsabgaben des Bundes befreit.

(2) Für Abschriften aus dem Datenverarbeitungsregister, die ein Betroffener zur Verfolgung seiner Rechte benötigt, ist kein Kostenersatz zu verlangen.

Mitteilungen an die Europäische Kommission und an die anderen Mitgliedstaaten der Europäischen Union

§ 54. (1) Von der Erlassung eines Bundesgesetzes, das die Zulässigkeit der Verarbeitung sensibler Daten betrifft, hat der Bundeskanzler anläßlich der Kundmachung des Gesetzes im Bundesgesetzblatt der Europäischen Kommission Mitteilung zu machen.

(2) Die Datenschutzbehörde hat den anderen Mitgliedstaaten der Europäischen Union und der Europäischen Kommission mitzuteilen, in welchen Fällen

(2a) To the extent the act does not constitute a criminal offence within the jurisdiction of the courts or is punishable under other administrative penal regulations, who, contrary to §§ 26, 27 or 28, does not in time give information on, corrects or deletes data, commits an administrative offence to be punished with a fine up to € 500.

(3) Attempts shall be punished.

(4) Data media or programs as well as picture transmitting or -recording devices can be confiscated (sects. 10, 17 and 18 VStG), if they are linked to an administrative offence according to para. 1 and 2.

(5) The District Administrative Authority [Bezirksverwaltungsbehörde] at the controllers [Auftraggeber] (processors [Dienstleister]) domicile or seat shall be the competent authority for decisions according to para. 1 to 4. If there is no domicile or seat in Austria, the District Administrative Authority at the seat of the Data Protection Authority [Datenschutzbehörde] shall be competent.

Part 11
Transitional and Final Provisions

Exemption from Fees

§ 53. (1) All applications submitted according to this Federal Act [Bundesgesetz] by data subjects [Betroffener] to safeguard their interests as well as all applications in the proceedings for notification and for register statements according to § 21 para. 3 shall be exempt from stamp duties and federal administrative fees.

(2) No fee shall be charged for copies of entries in the Data Processing Register [Datenverarbeitungsregister] needed by a data subject to assert his rights.

Communication to the European Commission and to the other Member States of the European Union

§ 54. (1) The Federal Chancellor [Bundeskanzler] shall communicate to the European Commission whenever a Federal Act [Bundesgesetz] concerning the right to process sensitive data has been adopted upon its promulgation in the Federal Law Gazette [Bundesgesetzblatt].

(2) The Data Protection Authority [Datenschutzbehörde] shall communicate to the other member states of the European Union and the European Commission in which

1. keine Genehmigung für den Datenverkehr in ein Drittland erteilt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 1 nicht als gegeben erachtet wurden;
2. der Datenverkehr in ein Drittland ohne angemessenes Datenschutzniveau genehmigt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 2 als gegeben erachtet wurden.

Feststellungen der Europäischen Kommission

§ 55. Der Inhalt der in einem Verfahren gemäß Art. 31 Abs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31, getroffenen Feststellungen der Europäischen Kommission über

1. das Vorliegen oder Nichtvorliegen eines angemessenen Datenschutzniveaus in einem Drittland oder
2. die Eignung bestimmter Standardvertragsklauseln oder Verpflichtungserklärungen zur Gewährleistung eines ausreichenden Schutzes der Datenverwendung in einem Drittland

ist vom Bundeskanzler im Bundesgesetzblatt gemäß § 4 des Bundesgesetzblattgesetzes, BGBl. I Nr. 100/2003, kundzumachen.

Verwaltungsangelegenheiten gemäß Art. 30 B-VG

§ 56. Der Präsident des Nationalrats ist Auftraggeber jener Datenanwendungen, die für Zwecke der ihm gemäß Art. 30 B-VG übertragenen Angelegenheiten durchgeführt werden. Übermittlungen von Daten aus solchen Datenanwendungen dürfen nur über Auftrag des Präsidenten des Nationalrats vorgenommen werden. Der Präsident trifft Vorsorge dafür, daß im Falle eines Übermittlungsauftrags die Voraussetzungen des § 7 Abs. 2 vorliegen und insbesondere die Zustimmung des Betroffenen in jenen Fällen eingeholt wird, in welchen dies gemäß § 7 Abs. 2 mangels einer anderen Rechtsgrundlage für die Übermittlung notwendig ist.

Sprachliche Gleichbehandlung

§ 57. Soweit in diesem Artikel auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

cases

1. no permit was issued for transborder data flows to a third country because the requirements of § 13 para. 2 sub-para 1 were considered not to have been met;
2. a permit was issued for transborder data flows to a third country without an adequate level of data protection because the requirements of § 13 para. 2 sub-para 2 are deemed to have been met.

Measures of the European Commission

§ 55. The content of findings of the European Commission made according to Art. 31 para. 2 of the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23 November 1995 p. 0031, on

1. whether a third country has an adequate level of data protection or
2. the suitability of certain standard contractual clauses or pledges to safeguard sufficient protection to the use of data [Datenverwendung] in a third country

shall be promulgated by the Federal Chancellor [Bundeskanzler] in the Federal Law Gazette according to § 4 BGBlG , Federal Law Gazette I No. 100/2003.

Administrative Matters pursuant to Art. 30 of the Federal Constitution

§ 56. The President of the National Council [Nationalrat] is the controller [Auftraggeber] of such data applications [Datenanwendungen] for purposes of such matters with which he has been entrusted pursuant to art. 30 B VG . Transmissions of data [Übermittlungen] from such data applications shall only take place if ordered by the President of the National Council. The President shall make provisions that in case of a transmission order the requirements of § 7 para. 2 are met and, in particular, that the consent of the data subject [Betroffener] is obtained in such cases where it is necessary pursuant to § 7 para. 2 for lack of another legal basis for the transmission.

Gender-Neutral Use of Language

§ 57. Insofar as expressions relating to natural persons in this article are given only in the male form, they shall apply to males and females equally. When the expressions are applied to specific natural persons, the form specific to the gender shall be used.

Manuelle Dateien

§ 58. Soweit manuell, dh. ohne Automationsunterstützung geführte Dateien für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenanwendungen im Sinne des § 4 Z 7. § 17 gilt mit der Maßgabe, daß die Meldepflicht nur für solche Dateien besteht, deren Inhalt gemäß § 18 Abs. 2 der Vorabkontrolle unterliegt.

Umsetzungshinweis

§ 59. Mit diesem Bundesgesetz wird die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S 31, umgesetzt.

Inkrafttreten

§ 60. (1) (Anm.: Durch Art. 2 § 2 Abs. 1 Z 24 und Abs. 2 Z 71, BGBl. I Nr. 2/2008, als nicht mehr geltend festgestellt.)

(2) Die übrigen Bestimmungen dieses Bundesgesetzes treten ebenfalls mit 1. Jänner 2000 in Kraft.

(3) §§ 26 Abs. 6 und 52 Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 136/2001 treten mit 1. Jänner 2002 in Kraft.

(4) § 48a Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. 135/2009 tritt mit 1. Jänner 2010 in Kraft.

(5) Das Inhaltsverzeichnis, § 4 Abs. 1 Z 4, 5, 7 bis 9, 11 und 12, § 8 Abs. 1, 2 und 4, § 12 Abs. 1, die Umnummerierung der Absätze in § 13, § 16 Abs. 1 und 3, § 17 Abs. 1, 1a und 4, § 19 Abs. 1 Z 3a und Abs. 2, die Umnummerierung der Absätze in § 19, die §§ 20 bis 22a samt Überschriften, § 24 Abs. 2a, § 24 Abs. 4, § 26 Abs. 1 bis 8 und 10, § 28 Abs. 3, § 30 Abs. 2a, 5 bis 6a, die §§ 31 und 31a samt Überschriften, § 32 Abs. 1, 4, 6 und 7, § 34 Abs. 1, 3 und 4, § 36 Abs. 3, 3a und 9, § 39 Abs. 5, § 40 Abs. 1 und 2, § 41 Abs. 2 Z 4a, § 42 Abs. 1 Z 1, § 42 Abs. 5, § 46 Abs. 1 Z 2 und 3, Abs. 2 bis 3a, § 47 Abs. 4, § 49 Abs. 3, § 50 Abs. 1 bis 2a, der 9a. Abschnitt, § 51, § 52 Abs. 2 und 4, § 55, § 61 Abs. 6 bis 9 sowie § 64 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 treten mit 1. Jänner 2010 in Kraft. Gleichzeitig treten § 4 Abs. 1 Z 10, § 13 Abs. 3 sowie § 51 Abs. 2 außer Kraft.

Manual Filing Systems

§ 58. Insofar as manual filing systems, i.e., filing systems [Dateien] managed without automatic processing, exist for such purposes and fields where the Federation [Bund] has the power to pass laws, they are deemed to be data applications [Daten¬anwendungen] according to § 4 sub-para. 7. § 17 shall apply insofar as the obligation to notification applies only to those filing systems whose content is subject to prior checking [Vorabkontrolle] according to § 18 para. 2.

Implementation Notice

§ 59. This Federal Act [Bundesgesetz] implements the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23 November 1995 p. 31 .

Entry into Force

§ 60. (Note: Repealed by Federal Law Gazette I No. 2/2008)

(2) The other provisions of this Federal Act shall enter into force on 1 January 2000 as well.

(3) Sects. 26 para. 6 and 52 para. 1 and 2 as formulated in the federal law published in Federal Law Gazette I No. 136/2001 shall enter into force on 1 January 2002.

(4) § 48a para 5 in the version of the Federal Act, Federal Law Gazette I No. 135/2009 enters into force on 1st January 2010.

(5) The table of contents, § 4 para 1 sub-para. 4, 5, 7 to 9, 11 and 12, § 8 para 1, 2 and 4, § 12 para 1, the re-numbering of the paragraphs in § 13, § 16 para 1 and 3, § 17 para 1, 1a and 4, § 19 para 1 sub-para. 3a and para 2, the re-numbering of the paragraphs in § 19, the §§ 20 to 22a including captions, § 24 para 2a, § 24 para 4, § 26 para 1 to 8 and 10, § 28 para 3, § 30 para 2a, 5 to 6a, the §§ 31 and 31a including captions, § 32 para 1, 4, 6 and 7, § 34 para 1, 3 and 4, § 36 para 3, 3a and 9, § 39 para 5, § 40 para 1a and 2, § 41 para 2 sub-para. 4a, § 42 para 1 sub-para. 1, § 42 para 5, § 46 para 1 sub-para. 2 and 3, para 2 to 3a, § 47 para 4, § 49 para 3, § 50 para 1 to 2a, chapter 9a., § 51, § 52 para 2 and 4, § 55, § 61 para 6 to 9 as well as § 64 in the version of the Federal Act, Federal Law Gazette I No. 133/2009, enter into force on 1st January 2010. Simultaneously § 4 para 1 v 10, § 13 para 3 as well as § 51 para 2 become ineffective.

(6) § 36 Abs. 6 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 tritt am 1. Juli 2010 in Kraft.

(6a) § 37 Abs. 2, § 38 Abs. 2 und § 61 Abs. 9 in der Fassung des Bundesgesetzes BGBl. I Nr. 57/2013 treten mit 1. Mai 2013 in Kraft.

(7) Das Inhaltverzeichnis, § 5 Abs. 4, § 10 Abs. 2, § 12 Abs. 4, § 13 Abs. 1, 2 Z 2, Abs. 3, 4 und 6, § 16 Abs. 1, § 17 Abs. 1, § 18 Abs. 2, § 19 Abs. 1 Z 6 und Abs. 2, § 20 Abs. 2 und 5 Z 2, § 21 Abs. 1 Z 3, § 22 Abs. 2 bis 4, § 22a Abs. 1, 3 bis 5, § 23 Abs. 2, § 26 Abs. 2, 5 und 7, § 27 Abs. 5 und 7, die Überschrift zu § 30, § 30 Abs. 1, 2, 2a, 4 bis 6a, die Überschrift zu § 31, § 31 Abs. 1, 2, 5, 6 und 8, § 31a, § 32 Abs. 5 bis 7, § 34 Abs. 3 und 4, die Überschrift zu § 35, § 35 Abs. 1, §§ 36 bis 40 samt Überschriften, § 41 Abs. 2 Z 1, § 44 Abs. 6 und 8, § 46 Abs. 2 Z 3 und Abs. 3, § 47 Abs. 3 und 4, § 48a Abs. 2, § 50 Abs. 1 und 2, § 50b Abs. 2, § 50c Abs. 1, § 52 Abs. 2 Z 2 und 3 sowie Abs. 5, § 54 Abs. 2 und § 61 Abs. 8 bis 10 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 treten mit 1. Jänner 2014 in Kraft. Gleichzeitig treten § 41 Abs. 2 Z 4a und die DSK-Vergütungsverordnung, BGBl. II Nr. 145/2006, außer Kraft. Die für die Bestellung des Leiters der Datenschutzbehörde und seines Stellvertreters notwendigen organisatorischen und personellen Maßnahmen können bereits vor Inkrafttreten des Bundesgesetzes BGBl. I Nr. 83/2013 getroffen werden.

(8) **(Verfassungsbestimmung)** § 2 Abs. 2 und § 35 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 treten mit 1. Jänner 2014 in Kraft.

Übergangsbestimmungen

§ 61. (1) Meldungen, die vor Inkrafttreten dieses Bundesgesetzes an das Datenverarbeitungsregister erstattet wurden, gelten als Meldungen im Sinne des § 17, soweit sie nicht im Hinblick auf das Entfallen von Meldepflichten gemäß § 17 Abs. 2 oder 3 gegenstandslos geworden sind. Desgleichen gelten vor Inkrafttreten dieses Bundesgesetzes durchgeführte Registrierungen als Registrierungen im Sinne des § 21.

(2) Soweit nach der neuen Rechtslage eine Genehmigung für die Übermittlung von Daten ins Ausland erforderlich ist, muß für Übermittlungen, für die eine Genehmigung vor Inkrafttreten dieses Bundesgesetzes erteilt wurde, eine Genehmigung vor dem 1. Jänner 2003 neu beantragt werden. Wird der Antrag rechtzeitig gestellt, dürfen solche Übermittlungen bis zur rechtskräftigen Entscheidung über den Genehmigungsantrag fortgeführt werden.

(6) § 36 para 6 in the version of the Federal Act, Federal Law Gazette I No. 133/2009, enters into force on 1 July 2010.

(6a) § 37 para. 2, § 38 para. 2 und § 61 para. 9 in the version of the Federal Act, Federal Law Gazette I No. 57/2013 enter into force on 1 May 2013.

(7) The table of contents, § 5 para. 4, § 10 para. 2, § 12 para. 4, § 13 para. 1, 2 Z 2, para. 3, 4 and 6, § 16 para. 1, § 17 para. 1, § 18 para. 2, § 19 para. 1 sub-para. 6 and para. 2, § 20 para. 2 and 5 sub-para. 2, § 21 para. 1 sub-para. 3, § 22 para. 2 up to 4, § 22a para. 1, 3 till 5, § 23 para. 2, § 26 para. 2, 5 and 7, § 27 para. 5 and 7, the title of § 30, § 30 para. 1, 2, 2a, 4 up to 6a, the title of § 31, § 31 para. 1, 2, 5, 6 and 8, § 31a, § 32 para. 5 up to 7, § 34 para. 3 and 4, the title of § 35, § 35 para. 1, §§ 36 up to 40 including titles, § 41 para. 2 sub-para. 1, § 44 para. 6 and 8, § 46 para. 2 sub-para. 3 and para. 3, § 47 para. 3 and 4, § 48a para. 2, § 50 para. 1 and 2, § 50b para. 2, § 50c para. 1, § 52 para. 2 sub-para. 2 and 3 as well as para. 5, § 54 para. 2 and § 61 para. 8 up to 10 in the version of the Federal Act Federal Law Gazette I No. 83/2013 enter into force on 1 January 2014. Simultaneously, § 41 para. 2 sub-para. 4a and the Reimbursement Ordinance of the Data Protection Commission [DSK-Vergütungsverordnung], Federal Law Gazette II No. 145/2006, become ineffective. All organisational and human resource measures needed to appoint the head of the Data Protection Authority and the deputy may be implementend before the Federal Act Federal Law Gazette I No. 83/2013 enters into force.

(8) **(Constitutional provision)** § 2 para. 2 and § 35 para. 2 in the version of the Federal Act, Federal Law Gazette I Nr. 83/2013 enter into force on 1 January 2014.

Transitional Provisions

§ 61. (1) Notifications that were made to the Data Processing Register [Datenverarbeitungsregister] before this Federal Act [Bundesgesetz] entered into force shall count as notifications according to § 17, insofar as they have not become irrelevant because the obligation to notify is no longer applicable. Likewise, registrations made before this Federal Act entered into force shall count as registrations according to § 21.

(2) Insofar as the law as it now stands requires a permit for transborder data transmission [Übermittlung], an application for a new permit must be filed before 1 January 2003 for such transmissions for which a permit was granted prior to this Federal Acts entry into force. If the application is filed in time, such transmissions may be carried out until the final decision about the application for the permit.

(3) Datenschutzverletzungen, die vor dem Inkrafttreten dieses Bundesgesetzes stattgefunden haben, sind, soweit es sich um die Feststellung der Rechtmäßigkeit oder Rechtswidrigkeit eines Sachverhalts handelt, nach der Rechtslage zum Zeitpunkt der Verwirklichung des Sachverhalts zu beurteilen; soweit es sich um die Verpflichtung zu einer Leistung oder Unterlassung handelt, ist die Rechtslage im Zeitpunkt der Entscheidung in erster Instanz zugrundezulegen. Ein strafbarer Tatbestand ist nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist; dies gilt auch für das Rechtsmittelverfahren.

(4) **(Verfassungsbestimmung)** Datenanwendungen, die für die in § 17 Abs. 3 genannten Zwecke notwendig sind, dürfen auch bei Fehlen einer im Sinne des § 1 Abs. 2 ausreichenden gesetzlichen Grundlage bis 31. Dezember 2007 vorgenommen werden, in den Fällen des § 17 Abs. 3 Z 1 bis 3 jedoch bis zur Erlassung von bundesgesetzlichen Regelungen über die Aufgaben und Befugnisse in diesen Bereichen.

(5) Manuelle Datenanwendungen, die gemäß § 58 der Meldepflicht unterliegen, sind, soweit sie schon im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bestanden haben, dem Datenverarbeitungsregister bis spätestens 1. Jänner 2003 zu melden. Dasselbe gilt für automationsunterstützte Datenanwendungen gemäß § 17 Abs. 3, für die durch die nunmehr geltende Rechtslage die Meldepflicht neu eingeführt wurde.

(6) Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, bleiben in ihrer registrierten Form rechtmäßig, wenn sie den am 31. Dezember 2009 geltenden datenschutzrechtlichen Bestimmungen genügen und die Datenschutzkommission keine Befristung verfügt hat. Hat die Datenschutzkommission hingegen eine Befristung einer solchen Videoüberwachung verfügt, bleibt diese bis zum Ablauf der Befristung, längstens aber bis zum 31. Dezember 2012 rechtmäßig.

(7) Soweit in einzelnen Vorschriften Verweise auf das Datenschutzgesetz, BGBl. Nr. 565/1978, enthalten sind, gelten diese bis zu ihrer Anpassung an dieses Bundesgesetz sinngemäß weiter.

(8) Die Verordnung nach § 16 Abs. 3 ist vom Bundeskanzler nach Maßgabe der technischen Möglichkeiten des Datenverarbeitungsregisters bis spätestens 1. September 2012 neu zu erlassen. Bis zum Inkrafttreten dieser Verordnung sind die §§ 16 bis 22, § 30 Abs. 3 und 6 sowie § 40 Abs. 1 (letzterer mit Ausnahme des Verweises auf § 31a Abs. 3) in der Fassung vor dem Bundesgesetz BGBl. I Nr. 133/2009 anzuwenden; § 22a, § 30 Abs. 2a und 6a, § 31a Abs. 1 und 2 sowie § 32 Abs. 7 sind bis dahin nicht anzuwenden. § 31 Abs. 3 in der Fassung vor dem Bundesgesetz BGBl. I Nr. 133/2009 ist bis dahin zusätzlich weiter anzuwenden. Die Erklärung, ob eine Datenanwendung

(3) Data protection violations that have taken place before this Federal Act entered into force shall, insofar as the legality or illegality of a set of facts is concerned, be adjudicated according to the legal provisions in force at the time the act was committed; insofar as an obligation to act or a forbearance is concerned, the law as its stands at the time when the decision of first instance is rendered shall be applied. A criminal offence shall be adjudicated according to the law that is more favourable to the offender overall; this also extends to appeal proceedings.

(4) **(Constitutional provision)** Data applications [Daten¬anwendungen] that are required for the purposes laid down in § 17 para. 3 may be continued even without a sufficient legal basis in terms of § 1 para. 2 until 31 December 2007, in the cases of § 17 para. 3 sub-para. 1 to 3 until federal regulations covering the functions and powers in these fields are enacted.

(5) Manual filing systems subject to notification according to § 58 shall be notified to the Data Processing Register no later than 1 January 2003, provided they already existed when this Federal Act entered into force. The same shall apply to automated data applications according to § 17 para. 3 that were made subject to notification by the new regulations.

(6) Notifications for video surveillance that were registered before §§ 50a to 50e entered into force remain lawful in the registered version if they correspond with the regulations on data protection in force on 31 December 2009 and the Data Protection Commission has not imposed a time limit. If, however, the Data Protection Commission has imposed a time limit for such video surveillance, it remains lawful till the time limit has expired, the latest till 31 December 2012.

(7) Insofar as individual provisions contain references to the Data Protection Act [Datenschutzgesetz], Federal Law Gazette No. 565/1978, such provisions shall be valid by analogous application until adjusted to conform to this Federal Act.

(8) The ordinance according to § 16 para 3 shall be re-issued by the Federal Chancellor, in accordance with the technical possibilities of the data processing register, on 1st September 2012 at the latest. Until this ordinance enters into force §§ 16 to 22, § 30 para 3 and 6 as well as § 40 para 1 (the latter with the exception of the reference to § 31a para 3) in the version of the Federal Act, Federal Law Gazette I No. 133/2009, is to be applied, § 22a, § 30 para 2a and 6a, § 31a para 1 and 2 as well as § 32 para 7 are not to be applied; up to such date. § 31 para 3 in the version before the Federal Act, Federal Law Gazette I No. 133/2009, is, in addition, to be applied. The

einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 genannten Tatbestände erfüllt (§ 19 Abs. 1 Z 3a), ist der Datenschutzkommission bei im Zeitpunkt des Inkrafttretens der neuen Verordnung nach § 16 Abs. 3 registrierten Datenanwendungen anlässlich der ersten über eine Streichung hinausgehenden Änderungsmeldung zu melden, die nach diesem Zeitpunkt erstattet wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 3a ist nicht erforderlich.

(9) Mit Ablauf des 31. Dezember 2013 tritt die Datenschutzbehörde an die Stelle der Datenschutzkommission. Zum Zeitpunkt des Inkrafttretens des Bundesgesetzes BGBl. I Nr. 83/2013 bei der Datenschutzkommission anhängige Verfahren sind nach Maßgabe der Bestimmungen dieses Bundesgesetzes in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 von der Datenschutzbehörde fortzuführen. Erledigungen der Datenschutzkommission gelten als entsprechende Erledigungen der Datenschutzbehörde. Die Bestimmungen des Verwaltungsgerichtsbarkeits-Übergangsgesetzes, BGBl. I Nr. 83/2013, bleiben unberührt. Nach Beendigung des Verfahrens vor dem Verwaltungsgerichtshof betreffend den Bescheid oder die Säumnis der Datenschutzkommission oder vor dem Verfassungsgerichtshof betreffend den Bescheid der Datenschutzkommission ist das Verfahren von der Datenschutzbehörde fortzusetzen.

(10) Die Bediensteten der Datenschutzkommission werden mit Inkrafttreten des BGBl. I Nr. 83/2013 als Bedienstete der Datenschutzbehörde übernommen.

Verordnungserlassung

§ 62. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

Verweisungen

§ 63. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollziehung

§ 64. Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung obliegt, der Bundeskanzler und die anderen Bundesminister im Rahmen ihres Wirkungsbereiches betraut.

statement, whether a data application matches at least one of the elements of § 18 para 2 sub-para. 1 to 4 (§ 19 para 1 sub-para. 3a), is to be notified to the data protection commission for data applications which are already registered when the new ordinance according to § 16 para 3 enters in to force at the occasion of the first notification of any change other than deletion. A notification solely with regard to § 19 para 1 sub-para. 3a is not necessary.

(9) The Data Protection Authority [Datenschutzbehörde] shall take the place of the Data Protection Commission [Datenschutzkommission] after 31 December 2013. Cases that have already been brought before the Data Protection Commission before the Federal Act, Federal Law Gazette I No. 83/2013, entered into force shall continue according to the provisions of this federal act in the version of Federal Law Gazette I No. 83/2013. Decisions of the Data Protection Commission shall count as equivalent decisions of the Data Protection Authority. The provisions of the Administrative Jurisdiction Transition Act, Federal Law Gazette I No. 83/2013, are unaffected. After the end of a procedure before the Administrative Court [Verwaltungsgerichtshof] concerning a ruling of the Data Protection Commission or an illegal delay or before the Constitutional Court [Verfassungsgerichtshof] concerning a ruling of the Data Protection Commission the procedure shall continue before the Data Protection Authority.

(10) The staff of the Data Protection Commission shall become staff of the Data Protection Authority once Federal Law Gazette I No. 83/2013 enters into force.

Enactment of Ordinances

§ 62. Ordinances [Verordnungen] based on this Federal Act [Bundesgesetz] in the current version in force may already be enacted as of the day following the promulgation of the legal provision to be implemented; they shall, however, not enter into force before the statutory provisions which are to be implemented.

References

§ 63. Insofar as provisions of this Federal Act [Bundesgesetz] refer to provisions of other Federal Acts, these shall be applied in the current version in force.

Execution

§ 64. The Federal Chancellor [Bundeskanzler] and the other Federal Ministers [Bundesminister] within their purview shall execute this Federal Act [Bundesgesetz] insofar as the execution has not been entrusted to the Federal Government [Bundesregierung].

Federal Act on Data Protection
(FADP)

of 19 June 1992 (Status as of 1 January 2014)

The Federal Assembly of the Swiss Confederation,

based on Articles 95, 122 and 173 paragraph 2 of the Federal Constitution[1],[2] and having regard to the Federal Council Dispatch dated 23 March 1988[3],

decrees:

Section 1: Aim, Scope and Definitions

Art. 1 Aim

This Act aims to protect the privacy and the fundamental rights of persons when their data is processed.

Art. 2 Scope

1 This Act applies to the processing of data pertaining to natural persons and legal persons by:

a. private persons;

b. federal bodies.

2 It does not apply to:

a. personal data that is processed by a natural person exclusively for personal use and which is not disclosed to outsiders;

b. deliberations of the Federal Assembly and in parliamentary committees;

AS **1993** 1945

1 SR **101**

2 Amended by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

3 BBl **1988** II 413

c. pending civil proceedings, criminal proceedings, international mutual assistance proceedings and proceedings under constitutional or under administrative law, with the exception of administrative proceedings of first instance;

d. public registers based on private law;

e. personal data processed by the International Committee of the Red Cross.

Art. 3 Definitions

The following definitions apply:

a. *personal data (data):* all information relating to an identified or identifiable person;

b. *data subjects:* natural or legal persons whose data is processed;

c. *sensitive personal data:* data on:
   1. religious, ideological, political or trade union-related views or activities,
   2. health, the intimate sphere or the racial origin,
   3. social security measures,
   4. administrative or criminal proceedings and sanctions;

d. *personality profile:* a collection of data that permits an assessment of essential characteristics of the personality of a natural person;

e. *processing:* any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data;

f. *disclosure:* making personal data accessible, for example by permitting access, transmission or publication;

g. *data file:* any set of personal data that is structured in such a way that the data is accessible by data subject;

h. *federal bodies:* federal authorities and services as well as persons who are entrusted with federal public tasks;

i.[4] *controller of the data file:* private persons or federal bodies that decide on the purpose and content of a data file;

j.[5] *formal enactment:*
   1. federal acts,
   2. decrees of international organisations that are binding on Switzerland and international treaties containing legal rules that are approved by the Federal Assembly;

4 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

5 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

k.[6] …

Section 2: General Data Protection Provisions

Art. 4 Principles

[1] Personal data may only be processed lawfully.[7]

[2] Its processing must be carried out in good faith and must be proportionate.

[3] Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law.

[4] The collection of personal data and in particular the purpose of its processing must be evident to the data subject.[8]

[5] If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information. Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles.[9]

Art. 5 Correctness of the data

[1] Anyone who processes personal data must make certain that it is correct. He must take all reasonable measures to ensure that data that is incorrect or incomplete in view of the purpose of its collection is either corrected or destroyed.[10]

[2] Any data subject may request that incorrect data be corrected.

Art. 6[11] Cross-border disclosure

[1] Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.

[2] In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:

6 Repealed by No. I of the Federal Act of 24 March 2006, with effect from 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
7 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
8 Inserted by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
9 Inserted by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
10 Second sentence inserted by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
11 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;

b. the data subject has consented in the specific case;

c. the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;

d. disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;

e. disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;

f. the data subject has made the data generally accessible and has not expressly prohibited its processing;

g. disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection.

3 The Federal Data Protection and Information Commissioner (the Commissioner, Art. 26) must be informed of the safeguards under paragraph 2 letter a and the data protection rules under paragraph 2 letter g. The Federal Council regulates the details of this duty to provide information.

Art. 7 Data security

1 Personal data must be protected against unauthorised processing through adequate technical and organisational measures.

2 The Federal Council issues detailed provisions on the minimum standards for data security.

Art. 7*a*[12]

Art. 8 Right to information

1 Any person may request information from the controller of a data file as to whether data concerning them is being processed.

2 The controller of a data file must notify the data subject:[13]

12 Inserted by No. I of the Federal Act of 24 March 2006 (AS **2007** 4983; BBl **2003** 2101). Repealed by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, with effect from 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

13 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

a.[14] of all available data concerning the subject in the data file, including the available information on the source of the data;

b. the purpose of and if applicable the legal basis for the processing as well as the categories of the personal data processed, the other parties involved with the file and the data recipient.

3 The controller of a data file may arrange for data on the health of the data subject to be communicated by a doctor designated by the subject.

4 If the controller of a data file has personal data processed by a third party, the controller remains under an obligation to provide information. The third party is under an obligation to provide information if he does not disclose the identity of the controller or if the controller is not domiciled in Switzerland.

5 The information must normally be provided in writing, in the form of a printout or a photocopy, and is free of charge. The Federal Council regulates exceptions.

6 No one may waive the right to information in advance.

Art. 9[15] Limitation of the duty to provide information

1 The controller of a data file may refuse, restrict or defer the provision of information where:

a. a formal enactment so provides;

b. this is required to protect the overriding interests of third parties.

2 A federal body may further refuse, restrict or defer the provision of information where:

a. this is required to protect overriding public interests, and in particular the internal or external security of the Confederation;

b. the information would jeopardise the outcome of a criminal investigation or any other investigation proceedings.

3 As soon as the reason for refusing, restricting or deferring the provision of information ceases to apply, the federal body must provide the information unless this is impossible or only possible with disproportionate inconvenience or expense.

4 The private controller of a data file may further refuse, restrict or defer the provision of information where his own overriding interests so require and he does not disclose the personal data to third parties.

5 The controller of a data file must indicate the reason why he has refused, restricted or deferred access to information.

14 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

15 Amended by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

Art. 10 Limitations of the right to information for journalists

1 The controller of a data file that is used exclusively for publication in the edited section of a periodically published medium may refuse to provide information, limit the information or defer its provision provided:

a. the personal data reveals the sources of the information;

b. access to the drafts of publications would have to be given;

c. the freedom of the public to form its opinion would be prejudiced.

2 Journalists may also refuse restrict or defer information if the data file is being used exclusively as a personal work aid.

Art. 10*a*[16] Data processing by third parties

1 The processing of personal data may be assigned to third parties by agreement or by law if:

a. the data is processed only in the manner permitted for the instructing party itself; and

b. it is not prohibited by a statutory or contractual duty of confidentiality.

2 The instructing party must in particular ensure that the third party guarantees data security.

3 Third parties may claim the same justification as the instructing party.

Art. 11[17] Certification procedure

1 In order to improve data protection and data security, the manufacturers of data processing systems or programs as well as private persons or federal bodies that process personal data may submit their systems, procedures and organisation for evaluation by recognised independent certification organisations.

2 The Federal Council shall issue regulations on the recognition of certification procedures and the introduction of a data protection quality label. In doing so, it shall take account of international law and the internationally recognised technical standards.

Art. 11*a*[18] Register of data files

1 The Commissioner maintains a register of data files that is accessible online. Anyone may consult the register.

16 Inserted by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
17 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
18 Inserted by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

2 Federal bodies must declare all their data files to the Commissioner in order to have them registered.

3 Private persons must declare their data files if:

a. they regularly process sensitive personal data or personality profiles; or

b. they regularly disclose personal data to third parties.

4 The data files must be declared before they are opened.

5 In derogation from the provisions in paragraphs 2 and 3, the controller of data files is not required to declare his files if:

a. private persons are processing the data in terms of a statutory obligation;

b. the Federal Council has exempted the processing from the registration requirement because it does not prejudice the rights of the data subjects;

c. he uses the data exclusively for publication in the edited section of a periodically published medium and does not pass on any data to third parties without informing the data subjects;

d. the data is processed by journalists who use the data file exclusively as a personal work aid;

e. he has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files;

f. he has acquired a data protection quality mark under a certification procedure in accordance with Article 11 and has notified the Commissioner of the result of the evaluation.

6 The Federal Council regulates the modalities for the declaration of data files for registration, the maintenance and the publication of the register, the appointment and duties of the data protection officer under paragraph 5 letter e and the publication of a list of controllers of data files that are relieved of the reporting obligation under paragraph 5 letters e and f.

Section 3: Processing of Personal Data by Private Persons

Art. 12 Breaches of privacy

1 Anyone who processes personal data must not unlawfully breach the privacy of the data subjects in doing so.

2 In particular, he must not:

a. process personal data in contravention of the principles of Articles 4, 5 paragraph 1 and 7 paragraph 1;

b. process data pertaining to a person against that person's express wish without justification;

c. disclose sensitive personal data or personality profiles to third parties without justification.[19]

3 Normally there is no breach of privacy if the data subject has made the data generally accessible and has not expressly prohibited its processing.

Art. 13 Justification

1 A breach of privacy is unlawful unless it is justified by the consent of the injured party, by an overriding private or public interest or by law.

2 An overriding interest of the person processing the data shall in particular be considered if that person:

a. processes personal data in direct connection with the conclusion or the performance of a contract and the personal data is that of a contractual party;

b. is or intends to be in commercial competition with another and for this purpose processes personal data without disclosing the data to third parties;

c. process data that is neither sensitive personal data nor a personality profile in order to verify the creditworthiness of another, and discloses such data to third parties only if the data is required for the conclusion or the performance of a contract with the data subject;

d. processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium;

e. processes personal data for purposes not relating to a specific person, in particular for the purposes of research, planning and statistics and publishes the results in such a manner that the data subjects may not be identified;

f. collects data on a person of public interest, provided the data relates to the public activities of that person.

Art. 14[20] Duty to provide information on the collection of sensitive personal data and personality profiles

1 The controller of the data file is obliged to inform the data subject of the collection of sensitive personal data or personality profiles; this duty to provide information also applies where the data is collected from third parties.

2 The data subject must be notified as a minimum of the following:

a. the controller of the data file;

19 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

20 Repealed by No. I of the Federal Act of 24 March 2006 (AS **2007** 4983; BBl **2003** 2101). Amended by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

b. the purpose of the processing;

c. the categories of data recipients if a disclosure of data is planned.

3 If the data is not collected from the data subject, the data subject must be informed at the latest when the data is stored or if the data is not stored, on its first disclosure to a third party.

4 The duty of the controller of the data file to provide information ceases to apply if the data subject has already been informed or, in cases under paragraph 3, if:

a. the storage or the disclosure of the data is expressly provided for by law; or

b. the provision of information is not possible or possible only with disproportionate inconvenience or expense.

5 The controller of the data file may refuse, restrict or defer the provision of information subject to the requirements of Article 9 paragraphs 1 and 4.

Art. 15[21] Legal claims

1 Actions relating to protection of privacy are governed by Articles 28, 28*a* and 28*l* of the Civil Code[22]. The plaintiff may in particular request that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed.

2 Where it is impossible to demonstrate that personal data is accurate or inaccurate, the plaintiff may request that a note to this effect be added to the data.

3 The plaintiff may request that notification of third parties or the publication of the correction, destruction, blocking, and in particular the prohibition of disclosure to third parties, the marking of the data as disputed or the court judgment.

4 Actions on the enforcement of a right to information shall be decided by the courts in a simplified procedure under the Civil Procedure Code of 19 December 2008[23]

Section 4: Processing of Personal Data by Federal Bodies

Art. 16 Responsible body and controls[24]

1 The federal body that processes or arranges for the processing of personal data in fulfilment of its tasks is responsible for data protection.

21 Amended by Annex 1 No. II 14 of the Civil Procedure Code of 19 Dec. 2008, in force since 1 Jan. 2011 (AS **2010** 1739; BBl **2006** 7221).
22 SR **210**
23 SR **272**
24 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

2 If federal bodies process personal data together with other federal bodies, with cantonal bodies or with private persons, the Federal Council may specifically regulate the control of and responsibility for data protection.[25]

Art. 17 Legal basis

1 Federal bodies may process personal data if there is a statutory basis for doing so.

2 They may process sensitive personal data and personality profiles only if a formal enactment expressly provides therefor or if, by way of exception:

a. such processing is essential for a task clearly defined in a formal enactment;

b. the Federal Council authorises processing in an individual case because the rights of the data subject are not endangered; or

c. the data subject has given his consent in an individual case or made his data general accessible and has not expressly prohibited its processing.[26]

Art. 17*a*[27] Automated data processing in pilot projects

1 The Federal Council may, having consulted the Commissioner and before a formal enactment comes into force, approve the automated processing of sensitive personal data or personality profiles if:

a. the tasks that require such processing required are regulated in a formal enactment;

b. adequate measures are taken to prevent breaches of privacy;

c. a test phase before the formal enactment comes into force is indispensable for the practical implementation of data processing.

2 A test phase may be mandatory for the practical implementation of data processing if:

a. the fulfilment of a task requires technical innovations, the effects of which must first be evaluated;

b. the fulfilment of a task requires significant organisational or technical measures, the effectiveness of which must first be tested, in particular in the case of cooperation between federal and the cantonal bodies; or

c. processing requires that sensitive personal data or personality profiles be transmitted online to cantonal authorities.

25 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

26 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

27 Inserted by No. I of the Federal Act of 24 March 2006 (AS **2006** 4873; BBl **2003** 2101, **2006** 3547). Amended by No. I of the Federal Act of 24 March 2006, in force since 15 Dec. 2006 (AS **2007** 4983 4991; BBl **2003** 2101).

3 The Federal Council shall regulate the modalities of automated data processing in an ordinance.

4 The competent federal body shall provide the Federal Council with an evaluation report at the latest within two years of the pilot system coming into operation. The report contains a proposal on whether the processing should be continued or terminated.

5 Automated data processing must be terminated in every case if within five years of the pilot systems coming into operation no formal enactment has come in force that contains the required legal basis.

Art. 18 Collection of personal data

1 In the case of systematic surveys, in particular by means of questionnaires, the federal organ shall disclose the purpose of and the legal basis for the processing, and the categories of persons involved with the data file and of the data recipients.

2 …[28]

Art. 18*a*[29] Duty to provide information on the collection of personal data

1 Federal bodies are obliged to inform the data subject of the collection of personal data; this duty to provide information also applies where the data is collected from third parties.

2 The data subject must be notified as a minimum of the following:

a. the controller of the data file;

b. the purpose of processing;

c. the categories of the data recipients where a disclosure of data is planned;

d. the right to information in accordance with Article 8;

e. the consequences of the refusal of the data subject to provide the requested personal data.

3 If the data is not collected from the data subject, the data subject must be informed at the latest when the data is stored or if the data is not stored, on its first disclosure to a third party.

4 The duty of the controller of the data file to provide information ceases to apply if the data subject has already been informed or, in cases under paragraph 3, if:

a. the storage or the disclosure of the data is expressly provided for by law; or

28 Repealed by No. I of the Federal Act of 24 March 2006, with effect from 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

29 Inserted by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

b. the provision of information is not possible or possible only with disproportionate inconvenience or expense.

5 If the duty to provide information would compromise the competitiveness of a federal body, the Federal Council may limit the application of the duty to the collection of sensitive personal data and personality profiles.

Art. 18*b*[30] Restriction of the duty to provide information

1 Federal bodies may refuse, restrict or defer the provision of information subject to the requirements of Article 9 paragraphs 1 and 2.

2 As soon as the reason for refusal, restriction or deferral ceases to apply, the federal bodies are bound by the duty to provide information unless compliance is not possible or possible only with disproportionate inconvenience or expense.

Art. 19 Disclosure of personal data

1 Federal bodies may disclose personal data if there is legal basis for doing so in accordance with Article 17 or if:[31]

a. the data is indispensable to the recipient in the individual case for the fulfilment of his statutory task;

b.[32] the data subject has consented in the individual case;

c.[33] the data subject has made the data generally accessible and has not expressly prohibited disclosure; or

d. the recipient demonstrates credibly that the data subject is withholding consent or blocking disclosure in order to prevent the enforcement of legal claims or the safeguarding of other legitimate interests; the data subject must if possible be given the opportunity to comment beforehand.

1bis Federal bodies may also disclose personal data within the terms of the official information disclosed to the general public, either ex officio or based on the Freedom of Information Act of 17 December 2004[34] if:

a. the personal data concerned is connected with the fulfilment of public duties; and

30 Inserted by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

31 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983; BBl **2003** 2101).

32 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

33 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

34 SR **152.3**

b. there is an overriding public interest in its disclosure.[35]

2 Federal bodies may on request also disclose the name, first name, address and date of birth of a person if the requirements of paragraph 1 are not fulfilled.

3 Federal bodies may make personal data accessible online if this is expressly provided for. Sensitive personal data and personality profiles may be made accessible online only if this is expressly provided for in a formal enactment.[36]

3bis Federal bodies may make personal data generally accessible by means of automated information and communication services if a legal basis is provided for the publication of such data or if they make information accessible to the general public on the basis of paragraph 1bis. If there is no longer a public interest in the accessibility of such data, the data concerned must be removed from the automated information and communication service.[37]

4 The federal body shall refuse or restrict disclosure, or make it subject to conditions if:

a. essential public interests or clearly legitimate interests of a data subject so require or

b. statutory duties of confidentiality or special data protection regulations so require.

Art. 20 Blocking disclosure

1 A data subject that credibly demonstrates a legitimate interest may request the federal body concerned to block the disclosure of certain personal data.

2 The federal body shall refuse to block disclosure or lift the block if:

a. there is a legal duty of disclosure; or

b. the fulfilment of its task would otherwise be prejudiced.

3 Any blocking of disclosure is subject to Article 19 paragraph 1bis.[38]

Art. 21[39] Offering documents to the Federal Archives

1 In accordance with the Archiving Act of 26 June 1998[40], federal bodies shall offer the Federal Archives all personal data that is no longer in constant use.

35 Inserted by Annex No. 4 of the Freedom of Information Act of 17 Dec. 2004, in force since 1 July 2006 (SR **152.3**).
36 Second sentence according to No. I of the Federal Act of 24 March 2006, with effect from 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
37 Inserted by Annex No. 4 of the Freedom of Information Act of 17 Dec. 2004, in force since 1 July 2006 (SR **152.3**).
38 Inserted by Annex No. 4 of the Freedom of Information Act of 17 Dec. 2004, in force since 1 July 2006 (SR **152.3**).
39 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
40 SR **152.1**

2 The federal bodies shall destroy personal data designated by the Federal Archives as not being of archival value unless it:

a. is rendered anonymous;

b.[41] must be preserved on evidentiary or security grounds or in order to safeguard the legitimate interests of the data subject.

Art. 22 Processing for research, planning and statistics

1 Federal bodies may process personal data for purposes not related to specific persons, and in particular for research, planning and statistics, if:

a. the data is rendered anonymous, as soon as the purpose of the processing permits;

b. the recipient only discloses the data with the consent of the federal body and

c. the results are published in such a manner that the data subjects may not be identified.

2 The requirements of the following provisions need not be fulfilled:

a. Article 4 paragraph 3 on the purpose of processing

b. Article17 paragraph 2 on the legal basis for the processing of sensitive personal data and personality profiles;

c. Article 19 paragraph 1 on the disclosure of personal data.

Art. 23 Private law activities of federal bodies

1 If a federal body acts under private law, the provisions for the processing of personal data by private persons apply.

2 Supervision is governed by the provisions on federal bodies.

Art. 24[42]

Art. 25 Claims and procedure

1 Anyone with a legitimate interest may request the federal body concerned to:

a. refrain from processing personal data unlawfully;

b. eliminate the consequences of unlawful processing;

c. ascertain whether processing is unlawful.

41 Amended by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

42 Repealed by Art. 31 of the Federal Act of 21 March 1997 on Measures to Safeguard Internal Security (SR **120**).

2 If it is not possible to prove the accuracy or the inaccuracy of personal data, the federal body must mark the data correspondingly.

3 The applicant may in particular request that the federal body:

a. corrects or destroys the personal data or blocks its disclosure to third parties;

b. communicates its decision to third parties, in particular on the correction, destruction, blocking of the data or marking of the data as disputed, or publishes the decision.

4 The procedure is governed by the Federal Act of 20 December 1968[43] on Administrative Procedure (Administrative Procedure Act). The exceptions contained in Articles 2 and 3 of the Administrative Procedure Act do not apply.

5 …[44]

Art. 25bis [45] Procedure in the event of the disclosure of official documents containing personal data

For as long as proceedings relating to access to official documents within the meaning of the Freedom of Information Act of 17 December 2004[46] that contain personal data are ongoing, the data subject may within the terms of such proceedings claim the rights accorded to him on the basis of Article 25 of this Act in relation to those documents that are the subject matter of the access proceedings.

Section 5: Federal Data Protection and Information Commissioner

Art. 26[47] Appointment and status

1 The Commissioner is appointed by the Federal Council for a term of office of four years. The appointment must be approved by the Federal Assembly.

2 The employment relationship is governed by the Federal Personnel Act of 24 March 2000[48], unless this Act provides otherwise.

2 The Commissioner fulfils his tasks independently without being subject to the directives of any authority. He is assigned to the Federal Chancellery for administrative purposes.

43 SR **172.021**
44 Repealed by Annex No. 26 of the Administrative Court Act of 17 June 2005, with effect from 1 Jan. 2007 (SR **173.32**).
45 Inserted by Annex No. 4 of the Freedom of Information Act of 17 Dec. 2004, in force since 1 July 2006 (SR **152.3**).
46 SR **152.3**
47 Amended by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).
48 SR **172.220.1**

3 He has a permanent secretariat and his own budget. He appoints his own staff.

5 The Commissioner is not subject to the system of assessment under Article 4 paragraph 3 of the Federal Personnel Act of 24 March 2000.

Art. 26*a*[49] Reappointment and termination of the term of office

1 The Commissioner is automatically reappointed for a further term of office unless, at least six months prior to the expiry of his term of office, the Federal Council has issued an order based on materially adequate grounds for the Commissioner not to be reappointed.

2 The Commissioner may request the Federal Council to be discharged from office at the end of any month subject to six months advance notice.

3 The Federal Council may dismiss the Commissioner from office before the expiry of his term of office if he:

a. wilfully or through gross negligence seriously violates his duties of office; or

b. he is permanently unable to fulfil his duties of office.

Art. 26*b*[50] Secondary occupation

The Federal Council may permit the Commissioner to carry on another occupation provided this does not compromise his independence and standing.

Art. 27 Supervision of federal bodies

1 The Commissioner[51] supervises compliance by federal bodies with this Act and other federal data protection regulations of the Confederation. The Federal Council is excluded from such supervision.

2 The Commissioner investigates cases either on his own initiative or at the request of a third party.

3 In investigating cases, he may request the production of files, obtain information and arrange for processed data to be shown to him. The federal bodies must assist in determining the facts of any case. The right to refuse to testify under Article 16 of the Administrative Procedure Act[52] applies by analogy.

49 Inserted by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

50 Inserted by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

51 Title according to Annex No. 4 of the Freedom of Information Act of 17 Dec. 2004, in force since 1 July 2006 (SR **152.3**). This amendment is taken into account throughout this Act.

52 SR **172.021**

4 If the investigation reveals that data protection regulations are being breached, the Commissioner shall recommend that the federal body concerned change the method of processing or abandon the processing. He informs the department concerned or the Federal Chancellery of his recommendation.

5 If a recommendation is not complied with or is rejected, he may refer the matter to the department or to the Federal Chancellery for a decision. The decision is communicated to the data subjects in the form of a ruling.[53]

6 The Commissioner has a right of appeal against the ruling under paragraph 5 and against the decision of the appeal authority.[54]

Art. 28 Advice to private persons

The Commissioner advises private persons on data protection matters.

Art. 29 Investigations and recommendations in the private sector

1 The Commissioner shall investigate cases in more detail on his own initiative or at the request of a third party if:

a. methods of processing are capable of breaching the privacy of larger number of persons (system errors);

b.[55] data files must be registered (Art. 11*a*);

c.[56] there is a duty to provide information in terms of Article 6 paragraph 3.

2 To this end, he may request files, obtain information and arrange for processed data to be shown to him. The right to refuse to testify under Article 16 of the Administrative Procedure Act[57] applies by analogy.

3 On the basis of his investigations, the Commissioner may recommend that the method of processing be changed or abandoned.

4 If a recommendation made by the Commissioner is not complied with or is rejected, he may refer the matter to the Federal Administrative Court for a decision. He has the right to appeal against this decision.[58]

53 Second sentence according to No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
54 Inserted by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
55 Amended by No. I of the Federal Act of 24 March 2006, in force since 1Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
56 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
57 SR **172.021**
58 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

Art. 30 Information

[1] The Commissioner shall submit a report to the Federal Assembly at regular intervals and as required. He shall provide the Federal Council with a copy of the report at the same time. The regular reports are published. [59]

[2] In cases of general interest, he informs the general public of his findings and recommendations. He may only publish personal data subject to official secrecy with consent of the authority responsible. If it refuses its consent, the President of the division of the Federal Administrative Court responsible for data protection makes the final decision.[60]

Art. 31 Additional tasks

[1] The Commissioner has the following additional tasks in particular:[61]

a. he assists federal and cantonal bodies on data protection issues.

b. he provides an opinion on draft federal legislation and on other federal measures that are relevant to data protection.

c. he cooperates with domestic and foreign data protection authorities.

d.[62] he provides an expert opinion on the extent to which foreign data protection legislation guarantees adequate protection.

e.[63] he examines safeguards and data protection rules notified to him under Article 6 paragraph 3.

f.[64] He examines the certification procedure under Article11 and may issue recommendations in accordance with Article 27 paragraph 4 or Article 29 paragraph 3.

g.[65] He carries out the tasks assigned to him under the Freedom of Information Act of 17 December 2004[66].

59 Amended by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

60 Wording of sentence according to Annex No. 26 of the Administrative Court Act of 17 June 2005, in force since 1 Jan. 2007 (SR **173.32**).

61 Amended by Annex No. 4 of the Freedom of Information Act of 17 Dec. 2004, in force since 1 July 2006 (SR **152.3**).

62 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

63 Inserted by Annex No. 4 of the Freedom of Information Act of 17 Dec. 2004 (SR **152.3**). Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

64 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

65 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).

66 SR **152.3**

2 He may also advise bodies of the Federal Administration even if, in accordance with Article 2 paragraph 2 letters c and d, this Act does not apply. The bodies of the Federal Administration may permit him to inspect their files.

Art. 32[67]

Section 6:[68] Legal Protection

Art. 33

1 Legal protection is governed by the general provisions on the administration of federal justice.

2 If the Commissioner establishes in a case investigation under Article 27 paragraph 2 or under Article 29 paragraph 1 that the data subjects are threatened with a disadvantage that cannot be easily remedied, he may apply to the President of the division of the Federal Administrative Court responsible for data protection for interim measures to be taken. The procedure is governed by analogy by Articles 79–84 of the Federal Act of 4 December 1947[69] on Federal Civil Procedure.

Section 7: Criminal Provisions

Art. 34 Breach of obligations to provide information, to register or to cooperate

1 On complaint, private persons are liable to a fine[70] if they:

a. breach their obligations under Articles 8–10 and 14, in that they wilfully provide false or incomplete information; or

b. wilfully fail:

1. to inform the data subject in accordance with Article 14 paragraph 1, or

2. to provide information required under Article 14 paragraph 2.[71]

2 Private persons are liable to a fine[72] if they wilfully:

67 Repealed by Annex No I of the Federal Act of 30 Sept. 2011 on Research involving Human Beings, with effect from 1 Jan. 2014 (AS **2013** 3215; BBl **2009** 8045).

68 Amended by Annex No. 26 des Administrative Court Act of 17 June 2005, in force since 1 Jan. 2007 (SR **173.32**).

69 SR **273**

70 Amended by Art. 333 of the Criminal Code (SR 311.0) in the version of the Federal Act of 13 Dec. 2002, in force since 1 Jan. 2007 (AS **2006** 3459).

71 Amended by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

a.[73] fail to provide information in accordance with Article 6 paragraph 3 or to declare files in accordance with Article11*a* or who in doing so wilfully provide false information; or

b. provide the Commissioner with false information in the course of a case investigation (Art. 29) or who refuse to cooperate.

Art. 35 Breach of professional confidentiality

[1] Anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their professional activities where such activities require the knowledge of such data is, on complaint, liable to a fine.[74]

[2] The same penalties apply to anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their activities for a person bound by professional confidentiality or in the course of training with such a person.

[3] The unauthorised disclosure of confidential, sensitive personal data or personality profiles remains an offence after termination of such professional activities or training.

Section 8: Final Provisions

Art. 36 Implementation

[1] The Federal Council shall issue the implementing provisions.

[2] …[75]

[3] It may provide for derogations from Articles 8 and 9 in relation to the provision of information by Swiss diplomatic and consular representations abroad.

[4] It may also specify:

a. which data files require processing regulations;

b. the requirements under which a federal body may arrange for the processing of personal data by a third party or for a third party;

c. how the means of identification of persons may be used.

72 Amended by Art. 333 of the Criminal Code (SR 311.0) in the version of the Federal Act of 13 Dec. 2002, in force since 1 Jan. 2007 (AS **2006** 3459).
73 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983 4991; BBl **2003** 2101).
74 Amended by Art. 333 of the Criminal Code (SR 311.0) in the version of the Federal Act of 13 Dec. 2002, in force since 1 Jan. 2007 (AS **2006** 3459).
75 Repealed by Art. 25 of the Archiving Act of 26 June 1998 (SR **152.1**).

5 It may conclude international treaties on data protection provided they comply with the principles of this Act.

6 It regulates how data files must be secured where the data may constitute a danger to life and limb for the data subjects in the event of war or other crisis.

Art. 37 Implementation by the cantons

1 Unless there are cantonal data protection regulations that ensure an adequate level of protection, Articles 1–11*a*, 16, 17, 18–22 and 25 paragraphs 1–3 of this Act apply to the processing of personal data by cantonal bodies in the implementation of federal law.[76]

2 The cantons shall appoint a controlling body to ensure compliance with data protection requirements. Articles 27, 30 and 31 are applicable in an analogous manner.

Art. 38 Transitional provisions

1 The controllers of data files must register existing data files that must be registered under Article 11 within one year of the commencement of this Act at the latest.

2 They must take the required measures within one year of the commencement of this Act to be able to provide the information required under Article 8.

3 Federal bodies may continue to use an existing data file with sensitive personal data or with personality profiles until 31 December 2000 without fulfilling the requirements of Article 17 paragraph 2.[77]

4 In matters relating to asylum and foreign nationals, the period mentioned in paragraph 3 is extended until the commencement of the totally revised Asylum Act[78] and the amendments to the Federal Act of 26 March 1931[79] on the Residence and Permanent Settlement of Foreign Nationals.[80]

Art. 38*a*[81] Transitional provision to the Amendment of 19 March 2010

The appointment of the Commissioner and the termination of his employment relationship are subject to the previous law until the end of the legislative period in which this amendment comes into force.

76 Amended by No. I of the Federal Act of 24 March 2006, in force since 1 Jan. 2008 (AS **2007** 4983; BBl **2003** 2101).
77 Amended by No. I of the des Federal Decree of 26 June 1998, in force until 31 Dec. 2000 (AS **1998** 1586; BBl **1998** 1579 1583).
78 SR **142.31**
79 SR **142.20**
80 Inserted by No. II of the Federal Decree of 20 June 1997, in force since 1 Jan. 1998 (AS **1997** 2372; BBl **1997** I 877). The Acts mentioned come into force on 1 Oct. 1999.
81 Inserted by No. 3 of the Federal Act of 19 March 2010 on the Implementation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in force since 1 Dec. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).

Art. 39 Referendum and commencement

1 This Act is subject to an optional referendum.

2 The Federal Council determines the date on which this Act comes into force.

Commencement Date: 1 July 1993[82]

Final Provision of the Amendment of 24 March 2006[83]

Within a year of the commencement of this Act, the controllers of data files must take the required measures to inform data subjects in accordance with Article 4 paragraph 4 and Article 7*a*.

82 Federal Council Decree of 14 June 1993 (AS **1993** 1958).
83 AS **2007** 4983 4991

Annex

Amendment of Federal Acts

…[84]

84 The amendments may be consulted under AS **1993** 1945.

PERSONAL DATA PROTECTION ACT OF THE REPUBLIC OF SLOVENIA

Ministry of Justice of the Republic of Slovenia

2013

MINISTRY OF JUSTICE OF SLOVENIA LEGISLATION

On the basis of the second indent, first paragraph of Article 107 and the first paragraph of Article 91 of the Constitution of the Republic of Slovenia, I hereby issue the

DECREE

on the promulgation of the Personal Data Protection Act (ZVOP-1)

I hereby promulgate the Personal Data Protection Act (ZVOP-1), which was adopted by the National Assembly of the Republic of Slovenia at its session of 15 July 2004.

No. 001-22-148/04
Ljubljana, 23 July 2004

Dr. Janez Drnovšek
President
of the Republic of Slovenia

PERSONAL DATA PROTECTION ACT (ZVOP-1)[1]

PART I
GENERAL PROVISIONS

Contents of the Act

Article 1

This Act determines the rights, responsibilities, principles and measures to prevent unconstitutional, unlawful[2] and unjustified encroachments on the privacy and dignity of an individual[3] (hereinafter: individual) in the processing of personal data.

Principle of lawfulness and fairness

Article 2

Personal data shall be processed lawfully[4] and fairly.

Principle of proportionality

Article 3

Personal data that are being processed must be adequate and in their extent appropriate in relation to the purposes for which they are collected and further processed.

Prohibition of discrimination

Article 4

Protection of personal data shall be guaranteed to every individual irrespective of nationality[5], race, colour, religious belief, ethnicity, sex, language, political or other belief, sexual orientation, material standing, birth, education, social position, citizenship, place or type of residence or any other personal circumstance.

---

[1] Personal Data Protection Act is in Slovene language: Zakon o varstvu osebnih podatkov. ZVOP-1 is its official acronym in Slovene language. This Act was published in: Official Gazette of the Republic of Slovenia, No. 86/2004, as of 5 August 2004. The full list of Official Gazettes, in which the Personal Data Protection Act and it changes since 2004 are published is: Official Gazette of the Republic of Slovenia, Nos. 86/2004, 113/2005 – ZInfP, 51/2007 – ZUstS-A and 67/2007. Its officially consolidated text (acronym: ZVOP-1-UPB1) is published in: Official Gazette of the Republic of Slovenia, No. 94/2007.

[2] A verbatim translation would be: "not in accordance with the statute".

[3] In original text of this Act in Slovene language the term "individual" is used both in its male and female form ("posameznik oziroma posameznica").

[4] A verbatim translation would be: "statutorily" - meaning by the statute/following a statute (a general act of Parliament).

[5] Citizenship.

Territorial application of this Act

Article 5

(1) This Act shall apply to the processing of personal data if the data controller is established, has its seat or is registered in the Republic of Slovenia, or if a subsidiary of the data controller is registered in the Republic of Slovenia.

(2) This Act shall also apply if the data controller is not established, does not have its seat or is not registered in a Member State of the European Union or is not a part of the European Economic Area and for the processing of personal data the data controller uses automated or other equipment located in the Republic of Slovenia, except where such equipment is used solely for the transfer of personal data across the territory of the Republic of Slovenia.

(3) The data controller from the previous paragraph must appoint a natural person or legal person that has its seat or is registered in the Republic of Slovenia to represent it in respect of the processing of personal data in accordance with this Act.

(4) This Act shall also apply to diplomatic-consular offices and other official representative offices of the Republic of Slovenia abroad.

Meaning of terms

Article 6

Terms used in this Act shall have the following meanings:

1. Personal data - is any data relating to an individual, irrespective of the form in which it is expressed.

2. Individual - is an identified or identifiable natural person to whom personal data relates; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, where the method of identification does not incur large costs or disproportionate effort or require a large amount of time.

3. Processing of personal data - means any operation or set of operations performed in connection with personal data that are subject to automated processing or which in manual processing are part of a filing system or which are intended for inclusion in a filing system, such as in particular collection, acquisition, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, communication, dissemination or otherwise making available, alignment or connecting, blocking, anonymising, erasure or destruction; processing may be performed manually or by using automated technology (means of processing).

4. Automated processing – is the processing of personal data using information technology means.

5. Filing system – is any structured set of data containing at least one piece of personal data, which is accessible according to criteria enabling the use or combination of the data, irrespective of whether the set is centralised, decentralised or dispersed on a functional or geographical basis; a structured set of data is a set of data organised in such a manner as to identify or enable identification of an individual.

6. Data controller - is a natural person or legal person or other public or private sector person which alone or jointly with others determines the purposes and means of the processing of personal data or a person provided by statute that also determines the purposes and means of processing.

7. Data processor - is a natural person or legal person that processes personal data on behalf and for the account of the data controller.

8. Data recipient – is a natural or legal person or other private or public sector person to whom personal data are supplied or disclosed.

9. Supply of personal data – is the supply or disclosure of personal data.

10. Foreign recipient and foreign data controller – is a recipient of personal data in a third country and a data controller in a third country.

11. Third country - is a country that is not a Member State of the European Union or a part of the European Economic Area.

12. Filing system catalogue - is a description of a filing system.

13. Register of Filing Systems - is a register containing data from filing system catalogues.

14. Personal consent of an individual – is a voluntary statement of the will of an individual that his personal data may be processed for a specific purpose, and this is given on the basis of information that must be provided to such individual by the data controller pursuant to this Act; personal consent of an individual may be written, oral or some other appropriate consent of the individual.

15. Written consent of the individual - is the signed consent of the individual having the form of a document, the provision of a contract, the provision of an order, an appendix to an application or other form in accordance with statute; a signature shall also mean on the basis of a statute a form equivalent to a signature given by means of telecommunication and a form equivalent by statute to a signature given by an individual who does not know how to write or is unable to write.

16. Oral or other appropriate consent of the individual - is consent given orally or by means of telecommunication or other appropriate means or in some other appropriate manner from which it can be concluded unambiguously that the individual has given his consent.

17. Blocking - is such labelling of personal data that restricts or prevents their further processing.

18. Anonymising - is such alteration to the form of personal data such that they can no longer be linked to the individual or where such link can only be made with disproportionate efforts, expense or use of time.

19. Sensitive personal data - are data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health status, sexual life, the entry in or removal from criminal record or records of minor offences that are kept on the basis of a statute that regulates minor offences (hereinafter: minor offence records); biometric characteristics are also sensitive personal data if their use makes it possible to identify an individual in connection with any of the aforementioned circumstances.

20. Same connecting codes - are the personal identification number and other uniform identification numbers defined by statute relating to an individual that can be used to obtain or retrieve personal data from filing systems in which the same connecting codes are also processed.

21. Biometric characteristics - are such physical, physiological and behavioural characteristics which all individuals have but which are unique and permanent for each individual specifically and which can be used to identify an individual, in particular by the use of fingerprint, recording of papillary ridges of the finger, iris scan, retinal scan, recording of facial characteristics[6], recording of an ear, DNA scan and characteristic gait.

22. Public sector - are state bodies, bodies of self-governing local communities, holders of public powers, public agencies, public funds, public institutes, universities, independent institutions of higher education and self-governing communities of nationalities.

23. Private sector - means legal or natural persons performing an activity in accordance with the statute regulating commercial companies or a commercial public service or craft, and persons of private law; public commercial institutes, public companies and commercial companies, irrespective of the share or influence held by the state, self-governing local communities or self-governing communities of nationalities, are a part of the private sector.

Exceptions in the application of this Act

Article 7

(1) This Act shall not apply to the processing of personal data performed by individuals exclusively for personal use, family life or for other domestic needs.

(2) Articles 26, 27 and 28 of this Act shall not apply to personal data, which are processed by political parties, trade unions, associations or religious communities relating to their members.

(3) The second paragraph of Article 25, Articles 26, 27 and 28, and Part V of this Act shall not apply to personal data which are processed by the media for the purposes of informing the public.

[6] A verbatim translation of the term "obraz" (in Slovene language) would be: "face".

(4) Data controllers with fewer than 50 employees shall not be required to fulfil the obligation laid down in the second paragraph of Article 25, and shall not be required to fulfil the obligations laid down in Articles 26 and 27 of this Act.

(5) The exemptions laid down in the preceding paragraph shall not apply to filing systems kept by data controllers in the public sector, notaries public, attorneys, detectives, bailiffs, private security providers, private healthcare workers, healthcare providers, and to data controllers that keep filings systems containing sensitive personal data and processing of sensitive personal data is a part of their registered activity.

PART II

PROCESSING OF PERSONAL DATA

Chapter 1

Legal grounds and purposes

General definition

Article 8

(1) Personal data may only be processed if the processing of personal data and the personal data being processed are provided by statute, or if the personal consent of the individual has been given for the processing of certain personal data.

(2) The purpose of processing personal data must be provided by statute, and in cases of processing on the basis of personal consent of the individual, the individual must be informed in advance in writing or in another appropriate manner of the purpose of processing of personal data.

Legal grounds in the public sector

Article 9

(1) Personal data in the public sector may be processed if the processing of personal data and the personal data being processed are provided by statute. Statute may provide that certain personal data may only be processed on the basis of personal consent of the individual.

(2) Holders of public powers may also process personal data on the basis of personal consent of the individual without statutory grounds where this does not involve the performance of their duties as holders of public powers. Filing systems created on such basis must be held separate from filing systems created on the basis of the performance of duties of the holder of public powers.

(3) Irrespective of the first paragraph of this Article, in the public sector personal data may be processed in respect of individuals that have contractual relations with the public sector or on the basis of the individual’s initiative are negotiating on the conclusion of a contract, provided

that the processing of personal data is necessary and appropriate for conducting negotiations for the conclusion of a contract or for the fulfilment of a contract.

(4) Irrespective of the first paragraph of this Article, personal data may in exceptions be processed in the public sector where they are essential for the exercise of lawful[7] competences, duties or obligations by the public sector, provided that such processing does not encroach on the justified interests of the individual to whom the personal data relate.

Legal grounds in the private sector

Article 10

(1) Personal data in the private sector may be processed if the processing of personal data and the personal data being processed are provided by statute, or if the personal consent of the individual has been given for the processing of certain personal data.

(2) Irrespective of the previous paragraph, in the private sector personal data may be processed in respect of individuals that have contractual relations with the private sector or on the basis of the individual's initiative are negotiating on the conclusion of a contract, provided that the processing of personal data is necessary and appropriate for conducting negotiations for the conclusion of a contract or for the fulfilment of a contract.

(3) Irrespective of the first paragraph of this Article, personal data may be processed in the private sector if this is essential for the fulfilment of the lawful[8] interests of the private sector and these interests clearly outweigh the interests of the individual to whom the personal data relate.

Contractual Processing

Article 11

(1) Data controller may by contract entrust individual tasks related to processing of personal data to data processor that is registered to perform such activities and ensures the appropriate procedures and measures pursuant to Article 24 of this Act.

(2) Data processor may perform individual tasks associated with processing of personal data within the scope of the client's authorisations, and may not process personal data for any other purpose. Mutual rights and obligations shall be arranged by contract, which must be concluded in writing and must also contain an agreement on the procedures and measures pursuant to Article 24 of this Act. Data controller shall oversee the implementation of procedures and measures pursuant to Article 24 of this Act.

(3) In the event of a dispute between the data controller and the data processor, the data processor shall be bound on the basis of a request from the data controller to return to the controller without delay the personal data processed under contract. He shall be obliged to destroy immediately or to supply any copies of such data to the state body competent by

[7] Provided for by statute (a general act of Parliament).
[8] Provided for by statute (a general act of Parliament).

statute for detection or prosecution of criminal offences, to a court or to another state body, if so provided by statute.

(4) In the event of cessation of a data processor, personal data shall be returned to the data controller without unnecessary delay.

Protection of the vital interests of the individual

Article 12

If processing of personal data is necessarily required to protect the life or body of an individual, his personal data may be processed irrespective of the fact that there are no other statutory legal grounds for the processing of such data.

Processing of sensitive personal data

Article 13

Sensitive personal data may only be processed in the following cases:

1. if the individual has given explicit personal consent for this, such consent as a rule being in writing, and in the public sector provided by statute;

2. if the processing is necessary in order to fulfil the obligations and special rights of a data controller in the area of employment in accordance with statute, which also provides appropriate guarantees for the rights of the individual;

3. if the processing is necessarily required to protect the life or body of an individual to whom the personal data relate, or of another person, where the individual to whom the personal data relate is physically or contractually[9] incapable of giving his consent pursuant to subparagraph 1 of this Article;

4. if they are processed for the purposes of lawful[10] activities by institutions, societies, associations, religious communities, trade unions or other non-profit organisations with political, philosophical, religious or trade-union aim, but only if the processing concerns their members or individuals in regular contact with them in connection with such aims, and if they

[9] This term "contractually" represents the abbreviation of the Slovene legal institute of "capacity to contract" (for the purposes of this Act), which is in Slovene "poslovna sposobnost". For example, a similar German legal term is "*Geschäftsfähigkeit*". In the Republic of Slovenia natural persons obtain the **partial capacity to contract** when they attain 15 years of age (see Article 108 of the Marriage and Family Relations Act, Official Gazette of the SRS, Nos. 15/76, 30/86, 1/89 and 14/89 – Consolidated Text, Official Gazette of the RS, Nos. 13/94, 82/94, 29/95, 26/99, 60/99 – Decision of the Constitutional Court, 70/2000, 64/2001, 110/2002, 16/2004, 69/2004 – Officially Consolidated Text, 101/2007 - Decision of the Constitutional Court, 90/2011 - Decision of the Constitutional Court and 84/2012 - Decision of the Constitutional Court) and obtain the **full capacity to contract** when they attain 18 years of age (Article 117, paragraph 1 of the Marriage and Family Relations Act), or if a minor (a person between 15 years and below 18 years of age) under certain conditions concludes a marital union (Article 117, paragraph 2) and a minor can also obtain it if he/she became a parent and if there are "significant" reasons for obtaining the full capacity to contract (Article 117, paragraph 3), following a decision by the court in non-contentious proceedings.

[10] Provided for by statute (a general act of Parliament).

do not supply such data to other individuals or persons of public or private sector without the written consent of the individual to whom they relate;

5. if the individual to whom the sensitive personal data relate publicly announces them without any evident or explicit purpose of restricting their use;

6. if they are processed by health-care workers and health-care staff in compliance with statute for the purposes of protecting the health of the public and individuals and the management or operation of health services;

7. if this is necessary in order to assert or oppose a legal claim;

8. if so provided by another statute in order to implement the public interest.

Protection of sensitive personal data

Article 14

(1) Sensitive personal data must during processing be specially marked and protected, such that access to them by unauthorised persons is prevented, except in instances from subparagraph 5 of Article 13 of this Act.

(2) In the transmission of sensitive personal data over telecommunications networks, data shall be considered as suitably protected if they are sent with the use of cryptographic methods and electronic signatures such that their illegibility or non-recognition is ensured during transmission.

Automated decision-making

Article 15

Automated data processing, in which a decision may be taken regarding an individual that could have legal effect in relation to him, or substantive influence on him, and which is based solely on automated data processing intended for the evaluation of certain personal aspects relating to him, such as in particular his success at work, credit rating, reliability, handling or compliance with conditions required, shall only be permitted if the decision:

1. is taken during the conclusion or implementation of a contract, provided that the request to conclude or implement a contract submitted by the individual to whom the personal data relate has been fulfilled or that there exist appropriate measures to protect his lawful[11] interests, such as in particular agreements enabling him to object to such decision or to express his position;

2. is provided by statute which also provides measures to protect the lawful[12] interests of the individual to whom the personal data relate, particularly the possibility of legal remedy against such decision.

[11] Provided for by statute (a general act of Parliament).
[12] Provided for by statute (a general act of Parliament).

Purpose of collection, and further processing

Article 16

Personal data may only be collected for specific and lawful[13] purposes, and may not be further processed in such a manner that their processing would be counter to these purposes, unless otherwise provided by statute.

Processing for historical, statistical and scientific-research purposes

Article 17

(1) Irrespective of the initial purpose of collection, personal data may be further processed for historical, statistical and scientific-research purposes.

(2) Personal data shall be supplied to the data recipient for the purpose of processing from the previous paragraph in an anonymised form, unless otherwise provided by statute or if the individual to whom the personal data relate gave prior written consent for the data to be processed without anonymising.

(3) Personal data supplied to data recipient in accordance with the previous paragraph shall on completion of processing be destroyed, unless otherwise provided by statute. The data recipient shall be obliged without delay after destruction of the data to inform the data controller who supplied him the personal data in writing when and how he destroyed them.

(4) Results of processing from the first paragraph of this Article shall be published in anonymised form, unless otherwise provided by statute or unless the individual to whom the personal data relate gave written consent for publication in a non-anonymised form or unless written consent for such publication has been given by the heirs to the deceased person under this Act.

Chapter 2

Protection of individuals

Accuracy and up to date personal data

Article 18

(1) Personal data being processed must be accurate and kept up to date.

[13] Provided for by statute (a general act of Parliament).

(2) Data controller may prior to input into a filing system verify the accuracy of personal data by examining an identity document or other suitable public document of the individual to whom the data relate.

Informing the individual of the processing of personal data

Article 19

(1) If personal data are collected directly from the individual to whom they relate, the data controller or his representative must communicate to the individual the following information, if the individual is not yet acquainted with them:
- data on the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively),
- the purpose of the processing of personal data.

(2) If in view of the special circumstances of collecting personal data from the previous paragraph there is a need to ensure lawful[14] and fair processing of personal data of the individual, the person from the previous paragraph must also communicate to the individual the additional information, if the individual is not yet acquainted with them, and in particular:
- a declaration as to the data recipient or the type of data recipients of his personal data,
- a declaration of whether the collection of personal data is compulsory or voluntary, and the possible consequences if the individual will not provide data voluntarily,
- information on the right to consult, transcribe, copy, supplement, correct, block and erase personal data that relate to him.

(3) If personal data were not collected directly from the individual to whom they relate, the data controller or his representative must communicate to the individual the following information no later than on the recording or supply of personal data to the data recipient:
- data on the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively),
- the purpose of the processing of personal data.

(4) If in view of the special circumstances of collecting personal data from the previous paragraph there is a need to ensure lawful[15] and fair processing of personal data of the individual, the person from the previous paragraph must also communicate to the individual additional information, and in particular:
- information on the type of personal data collected,
- a declaration as to the data recipient or the type of data recipients of his personal data,
- information on the right to consult, transcribe, copy, supplement, correct, block and erase personal data that relate to him.

(5) Information from the third and fourth paragraphs of this Article shall not need to be ensured if in order to process personal data for historical, statistical or scientific-research purposes it would be impossible or would incur large costs or disproportionate effort or would require a large amount of time, or if the recording or supply of personal data is expressly provided by statute.

[14] Verbatim: statutory (in accordance with a statute, meaning mostly in accordance with this Act).
[15] Verbatim: statutory (in accordance with a statute, meaning mostly in accordance with this Act).

Use of the same connecting code

Article 20

(1) In the acquisition of personal data from filing systems in the areas of health, police, national intelligence-security activities, national defence, judiciary and the state prosecution and criminal record and minor offence records, the same connecting code may not be used in such manner that only such code would be used to obtain personal data.

(2) Irrespective of the previous paragraph, the same connecting code may exceptionally be used to obtain personal data if this is the only item of data in a specific case that can enable the detection or prosecution of a criminal offence *ex officio*, to protect the life or body of an individual, or to ensure the implementation of the tasks of the intelligence and security bodies provided by statute. An official annotation or other written record must be made thereof without delay.

(3) The first paragraph of this Article shall not apply to the land register and the commercial register.

Duration of storage of personal data

Article 21

(1) Personal data may only be stored for as long as necessary to achieve the purpose for which they were collected or further processed.

(2) On completion of the purpose of processing, personal data shall be erased, destroyed, blocked or anonymised, unless pursuant to the statute governing archive materials and archives they are defined as archive material, or unless a statute otherwise provides for an individual type of personal data.

Supply of personal data

Article 22

(1) Data controllers shall be obliged against payment of the cost of supply, unless otherwise provided by statute, to supply personal data to data recipients.

(2) The data controller of the Central Population Register or of Records of Permanently and Temporarily Registered Residents shall be obliged in the manner defined for the issuing of certificates to supply to authorised party demonstrating a lawful interest in exercising rights before public sector persons the personal name and address of permanent or temporary residence of an individual against whom they are exercising their rights.

(3) Data controller shall be obliged for each supply of personal data to ensure that it is subsequently possible to determine which personal data were supplied, to whom, when and on

what basis, for the period covered by statutory protection of the rights of an individual due to non-allowed supply of personal data.

(4) Irrespective of the first paragraph of this Article, data controllers in the public sector shall be bound to supply to data recipient in the public sector personal data without payment of the cost of supply, unless otherwise provided by statute or unless it involves use for historical, statistical or scientific-research purposes.

Protection of personal data of deceased individuals

Article 23

(1) Data controller may supply data on a deceased individual only to those data recipients authorised to process personal data by statute.

(2) Irrespective of the previous paragraph, data controller shall supply data on a deceased individual to the person who under the statute governing inheritance is the deceased person's legal heir of the first or second order, if they demonstrate a lawful interest in the use of personal data and the deceased individual did not prohibit in writing the supply of such personal data.

(3) Unless otherwise provided by statute, a data controller may also supply data from the previous paragraph to any other person intending to use such data for historical, statistical or scientific-research purposes if the deceased individual did not prohibit in writing the supply of such personal data.

(4) If the deceased individual did not issue a prohibition from the previous paragraph, persons who under the statute governing inheritance are his legal heirs of the first or second order may prohibit in writing the supply of his data, unless otherwise provided by statute.

Chapter 3

Security of Personal Data

Contents

Article 24

(1) Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data:
1. by protecting premises, equipment and systems software, including input-output units;

2. by protecting software applications used to process personal data;

3. by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;

4. by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;

5. by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

(2) In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient.

(3) The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed.

(4) Functionaries, employees and other individuals performing work or tasks at persons that process personal data shall be bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy of personal data shall also be binding on them after termination of their function, work or tasks, or the performance of contractual processing services.

Duty to secure

Article 25

(1) Data controllers and data processors shall be bound to ensure the protection of personal data in the manner set out in Article 24 of this Act.

(2) Data controllers shall prescribe in their internal acts the procedures and measures for security of personal data and shall define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data.

Chapter 4

Notification of filing systems

Filing system catalogue

Article 26

(1) Data controller shall establish for each filing system a filing system catalogue containing:
1. title of the filing system;

2. data on the data controller (for natural person: personal name, address where activities are performed or address of permanent or temporary residence, and for sole trader his official name, registered office, seat and registration number; for legal person: title or registered office and address or seat of the data controller and registration number);

3. legal basis for processing personal data;

4. the category of individuals to whom the personal data relate;

5. the type of personal data in the filing system;

6. purpose of processing;

7. duration of storage of personal data;

8. restrictions on the rights of individuals with regard to personal data in the filing system and the legal basis for such restrictions;

9. data recipients or categories of data recipients of personal data contained in the filing system;

10. whether the personal data are transferred to a third country, to where, to whom and the legal grounds for such transfer;

11. a general description of security of personal data;

12. data on connected filing systems from official records and public books.

13. data on the representative from the third paragraph of Article 5 of this Act (for natural person: personal name, address where activities are performed or address of permanent or temporary residence, and for sole trader his official name, registered office, seat and registration number; for legal person: title or registered office and address or seat of the data controller and registration number).

(2) Data controller must ensure that the contents of the catalogue are accurate and up to date.

Notification of the supervisory body

Article 27

(1) Data controller shall supply data from subparagraphs 1, 2, 4, 5, 6, 9, 10, 11, 12 and 13 of the first paragraph of Article 26 of this Act to the National Supervisory Body for Personal Data Protection at least 15 days prior to the establishing of a filing system or prior to the entry of a new type of personal data.

(2) Data controller shall supply to the National Supervisory Body for Personal Data Protection modifications to the data from the previous paragraph no later than eight days from the date of modification.

~~(3) Data from the first paragraph of this Article shall not need to be supplied by that data controller that do not have more than 20 persons employed for an indefinite period and relating to those filing systems they maintain on their employees in accordance with the statute governing filing systems in the area of labour. In this case each person must be provided with information from Article 26 of this Act.~~

[Repealed by the Act on Changes and Amendments to the Personal Data Protection Act (ZVOP-1A), Official Gazette of the RS, No. 67/2007.]

Register

Article 28

(1) The National Supervisory Body for Personal Data Protection shall manage and maintain a Register of Filing Systems containing data from Article 27 of this Act, in the manner defined by the methodology of its management.

(2) The Register shall be managed using information technology and shall be published on the website of the National Supervisory Body for Personal Data Protection (hereinafter: the website).

(3) The rules on the methodology[16] from the first paragraph of this Article shall be defined by the Minister responsible for justice, on the proposal of the Chief National Supervisor for Personal Data Protection[17] (hereinafter: the Chief National Supervisor).

PART III

RIGHTS OF THE INDIVIDUAL

Examination of the Register

Article 29

(1) The National Supervisory Body for Personal Data Protection shall be obliged to permit anyone to consult the Register of Filing Systems and to transcribe the data.

(2) The consultation and transcription of data must as a rule be permitted and enabled on the same day, and no later than within eight days, otherwise the request shall be deemed to have been refused.

Right of the individual to information

Article 30

(1) Data controller shall on request of the individual be obliged:

1. to enable consultation of the filing system catalogue;

[16] See: Rules on the Methodology of Managing the Register of Filing Systems, published in: Official Gazette of the RS, Nos. 28/2005 and 30/2011 (in Slovene language: "Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov").

[17] In original text of this Act in Slovene language the term "the Chief National Supervisor for Protection of Personal Data" is used both in its female and male form ("glavna državna nadzornica oziroma glavni državni nadzornik za varstvo osebnih podatkov").

2. to certify whether data relating to him are being processed or not, and to enable him to consult personal data contained in filing system that relate to him, and to transcribe or copy them;

3. to supply him an extract of personal data contained in filing system that relate to him;

4. to provide a list of data recipients to whom personal data were supplied, when, on what basis and for what purpose;

5. to provide information on the sources on which records contained about the individual in a filing system are based, and on the method of processing.

6. to provide information on the purpose of processing and the type of personal data being processed, and all necessary explanations in this connection;

7. to explain technical and logical-technical procedures of decision-making, if the controller is performing automated decision-making through the processing of personal data of an individual.

(2) The extract from subparagraph 3 of the previous paragraph may not replace the document or certificate under the regulations on administrative or other procedures, and this shall be indicated on the extract.

Procedure for information

Article 31

(1) The request from Article 30 of this Act shall be lodged in writing or orally in a record with the data controller. Such request may be lodged once every three months, and in respect of sensitive personal data and personal data under the provisions of Chapter 2, Part VI of this Act, once a month. When required to ensure fair, lawful or proportionate processing of personal data, particularly when an individual's personal data in a filing system are frequently updated or sent or could be frequently updated or sent to data recipients, the data controller must permit the individual to lodge the request within an appropriately shorter period, which is not less than five days from the day of acquainting with personal data that relate to him or [from the] refusal of this acquaintance.

(2) The data controller must enable the individual to consult, transcribe, copy and obtain a certificate pursuant to subparagraphs 1 and 2 of the first paragraph of Article 30 of this Act as a rule on the same day that the request is received, and no later than within 15 days, or within 15 days to inform the individual in writing of the reasons why he will not enable consultation, transcription, copying or the issuing of a certificate.

(3) The data controller shall be obliged to supply the extract from subparagraph 3, the list from subparagraph 4, information from subparagraphs 5 and 6 and the explanation from subparagraph 7 of the first paragraph of Article 30 of this Act to the individual within 30 days from the date he received the request, or within the same interval to inform him in writing of the reasons why he will not supply the extract, list, information or explanation.

(4) If the data controller fails to act in accordance with the second and third paragraphs of this Article, the request shall be deemed to have been refused.

(5) Costs relating to the request and consultation from this Article shall be borne by the data controller.

(6) For the transcription, copying and written certificate pursuant to Item 2, and the extract pursuant to Item 3, the list from Item 4, the information from Items 5 and 6 and the explanation from Item 7 of the first paragraph of Article 30 of this Act, the data controller may charge the individual only material costs according to a pre-specified tariff, while an oral confirmation pursuant to Item 2, oral provision of information pursuant to Item 5, oral provision of information pursuant to Item 6, and oral explanation pursuant to Item 7 shall be free-of-charge. If despite having received an oral confirmation, information or explanation pursuant to Items 2, 5, 6 and 7 of the first paragraph of Article 30, an individual requests confirmation, information or an explanation in written form, the data controller must provide it.

(7) The Minister responsible for justice, at the proposal of the Information Commissioner, shall issue rules[18] prescribing a tariff for the material costs referred to in the preceding paragraph and shall publish them in the Official Gazette of the Republic of Slovenia.

Right to supplement, correct, block, erase and to object

Article 32

(1) On the request of an individual to whom personal data relate, the data controller must supplement, correct, block or erase personal data which the individual proves as being incomplete, inaccurate or not up to date, or that they were collected or processed contrary to statute.

(2) On the request of the individual the data controller must inform all data recipients and data processors to whom the controller has supplied the personal data of the individual, before the measures from the previous paragraph have been carried out, of their supplementation, correction, blocking or erasure pursuant to the previous paragraph. Exceptionally the data controller shall not need to do this if it would incur large costs, disproportionate efforts or would require a large amount of time.

(3) Individuals whose personal data are processed in accordance with the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act shall have the right through objection at any time to demand the cessation of their processing. The data controller shall grant the objection if the individual demonstrates that the conditions for processing have not been fulfilled pursuant to the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act. In this case the personal data of the individual may no longer be processed.

(4) If the data controller does not grant the objection from the previous paragraph, the individual that lodged the objection may request that the National Supervisory Body for

[18] See: Rules on the charging of expenses concerning the execution of the individual's right to acquaint himself with his own personal data, published in: Official Gazette of the RS, Nos. 85/2007 and 5/2012 (in Slovene language: "Pravilnik o zaračunavanju stroškov pri izvrševanju pravice posameznika do seznanitve z lastnimi osebnimi podatki").

Personal Data Protection decides on whether the processing is in accordance with the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act. The individual may lodge such request within seven days of delivery of the decision regarding on objection.

(5) The National Supervisory Body for Personal Data Protection shall decide on the request from the previous paragraph within two months of receipt of the request. The lodging of a request shall withhold the processing of personal data of the individual in respect of which the request was lodged.

(6) The costs of all actions of the data controller from the previous paragraphs shall be borne by the data controller.

Procedure of supplementing, correction, blocking, deletion and objection

Article 33

(1) The request or objection from Article 32 of this Act shall be lodged in writing or orally in an annotation with the data controller.

(2) The data controller shall be obliged to perform the supplementing, correction, blocking or deletion of personal data within 15 days of the date of receipt of the request, and to inform the person who lodged the request thereof, or within the same interval to inform him of the reasons why he will not do so. The controller must decide on an objection within the same deadline.

(3) If the data controller fails to act pursuant to the previous paragraph, the request shall be deemed to have been refused.

(4) If the data controller concludes on his own that the personal data are incomplete, inaccurate or not up to date, he shall supplement or correct them and inform the individual thereof, unless otherwise provided by statute.

(5) Costs relating to the supplementing, correction and erasure of personal data, and of the notification and decision on the objection, shall be borne by the data controller.

Judicial protection of the rights of the individual

Article 34

(1) Individual who finds that his rights provided by this Act have been violated may request judicial protection for as long as such violation lasts.

(2) If the violation from the previous paragraph ceases, the individual may file a suit to rule that the violation existed if he is not provided with other judicial protection in relation to the violation.

(3) The competent court shall decide in the procedure under the provisions of the statute regulating administrative disputes unless otherwise provided by this Act.

(4) The procedure shall not be public unless the court decides otherwise at the suggestion of the individual for well-founded reasons.

(5) The procedure shall be urgent and a priority.

Temporary injunction

Article 35

In a suit filed due to violations of rights from Article 32 of this Act, an individual may request the court to bind the data controller, until a final decision is issued in the administrative dispute, to prevent any kind of processing of the disputed personal data, if their processing could cause with difficulty reparable damage to the individual, to whom the personal data relate, while the postponement of processing should not be contrary to the public interests and neither is there any danger of greater irredeemable damage being done to the opposing party.

Restriction of the rights of an individual

Article 36

(1) The rights of an individual from the third and fourth paragraphs of Article 19, Articles 30 and 32 of this Act may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others.

(2) Restrictions from the previous paragraph may only be provided in the extent necessary to achieve the purpose for which the restriction was provided.

PART IV

INSTITUTIONAL PERSONAL DATA PROTECTION

Chapter 1

Supervisory body for personal data protection

Supervisory body

Article 37

(1) The National Supervisory Body for Personal Data Protection (hereinafter: the National Supervisory Body) shall have the status of supervisory body for the protection of personal data.

(2) The National Supervisory Body shall undertake inspection supervision on the implementation of the provisions of this Act and other tasks under this Act and other regulations regulating the protection or processing of personal data or the transfer of personal data from the Republic of Slovenia. The National Supervisory Body shall also undertake other tasks in accordance with statute.

(3) The National Supervisory Body shall ensure uniform realisation of measures in the area of protection of personal data.

~~***Status and organisation of the National Supervisory Body***~~

~~*Article 38*~~

~~*(1) The National Supervisory Body shall be a self dependent*[19] *state body.*~~

~~*(2) The National Supervisory Body shall be headed by a Chief National Supervisor, who shall be a state functionary. His salary shall be regulated by the decision of the National Assembly laying down the ranking of official functions into salary brackets.*~~

~~*(3) The National Supervisory Body shall employ at least four National Supervisors for Personal Data Protection*[20] *(hereinafter: the Supervisor). At least one of them must be a university graduate in law.*~~

~~*(4) The Chief National Supervisor shall head and represent the National Supervisory Body, organise and coordinate the work of Supervisors and carry out inspection supervision pursuant to this Act.*~~

~~*(5) Administrative and technical tasks for the National Supervisory Body shall be performed by the Ministry responsible for justice.*~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05; see Articles 1, 2, 8 and 9 of this Act in Appendix 2]

~~***Funds for the work of the National Supervisory Body***~~

~~*Article 39*~~

~~*Funds for the work of the National Supervisory Body shall be provided in the Budget of the Republic of Slovenia. The level of funds shall be determined by the National Assembly of the*~~

[19] In Slovene language "self-dependent" is: "samostojen". A literal translation would be: "standing on its own". Self-dependent means from the viewpoint of legal terminology less than independence and more than autonomy. A similar legal term in German language is "*Selbständigkeit*". However, in actual terms self-dependent is understood to mean nearly the same as independent.

[20] In original text of this Act in Slovene language the term "National Supervisors for Personal Data Protection" is used in its female and male form ("državna nadzornica oziroma državni nadzornik za varstvo osebnih podatkov").

~~*Republic of Slovenia (hereinafter: National Assembly) on the proposal of the Chief National Supervisor.*~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05; see Article 5 of this Act in Appendix 2]

~~Appointment of the Chief National Supervisor~~

~~Article 40~~

~~(1) The Chief National Supervisor shall be appointed by the National Assembly on the proposal of the Minister responsible for justice.~~

~~(2) The Chief National Supervisor shall be appointed from among those individuals that fulfil the conditions for appointment to the title of Supervisor under this Act.~~

~~(3) The vacancy for the post of Chief National Supervisor shall be advertised by the Ministry responsible for justice ex officio no later than three months from the expiry of the term of office of the Chief National Supervisor or within one month of early dismissal. The vacancy shall be advertised in the Official Gazette of the Republic of Slovenia, and the deadline for applications may not be shorter than 15 days.~~

~~(4) The Chief National Supervisor shall be appointed for a period of eight years and may be re-appointed.~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05; see Article 6 of this Act in Appendix 2]

~~Dismissal of the Chief National Supervisor~~

~~Article 41~~

~~(1) The Chief National Supervisor may be subject to early dismissal only in the following cases:~~
~~- if he tenders a statement of resignation to the National Assembly;~~
~~- if he is convicted by a final decision of a criminal offence with a punishment of deprivation of liberty;~~
~~- if he cannot perform his function for health or other well-founded reasons for more than six months;~~
~~- if he becomes permanently incapable of performing his function.~~

~~(2) The Chief National Supervisor shall be dismissed early and his term of office shall cease on the day the National Assembly determines the onset of reasons from the previous paragraph.~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05; see Article 7 of this Act in Appendix 2]

~~Deputising for the Chief National Supervisor~~

~~Article 42~~

~~The Chief National Supervisor shall from among the Supervisors appoint his Deputy, who shall deputise for him during his absence or temporary incapacity.~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05]

~~The Supervisor~~

~~Article 43~~

~~(1) Persons that have university education, five years of working experience, of which at least one year has been in work with personal data, and have passed the professional examination[21] for the position of inspector pursuant to the statute governing inspection supervision, may be appointed as Supervisor.~~

~~(2) Supervisors shall have the status, rights and obligations provided for Inspectors by the statute governing inspection supervision and by the statute governing civil servants, unless otherwise provided by this Act.~~

~~(3) Supervisors shall be appointed by the Chief National Supervisor in accordance with the statute governing civil servants.~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05; see Article 8 of this Act in Appendix 2]

~~Self-dependence of Supervisors~~

~~Article 44~~

~~(1) In the performance of tasks of inspection supervision and other tasks under this Act within the framework of their authorisations, Supervisors shall be independent and shall undertake them within the framework of and on the basis of the Constitution and statutes.~~

~~(2) In relation to the performance of tasks not comprising the performance of inspection supervision, they shall be bound by the written instructions of the Chief National Supervisor.~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05; see Article 8 of this Act in Appendix 2]

~~Employment and assignment in the National Supervisory Body~~

~~Article 45~~

~~(1) The Chief National Supervisor shall define in accordance with the statute governing civil servants in the act on systematisation the internal organisation of the National Supervisory Body and the required number of civil servants of the National Supervisory Body performing legal tasks and the required number of civil servants performing ancillary work.~~

~~(2) Civil servants of state bodies may on the basis of a proposal of the Chief National Supervisor and with their written agreement and the consent of the head of their state body be assigned to perform legal tasks or ancillary work from the previous paragraph at the~~

[21] See: Rules on the specific part of the professional examination taken by state supervisor for personal data protection, published in: Official Gazette of the RS, No. 57/2006 (in Slovene language: "Pravilnik o posebnem delu strokovnega izpita za državnega nadzornika za varstvo osebnih podatkov").

~~*National Supervisory Body for a period of up to three years. Judges, State Prosecutors and Assistant State Prosecutors may be assigned to perform such tasks pursuant to the provisions of statutes regulating the judicial service and the state prosecutor's office.*~~

~~*(3) Servants and functionaries from the previous paragraph may not perform the tasks of inspection supervision.*~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05]

Chapter 2

Tasks of the National Supervisory Body

~~**Reports of the National Supervisory Body**~~

~~Article 46~~

~~(1) The National Supervisory Body shall submit an Annual Report on its work to the National Assembly no later than by 31 May for the previous year, and shall publish this Report on its website.~~

~~(2) The Annual Report shall contain data on the work of the National Supervisory Body in the previous year and assessments and recommendations in the area of protection of personal data.~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05; see Article 14 of this Act in Appendix 2]

Cooperation with other bodies

Article 47

The National Supervisory Body shall in its work cooperate with state bodies, the competent bodies of the European Union for the protection of individuals in the processing of personal data, international organisations, foreign supervisory bodies for the protection of personal data, institutes, societies, nongovernmental organisations in the area of protection of personal data or privacy and other organisations and bodies regarding all issues important for the protection of personal data.

Competences regarding regulations

Article 48

(1) The National Supervisory Body shall issue prior opinions to Ministries, the National Assembly, self-governing local community bodies, other state bodies and holders of public powers regarding the compliance of the provisions of draft statutes and other regulations with the statutes and other regulations regulating personal data.

~~(2) The National Supervisory Body may file a request to the Constitutional Court of the Republic of Slovenia (hereinafter: the Constitutional Court) to assess the constitutionality of statutes, other regulations and general acts issued to exercise public powers if the question of constitutionality and lawfulness arises in connection with a procedure it conducts.~~

[Repealed by the Act on Changes and Amendments to the Constitutional Court Act, Official Gazette of the RS, No. 51/2007. This provision on direct access to the Constitutional Court was transferred into Article 23.a, paragraph 1, item 6 of the Constitutional Court Act. See Appendix 3]

Publicity concerning work

Article 49

(1) The National Supervisory Body may:
1. issue an internal journal and professional literature;

2. on the website or in another appropriate manner publish the prior opinion from the first paragraph of Article 48 of this Act, after the statute or other regulation has been adopted and published in the Official Gazette of the Republic of Slovenia, in the journal of a self-governing local community or publish it in another lawful[22] manner;

3. on the website or in another appropriate manner publish requests from the second paragraph of Article 48 of this Act, after the Constitutional Court has received them;

4. on the website or in another appropriate manner publish decisions and rulings of the Constitutional Court on requests from the second paragraph of Article 48 of this Act;

5. on its website or in another appropriate manner publish decisions and rulings of courts of general jurisdiction and the Administrative Court relating to the protection of personal data, such that it is not possible to read from them the personal data of parties, injured parties, witnesses or experts;

6. issue non-binding opinions on the compliance of codes of professional ethics, general terms of business or drafts thereof with regulations in the area of the protection of personal data;

7. issue non-binding opinions, clarifications and positions on issues in the area of protection of personal data, and publish them on the website or in another appropriate manner;

8. prepare and issue non-binding instructions and recommendations regarding protection of personal data in individual fields;

9. issue public statements on inspection supervision undertaken in individual cases;

10. hold media conferences relating to the work of the National Supervisory Body and publish transcripts of statements or recordings of statements from media conferences on the website;

11. publish other important announcements on its website.

[22] Verbatim: statutory (in accordance with a statute).

(2) The National Supervisory Body may for the performance of competences from subparagraphs 6, 7 and 8 of the previous paragraph call for cooperation from representatives of associations and other nongovernmental organisations in the area of protection of personal data, privacy and consumers.

Chapter 3

Inspection supervision

Application of the statute governing inspection supervision

Article 50

For the performance of inspection supervision under this Act, the provisions of the statute governing inspection supervision shall apply, unless otherwise provided by this Act.

Scope of inspection supervision

Article 51

Within the framework of inspection supervision the National Supervisory Body shall:
1. supervise the lawfulness[23] of processing of personal data;

2. supervise the suitability of measures for security of personal data and the implementation of procedures and measures for security of personal data pursuant to Articles 24 and 25 of this Act;

3. supervise the implementation of the provisions of the statute regulating the filing system catalogue, the Register of Filing Systems and the recording of the supply of personal data to individual data recipients;

4. supervise the implementation of the statutory provisions regarding the transfer of personal data to third countries and on the supply thereof to foreign data recipients.

Direct performance of inspection supervision

Article 52

(1) Inspection supervision shall be performed directly by Supervisors within the limits of competence of the National Supervisory Body.

(2) Supervisor shall demonstrate his authorisation to perform the tasks of inspection supervision with an official identity card, which shall contain a photograph of the Supervisor, his personal name, professional or scientific title and other necessary data. The Minister

[23] Verbatim: statutory compliance (in accordance with a statute).

responsible for justice shall prescribe the form and content of the official identity card in detail[24].

Competences of the Supervisor

Article 53

In performing inspection supervision, the Supervisor shall be entitled:
1. to examine documentation relating to the processing of personal data, irrespective of their confidentiality or secrecy, and the transfer of personal data to third countries and the supply to foreign data recipients;

2. to examine the contents of filing systems, irrespective of their confidentiality or secrecy, and filing system catalogues;

3. to examine documentation and acts regulating the security of personal data;

4. to examine premises in which personal data are processed, computer and other equipment, and technical documentation;

5. to verify measures and procedures to secure personal data, and the implementation thereof;

6. to exercise other competences provided by the statute regulating inspection supervision and the statute regulating the general administrative procedure;

7. to perform other matters provided by statute.

Inspection measures

Article 54

(1) The Supervisor who in performing inspection supervision detects a violation of this Act or of another statute or regulation regulating protection of personal data shall have the right immediately:
1. to order the elimination of irregularities or deficiencies he detects in the manner and within the interval he himself defines;

2. to order the prohibition of processing of personal data by persons in the public or private sector who have failed to ensure or failed to implement measures and procedures to secure personal data;

[24] See Rules on the Official Identity Card of State Supervisor for personal data protection, published in: Official Gazette RS, No. 35/2013 (in Slovene language: "Pravilnik o službeni izkaznici državnega nadzornika za varstvo osebnih podatkov").

3. to order the prohibition of processing of personal data and the anonymising, blocking, erasure or destruction of personal data whenever he concludes that the personal data are being processed in contravention of the statutory provisions;

4. to order the prohibition of the transfer of personal data to third countries, or their supply to foreign data recipients, if they are transferred or supplied in contravention of the statutory provisions or binding international treaty;

5. to order other measures provided by the statute regulating inspection supervision and the statute regulating the general administrative procedure.

(2) Measures from the previous paragraph may not be ordered against a person who is performing in the electronic communications network services of data transfer, including temporary storage of data and other operations in connection with data which are mainly or entirely in the function of performing or facilitating the transfer of data over networks, if that person himself has no interest linked to the content of such data, and this is not a person who may himself or together with a limited circle of persons linked to him effectively control access to such data.[25]

(3) If a supervisor determines during inspection supervision that there exists a suspicion of the commission of a criminal offence or minor offence, he shall file a criminal notification or implement a procedure in accordance with the statute regulating minor offences.

Judicial protection

Article 55

There shall be no appeal against a decision or ruling of the Supervisor from the first paragraph of Article 54 of this Act, but an administrative dispute shall be permitted.

Notification to complainant

Article 56

The Supervisor shall be obliged to notify complainant of all important conclusions and actions in the procedure of inspection supervision.

~~***Competences of the National Supervisory Body regarding access to information of a public character***~~

~~*Article 57*~~

[25] For a possible interpretation of Article 54, paragraph 2 of the Personal Data Protection Act of the Republic of Slovenia see: Bostjan Makarovic: The new Slovenian personal data protection act: Statutory limits to injunctive regulation of the internet, Computer & Security Law Report (2005), 21, Elsevier Ltd., pp. 322-327, especially pp. 326-327.

~~*(1) The National Supervisory Body may initiate an administrative dispute against a decision of the Commissioner for Access to Information of a Public Character*[26]*, if it assesses that such decision has violated the protection of personal data.*~~

~~*(2) The administrative dispute procedure from the previous paragraph shall be urgent and a priority.*~~

~~*(3) The National Supervisory Body shall be bound to deliver to the Commissioner for Access to Information of a Public Character a decision or ruling in which the Supervisor has taken a position regarding the issue of information of a public character.*~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05]

Protection of secrecy

Article 58

(1) The Supervisor shall be obliged to protect the secrecy of personal data he encounters in performing inspection supervision, and also after ceasing to perform the Supervisor's service.

(2) The obligation from the previous paragraph shall also apply to all civil servants at the National Supervisory Body.

Chapter 4

Cooperation and external supervision in the area of personal data protection

The Human Rights Ombudsman

Article 59

(1) The Human Rights Ombudsman[27] (hereinafter: the Ombudsman) shall perform his tasks in the area of personal data protection in relation to state bodies, self-governing local community bodies and holders of public powers in accordance with the statute regulating the Human Rights Ombudsman.

(2) Personal data protection shall be a special area of the Ombudsman for which one of the Deputy Ombudsmen shall be responsible.

The Annual Report

Article 60

[26] See: Act on Access to Information of a Public Character (Official Gazette of the RS, Nos. 24/2003, 61/2005, 113/2005 - ZInfP, 28/2006 and 117/2006 - ZDavP-2). In Slovene language: "Zakon o dostopu do informacij javnega značaja".

[27] In original text of this Act in Slovene language the term "the Human Rights Ombudsman" is used both in its female and male form ("varuhinja oziroma varuh človekovih pravic").

The Ombudsman shall report in his Annual Report to the National Assembly on conclusions, proposals and recommendations, and on the situation in the area of personal data protection.

Competence of the National Assembly

Article 61

The competent working body of the National Assembly shall monitor the situation in the area of personal data protection and the implementation of the provisions of this Act.

PART V

TRANSFER OF PERSONAL DATA

Chapter 1

Transfer of personal data to Member States of the European Union and the European Economic Area

Free flow of personal data

Article 62

Whenever personal data are supplied to data controller, data processor or data recipient established, has its seat or is registered in a Member State of the European Union or the European Economic Area or otherwise subject to the legal order thereof, the provisions of this Act on the transfer of personal data to third countries shall not apply.

Chapter 2

Transfer of personal data to third countries

General provision

Article 63

(1) The supply of personal data that are processed or will be processed only after being supplied to a third country, shall be permitted in accordance with the provisions of this Act and provided that the National Supervisory Body issues a decision that the country to which the data are transferred ensures an adequate level of protection of personal data.

(2) The decision from the previous paragraph shall not be required if the third country is on the list of those countries from Article 66 of this Act that have been found to fully ensure an adequate level of protection of personal data.

(3) The decision from the first paragraph of this Article shall not be required if the third country is on the list of those countries from Article 66 of this Act that have been found in

part to ensure an adequate level of protection of personal data, if those personal data are transferred and for those purposes for which an adequate level of protection has been found.

Procedure for determining an adequate level of protection of personal data

Article 64

(1) The National Supervisory Body shall initiate a procedure to determine an adequate level of protection of personal data in a third country on the basis of a conclusion of inspection supervision or at the suggestion of a natural person or legal person who can show a legal interest in the issuing of a decision.

(2) At the request of the National Supervisory Body, the Ministry responsible for foreign affairs shall obtain from the competent body of a third country the necessary information as to whether such country ensures an adequate level of protection of personal data.

(3) The National Supervisory Body may obtain additional information on the adequate level of protection of personal data in a third country directly from other supervisory bodies and the competent body of the European Union.

(4) The National Supervisory Body shall issue a decision within two months of receipt of full information from the second and third paragraphs of this Article. It may also issue a decision only for a certain type of personal data or for their processing for an individual purpose.

(5) The National Supervisory Body shall be obliged no later than within 15 days of the issuing of a decision that a third country fails to ensure an adequate level of protection of personal data to inform the competent body of the European Union in writing.

Judicial protection

Article 65

There shall be no appeal against a decision from the fourth paragraph of Article 64 of this Act, but an administrative dispute shall be permitted.

List

Article 66

(1) The National Supervisory Body shall maintain a list of third countries for which it finds that have fully or partly ensured an adequate level of protection of personal data, or have not ensured such protection. If it has been determined that a third country only partly ensures an adequate level of protection of personal data, the list shall also set out in which part an adequate level has been ensured.

(2) The Chief National Supervisor shall publish the list from the previous paragraph in the Official Gazette of the Republic of Slovenia.

Binding of National Supervisory Body in decision-making

Article 67

The National Supervisory Body shall in its decision-making be bound by the decisions of the competent body of the European Union with regard to assessment as to whether third countries ensure an adequate level of protection of personal data.

Decision-making on the transfer of personal data

Article 68

(1) In decision-making on the adequate level of protection of personal data in a third country, the National Supervisory Body shall be bound to determine all circumstances relating to the transfer of personal data. In particular, it shall be obliged to take account of the type of personal data, the purpose and duration of proposed processing, the legal arrangements in the country of origin and the recipient country, including arrangements for protection of personal data of foreign citizens, and measures to secure personal data used in such countries.

(2) In decision-making from the previous paragraph, the National Supervisory Body shall in particular take account of:
1. whether the transferred personal data are used solely for the purpose for which they were transferred, or whether the purpose may change only on the basis of permission of the data controller supplying the data or on the basis of personal consent of the individual to whom the personal data relate;

2. whether the individual to whom personal data relate has the possibility of determining the purpose for which his personal data have been used, to whom they were supplied and the possibility of correcting or erasing inaccurate or outdated personal data, unless this is prevented due to the secrecy of the procedure by binding international treaties;

3. whether the foreign data controller performs adequate organisational and technical procedures and measures to protect personal data;

4. whether there is an assigned contact person authorised to provide information to the individual to whom the personal data relate, or to the National Supervisory Body on the processing of personal data transferred;

5. whether the foreign data recipient may transfer personal data only on the condition that another foreign data recipient to whom personal data will be supplied ensures adequate protection of personal data also for foreign citizens;

6. whether effective legal protection is ensured for individuals whose personal data were transferred.

Rules

Article 69

Following a proposal of the Chief National Supervisor, the Minister responsible for justice, with the consent of the Minister responsible for foreign affairs, shall issue rules that define in greater detail the information considered necessary in the decision-making of the National Supervisory Body on the transfer of personal data to third countries[28].

Special provisions

Article 70

(1) Irrespective of the first paragraph of Article 63 of this Act, personal data may be transferred and supplied to a third country, if:
1. so provided by another statute or binding international treaty;

2. the individual to whom the personal data relate gives personal consent and is aware of the consequences of such supply;

3. the transfer is necessary for the fulfilment of a contract between the individual to whom the personal data relate and the data controller, or for the implementation of pre-contractual measures adopted in response to the request of the individual to whom the personal data relate;

4. the transfer is necessary for the conclusion or implementation of a contract to the benefit of the individual to whom the personal data relate, concluded between the data controller and a third party;

5. the transfer is necessary in order to protect from serious danger the life or body of an individual to whom the personal data relate;

6. the transfer is performed from registers, public books or official records which are intended by statute to provide information to the public and which are available for consultation by the general public or to any person who demonstrates a legal interest that in the individual case the conditions provided by statute for consultation have been met;

7. the data controller ensures adequate measures of protection of personal data and of the fundamental rights and freedoms of individuals, and declares the possibility of their fulfilment or protection, especially in the provisions of contracts or in the general terms of business.

(2) In the case of transfer of personal data under subparagraph 7 of the previous paragraph, the person intending to transfer personal data must obtain a special decision from the National Supervisory Body permitting the transfer of personal data.

(3) The person may transfer personal data only upon receipt of the decision from the previous paragraph permitting transfer.

[28] See: Rules on Acquiring Required Information for the Decision-making on the Transfer of Personal Data to Third Countries, published in: Official Gazette of the RS, No. 79/2005 (in Slovene language: "Pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države").

(4) There shall be no appeal against a decision from the second paragraph of this Article, but an administrative dispute shall be permitted. The administrative dispute procedure shall be urgent and a priority.

(5) The National Supervisory Body shall be obliged no later than within 15 days of the issuing of a decision from the second paragraph of this Article to communicate it to the competent body of the European Union and to the Member States of the European Union.

(6) If the competent body of the European Union decides upon receipt of a decision that the transfer on the basis of a decision from the second paragraph of this Article is not permissible, the National Supervisory Body shall be bound by that body's decision, and shall be obliged within five days of receipt of such decision to issue to the person from the second paragraph of this Article a new decision prohibiting him from making further transfer of personal data.

Recording of a transfer

Article 71

The transfer of personal data to a third country shall be recorded in accordance with the provisions of subparagraph 10 of the first paragraph of Article 26 of this Act.

PART VI

SECTORAL ARRANGEMENTS

Chapter 1

Direct marketing

Rights and responsibilities of controller

Article 72

(1) Data controller may use the personal data of individuals that he obtained from publicly accessible sources or within the framework of the lawful[29] performance of activities, also for the purposes of offering goods, services, employment or temporary performance of work through the use of postal services, telephone calls, electronic mail or other telecommunications means (hereinafter: direct marketing[30]) in accordance with the provisions of this Chapter, unless otherwise provided by another statute.

(2) For the purposes of direct marketing, data controller may use only the following personal data collected in accordance with the previous paragraph: personal name, address of

[29] Verbatim: statutory (in accordance with a statute).
[30] The definition of direct marketing is therefore: "Data controller's use the personal data of individuals that he obtained from publicly accessible sources or within the framework of the lawful performance of activities, also for the purposes of offering goods, services, employment or temporary performance of work through the use of postal services, telephone calls, electronic mail or other telecommunications means.".

permanent or temporary residence, telephone number, e-mail address and fax number. On the basis of personal consent of the individual, data controller may also process other personal data, but may only process sensitive personal data if he possesses the personal consent of an individual, that is explicit and as a rule in writing.

(3) Data controller must perform direct marketing in such a way that upon the performance of direct marketing the individual is informed of his rights from Article 73 of this Act.

(4) If a data controller intends to supply personal data from the second paragraph of this Article to other data recipients for the purposes of direct marketing or to data processors, he shall be bound to inform the individual of this and prior to the supply of personal data obtain the individual's written consent. The notification to the individual regarding the intended supply must contain information as to the data intended to be supplied, to whom, and for what purpose. The costs of notification shall be borne by the data controller.

Rights of individual

Article 73

(1) Individual may at any time in writing or in another agreed manner request that the data controller permanently or temporarily cease to use his personal data for the purpose of direct marketing. The data controller shall be obliged within 15 days to prevent as appropriate the use of personal data for the purpose of direct marketing, and within the subsequent 5 days to inform in writing or another agreed manner the individual who so requested.

(2) The costs of all actions of the data controller in relation to request from the previous paragraph shall be borne by the controller.

Chapter 2

Video surveillance

General provisions

Article 74

(1) The provisions of this Chapter shall apply to the implementation of video surveillance, unless otherwise provided by another statute.

(2) A public or private sector person that conducts video surveillance must publish a notice to that effect. Such notice must be visible and plainly made public in a manner that enables individuals to acquaint themselves about its implementation at the latest when the video surveillance of them begins.

(3) The notice from the previous paragraph must contain the following information:
1. that video surveillance is taking place;

2. the title of the person in the public or private sector implementing it;

3. a telephone number to obtain information as to where and for which period recordings from the video surveillance system are stored.

(4) Through notification from the second paragraph of this Article the individual shall be deemed to have been informed of the processing of personal data pursuant to Article 19 of this Act.

(5) The video surveillance system used to conduct video surveillance must be protected against access by unauthorised persons.

Access to official office premises and business premises

Article 75

(1) The public and private sector may implement video surveillance of access to their official office premises or business premises if necessary for the security of people or property, for ensuring supervision of entering to or exiting from their official or business premises, or where due to the nature of the work there exists a potential threat to employees. The decision shall be taken by the competent functionary, head, director or other competent or authorised individual of the person in the public sector or person in the private sector. The written decision must explain the reasons for the introduction of video surveillance. The introduction of video surveillance may also be laid down by statute or a regulation issued pursuant thereto.

(2) Video surveillance may only be implemented in a manner that does not show recordings of the interior of residential buildings that do not affect entrance to their premises, or recordings of entrances to apartments.

(3) All employees of the person in the public or private sector working in the premises under surveillance must be informed in writing of the implementation of video surveillance.

(4) The filing system under this Article shall contain a recording of the individual (an image or sound), and the date and time of entry to and exit from the premises, it may also contain the personal name of the recorded individual, the address of his permanent or temporary residence, employment, the number and data on the type of his personal document, and the reason for entry, if the personal data listed are collected in addition to or through the recording of the video surveillance system.

(5) Personal data from the previous paragraph may be stored for a maximum of one year from their creation, and shall then be erased, unless otherwise provided for by statute.

Apartment buildings

Article 76

(1) The written consent of joint owners with a share of more than 70% of the ownership shall be required for the introduction of video surveillance in an apartment building.

(2) Video surveillance may only be introduced in an apartment building when necessary for the security of people and property.

(3) Video surveillance in apartment buildings may only monitor access to entrances and exits and common areas of apartment buildings. Video surveillance of the housekeeper's apartment and the workshop for the housekeeper shall be prohibited.

(4) It shall be prohibited to enable or implement current or subsequent examination of recordings of video surveillance systems through internal cable television, public cable television, the Internet or the use of other telecommunications means able to transmit such recordings.

(5) Entrances to individual apartments may not be recorded by video surveillance systems.

Work areas

Article 77

(1) Video surveillance within work areas may only be implemented in exceptional cases when necessarily required for the safety of people or property or to protect secret data and business secrets, and where such purpose cannot be achieved by milder means.

(2) Video surveillance may only be implemented for those parts of areas where the interests from the previous paragraph must be protected.

(3) Video surveillance shall be prohibited in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas.

(4) Employees must be informed in advance in writing prior to the commencement of implementation of video surveillance.

(5) Prior to the introduction of video surveillance in a person of the public or private sector, the employer shall be obliged to consult the representative trade union at the employer.

(6) In the area of national defence, national intelligence-security activities and the protection of secret data, the fourth and fifth paragraphs of this Article shall not apply.

Chapter 3

Biometrics

General provision

Article 78

The properties of an individual shall be determined or compared through the processing of biometric characteristics so as to identify him or confirm his identity (hereinafter: biometric measures) under the conditions provided by this Act.

Biometric measures in the public sector

Article 79

(1) Biometric measures in the public sector may only be provided for by statute if it is necessarily required for the security of people or property or to protect secret data and business secrets, and this purpose cannot be achieved by milder means.

(2) Irrespective of the previous paragraph, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.

Biometric measures in the private sector

Article 80

(1) The private sector may implement biometric measures only if they are necessarily required for the performance of activities, for the security of people or property, or to protect secret data or business secrets. Biometric measures may only be used on employees if they were informed in writing thereof in advance.

(2) If the implementation of specific biometric measures in the private sector is not regulated by statute, a data controller intending to implement biometric measures shall prior to introducing the measures be obliged to supply the National Supervisory Body with a description of the intended measures and the reasons for the introduction thereof.

(3) The National Supervisory Body shall on receipt of information from the previous paragraph be obliged within two months to decide whether the intended introduction of biometric measures complies with this Act, and in particular with the conditions from the first sentence of the first paragraph of this Article. The deadline may be extended by a maximum of one month if the introduction of such measures would affect more than 20 employees in a person in the private sector, or if the representative trade union at the employer requests to participate in the administrative procedure.

(4) The data controller may implement biometric measures upon receipt of a decision from the previous paragraph whereby the implementation of biometric measures is permitted.

(5) There shall be no appeal against a decision of the National Supervisory Body from the third paragraph of this Article, but an administrative dispute shall be permitted.

Biometric measures in connection with public sector employees

Article 81

Irrespective of the provision of Article 79 of this Act, biometric measures may be implemented in the public sector in connection with entry into a building or parts of a

building and recording the presence of employees at work, and they shall be implemented with the *mutatis mutandis* application of the second, third and fourth paragraphs of Article 80 of this Act.

Chapter 4

Records of entry to and exit from premises

Records

Article 82

(1) Persons in the public or private sector may, for the purposes of protecting property or the life and bodies of individuals, and order in their premises, require individuals intending to enter or leave such premises to state all or some of the personal data from the second paragraph of this Article and the reason for entry or exit. If required, the personal data may be verified by examining a personal document of the individual.

(2) The records of entry and exit may only contain the following personal data for individuals: personal name, number and type of personal document, address of permanent or temporary residence, employment, and the date of, time of and reason for entry or exit to or from the premises.

(3) Records from the previous paragraph shall be regarded as official records in accordance with the statute regulating the general administrative procedure, if the acquisition of data is required in terms of benefiting a minor or for the implementation of the competences of the police, and intelligence-security activities.

(4) Personal data from the records from the second paragraph of this Article may be stored for a maximum of three years from their recording, and then shall be erased, unless otherwise provided by statute.

Chapter 5

Public books and protection of personal data

Statutory purpose of public books

Article 83

Personal data from public books regulated by statute may only be used in accordance with the purpose for which they were collected or are processed, if the statutory purpose of their collection or processing is defined or definable.

Chapter 6

Connecting filing systems

Official records and public books

Article 84

(1) Filing systems from official records and public books may be connected if so provided by statute.

(2) Data controllers or a data controller connecting two or more filing systems kept for different purposes shall be obliged to inform the National Supervisory Body in writing thereof in advance.

(3) If at least one filing system to be connected contains sensitive data, or if the connecting would result in disclosure of sensitive data, or if implementation of the connecting requires the use of the same connecting code, connecting shall not be permitted without the prior permission of the National Supervisory Body.

(4) The National Supervisory Body shall permit connecting from the previous paragraph on the basis of a written application of the data controller if it determines that the data controller ensures adequate protection of personal data.

(5) There shall be no appeal against decisions from the previous paragraph, but an administrative dispute shall be permitted.

Prohibition of connecting

Article 85

Connecting filing systems from criminal record and minor offence records to other filing systems, and connecting filing systems from criminal records and minor offence records, shall be prohibited.

Special provisions

Article 86

Data on connected filing systems from official records and public books shall be kept separately in the Register of Filing Systems.

Chapter 7

Expert supervision

Application of the provisions of this Chapter

Article 87

Unless otherwise provided by another statute, the provisions of this Chapter shall apply for the processing of personal data in expert supervision provided by the statute[31].

General provisions

Article 88

(1) Public sector person performing expert supervision (hereinafter: implementer of expert supervision) may process personal data processed by data controllers over whom by statute he is competent to implement expert supervision.

(2) Expert supervisor shall have the right to consult, extract, transcribe or copy all personal data from the previous paragraph, but during their processing for the purposes of expert supervision and production of a report or assessment he shall be bound to protect their secrecy. In report or assessment upon the conclusion of expert supervision, implementer of expert supervision may note down only those personal data that are essential for achieving the purpose of the expert supervision.

(3) The costs of consultation, extraction, transcription or copying from the previous paragraph shall be borne by the data controller.

Expert supervision and further processing of personal data

Article 89

(1) In performing expert supervision, where in accordance with the first paragraph of Article 88 of this Act personal data are processed, implementer of expert supervision may inform in writing the individual to whom the personal data relate, that he is performing expert supervision and inform the individual that he may give his opinion in writing or orally.

(2) The individual from the previous paragraph may supply to the implementer of expert supervision for the purposes of performing expert supervision the personal data of another individual that may know something about the matter in which expert supervision is being performed. If the implementer of expert supervision deems it necessary, he may conduct an interview also with the other individual.

[31] This means other statutes, not the Personal Data Protection Act.

Expert supervision and sensitive personal data

Article 90

If in the performance of expert supervision sensitive personal data are processed, the implementer of expert supervision shall make an official annotation or other official record of this in the case file of the data controller.

PART VII

PENAL PROVISIONS

General violations of the provisions of this Act

Article 91

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity:
1. if he processes personal data without having the statutory grounds or personal consent of the individual to so do (Article 8);

2. if he entrusts an individual task relating to the processing of personal data to another person without concluding a contract in accordance with the second paragraph of Article 11;

3. if he processes sensitive personal data in contravention of Articles 13 or does not protect them in accordance with Article 14:

4. if he automatically processes personal data in contravention of Article 15;

5. if he collects personal data for purposes that are not defined and lawful[32], or if he continues to process them in contravention of Article 16;

6. if he supplies to a data recipient personal data in contravention of the second paragraph of Article 17 or if he does not destroy personal data in accordance with the third paragraph of Article 17 or does not publish the results of processing in accordance with the fourth paragraph of Article 17;

7. if he does not inform the individual of the processing of personal data in accordance with Article 19;

8. if he uses the same linking code in contravention of Article 20;

[32] Verbatim: statutory (in accordance with a statute).

9. if he does not delete, destroy, block or anonymise personal data after the purpose for which they were processed has been achieved in accordance with the second paragraph of Article 21;

10. if he acts in contravention of Article 22;

11. if he fails to ensure that the filing system catalogue contains data provided by statute (Article 26);

12. if he fails to supply data for the needs of the Register of Filing Systems (Article 27);

13. if he acts in contravention of the first or second paragraphs of Article 30 or the second, third or fifth paragraphs of Article 31;

14. if he acts in contravention of Article 32 or the second or fifth paragraphs of Article 33;

15. if he acts in contravention of the first paragraph of Article 63 or in contravention of Article 70 transfers personal data to a third country;

(2) A fine from EUR 830 to 2.080 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

(3) A fine from EUR 830 to 2.080 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine from EUR 200 to 830 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

Violation of the provisions on contractual processing

Article 92

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity, if he oversteps the authorisation contained in the contract from the second paragraph of Article 11 or does not return personal data in accordance with the third paragraph of Article 11.

(2) A fine from EUR 830 to 2.080 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

(3) A fine from EUR 830 to 2.080 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine from EUR 200 to 830 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

Violation of the provisions on security of personal data

Article 93

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity, if he processes personal data in accordance with this Act and fails to ensure security of personal data (Articles 24 and 25).

(2) A fine from EUR 830 to 1.250 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

(3) A fine from EUR 830 to 1.250 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine from EUR 200 to 830 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

Violation of the provisions on direct marketing

Article 94

(1) A fine from EUR 2.080 to 4.170 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity, if in accordance with this Act he processes personal data for the purposes of direct marketing and does not act in accordance with Articles 72 or 73.

(2) A fine from EUR 410 to 1.250 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

(3) A fine from EUR 200 to 830 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

Violation of general provisions on video surveillance

Article 95

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity:
1. if he does not publish a notice in the manner set out in the second paragraph of Article 74;

2. if the notice does not contain the information from the third paragraph of Article 74;

3. if he does not protect the video surveillance system used to perform video surveillance in contravention of the fifth paragraph of Article 74.

(2) A fine from EUR 830 to 1.250 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.

(3) A fine from EUR 830 to 1.250 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine from EUR 200 to 830 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

Violation of the provisions on video surveillance regarding access to official office premises and business premises

Article 96

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity:
1. if he implements video surveillance without an explained written decision or without other legal grounds from the first paragraph of Article 75;

2. if he implements video surveillance so as to show recordings of the interior of residential buildings that do not affect access to his premises or recordings of entrances to apartments (second paragraph of Article 75);

3. if he does not inform employees in writing (third paragraph of Article 75);

4. if he stores personal data in contravention of the fifth paragraph of Article 75.

(2) A fine from EUR 830 to 1.250 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

(3) A fine from EUR 830 to 1.250 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine from EUR 200 to 830 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

Violation of the provisions on video surveillance in apartment buildings

Article 97

(1) A fine from EUR 2.080 to 8.340 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity, who implements video surveillance in contravention of Article 76.

(2) A fine from EUR 410 to 1.250 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

(3) A fine from EUR 830 to 1.250 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine from EUR 200 to 410 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

Violation of the provisions on video surveillance in work areas

Article 98

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity, who implements video surveillance in work areas in contravention of Article 77.

(2) A fine from EUR 1.250 to 2.080 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

(3) A fine from EUR 1.250 to 2.080 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine from EUR 830 to 1.200 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

Violation of the provisions on biometrics in the public sector

Article 99

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person in the public sector who implements biometric measures in contravention of Article 79.

(2) A fine from EUR 1.250 to 2.080 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person in the public sector.

(3) A fine from EUR 1.250 to 2.080 shall be imposed for a minor offence from the first paragraph of this Article on the responsible person of the state body or body of self-governing local community who commits the act from the first paragraph of this Article.

Violation of the provisions on biometrics in the private sector

Article 100

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity, who implements biometric measures in contravention of Article 80.

(2) A fine from EUR 1.250 to 2.080 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

Violation of the provisions on records of entry and exit

Article 101

(1) A fine from EUR 2.080 to 4.170 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity:
1. who uses entry and exit records as official records in contravention of the third paragraph of Article 82;

2. who acts in contravention of the fourth paragraph of Article 82.

(2) A fine from EUR 200 to 830 shall be imposed for a minor offence on the responsible person of the legal person, sole trader or individual independently performing an activity who commits a minor offence from the previous paragraph.

(3) A fine from EUR 200 to 830 shall be imposed for a minor offence on the responsible person of the state body or body of self-governing local community who commits a minor offence from the first paragraph of this Article.

(4) A fine from EUR 200 to 410 shall be imposed for a minor offence on the individual who commits a minor offence from the first paragraph of this Article.

Violation of the provisions on connecting filing systems

Article 102

(1) A fine from EUR 830 to 2.080 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community, who connects filing systems in contravention of the third paragraph of Article 84.

(2) A fine from EUR 830 2.080 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community, who connects filing systems from criminal record and minor offence records with other filing systems, or connects filing systems from criminal records with filing systems from records on minor offences (Article 85).

Violation of the provisions on expert supervision

Article 103

(1) A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person:
1. if he performs expert supervision in contravention of the second paragraph of Article 88;

2. if he does not make an official annotation or other official record in contravention of Article 90 of this Act.

(2) A fine from EUR 830 to 1.250 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person.

(3) A fine from EUR 830 to 1.250 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine from EUR 200 to 830 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

PART VIII

TRANSITIONAL AND FINAL PROVISIONS

~~Competences of the Commissioner for Access to Information of a Public Character regarding protection of personal data~~

~~Article 104~~

~~(1) Until the entry into force of the statute governing this issue, the Commissioner for Access to Information of a Public Character may initiate an administrative dispute against a decision or resolution of the National Supervisory Body, if he determines that this has violated access to information of a public nature.~~

~~(2) The administrative dispute procedure from the previous paragraph shall be urgent and a priority.~~

~~(3) The Commissioner for Access to Information of a Public Character shall be bound to deliver to the National Supervisory Body a decision or resolution in which the he has taken a position regarding the issue of protection of personal data.~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05]

Deadline for issuing implementing regulations

Article 105

(1) The rules from the third paragraph of Article 28 and Article 69 of this Act shall be issued within two months of the entry into force of this Act.

(2) The regulation from the second paragraph of Article 52 of this Act shall be issued by 1 January 2006.

Transitional arrangements

Article 106

(1) Public funds may on the basis of personal consent from individuals process and collect personal data relating to them if such data are necessary and appropriate for the implementation of their tasks and competences, irrespective of the provisions of statutes regulating their tasks and competences and of the provisions of this Act until the entry into force of a special statute regulating this issue.

(2) Data controllers may supply to the public and publish the personal name, title or function, official telephone number and official electronic mail address of the head and those employees whose work is important for operations with clients or users of services, until the entry into force of a special statute regulating this issue.

The term data controller

Article 107

The terms "filing system controller", "controller of data", "databases controller" or "database controller" which are provided in statutes shall be deemed to mean the term "data controller" under this Act.

~~***Start of operation of the National Supervisory Body for Personal Data Protection***~~

~~*Article 108*~~

~~*(1) The National Supervisory Body for Personal Data Protection shall begin to operate on 1 January 2006.*~~

~~*(2) Until the National Supervisory Body for Personal Data Protection starts to operate, its competences and tasks under this Act shall be performed by the Inspectorate for Personal Data Protection of the Republic of Slovenia as a body within the Ministry of Justice and by Inspectors appointed pursuant to the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01- correction, 52/02-ZDU-1 and 73/04 – ZUP-C).*~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05]

~~***Appointment of the Chief National Supervisor***~~

~~*Article 109*~~

~~*(1) The procedure for appointment of the Chief National Supervisor shall start no later than on 1 June 2005.*~~

~~*(2) On the day of the appointment of the Chief National Supervisor, the term of office of the Chief Inspector for Personal Data Protection shall cease.*~~

~~*(3) If the Chief National Supervisor is appointed prior to the start of work of the National Supervisory Body for Personal Data Protection, the Chief National Supervisor shall be the head of the Inspectorate for Personal Data Protection of the Republic of Slovenia as a body within the Ministry of Justice up until the start of work by the National Supervisory Body for Personal Data Protection.*~~

~~*(4) If the Chief National Supervisor is not appointed by the time the National Supervisory Body for Personal Data Protection begins working, his function shall be performed by the Chief Inspector for Personal Data Protection as Acting Chief National Supervisor until the appointment is made.*~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05]

~~***Take-over of employees and archives***~~

~~*Article 110*~~

~~*(1) The National Supervisory Body for Personal Data Protection shall take over Inspectors and other employees who on the day the National Supervisory Body for Personal Data Protection begins operating are performing work at the Inspectorate for Personal Data Protection of the Republic of Slovenia.*~~

~~*(2) Unfinished matters, archives and records maintained by the Inspectorate for Personal Data Protection of the Republic of Slovenia shall be transferred to the National Supervisory Body for Personal Data Protection.*~~

[Repealed by the Information Commissioner Act, Official Gazette of the RS, No. 113/05]

Application of individual provisions of this Act

Article 111

(1) The provisions of the second paragraph of Article 48 and subparagraphs 3 and 4 of the first paragraph of Article 49 of this Act shall start to apply on the day the National Supervisory Body for Personal Data Protection begins operating.

(2) Until the establishing of the website of the National Supervisory Body for Personal Data Protection, the information which the National Supervisory Body shall publish under this Act on its website shall be published on the website of the Ministry of Justice.

Completion of current proceedings

Article 112

If a decision or ruling of an Inspector has been issued prior to the entry into force of this Act, the procedure shall be completed under the provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01- correction, 52/02-ZDU-1 and 73/04 – ZUP-C).

Transfer of management of the Register of Filing Systems

Article 113

(1) The Joint Catalogue of Personal Data managed under the provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01 – correction, 52/02 – ZDU-1 and 73/04 – ZUP-C), shall on the date of entry into force of this Act be renamed the Register of Filing Systems.

(2) Until 1 January 2006 the Register from the previous paragraph shall be managed and maintained by the Ministry of Justice, and on that date it shall be handed over to the National Supervisory Body for Personal Data Protection.

Supplement to data in the Register of Filing Systems

Article 114

Data controllers who have supplied personal data under the provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01 – correction, 52/02 – ZDU-1 and 73/04 – ZUP-C) to the Joint Catalogue of Personal Data must supply all data from Article 27 of this Act to the competent body from Article 113 of this Act within one year of the entry into force of the implementing regulation from the third paragraph of Article 28 of this Act.

Cessation of validity

Article 115

(1) On the day this Act enters into force, the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01- correction, 52/02-ZDU-1 and 73/04 – ZUP-C) shall cease to have effect.

(2) On the day the National Supervisory Body for Personal Data Protection begins operating, the second subparagraph of the first paragraph and the third paragraph of Article 13 of the Regulation on Bodies within Ministries (Official Gazette of the Republic of Slovenia, No. 58/03) shall cease to have effect.

(3) On the day this Act enters into force, the provisions of the first paragraph of Article 110 and the second paragraph of Article 111 of the Electronic Communications Act (Official Gazette of the Republic of Slovenia, No. 43/04) shall cease to have effect in that part laying down the collection, processing and publication of the EMŠO – the unique personal registration number.

Amendment of other statute

Article 116

In the Act Ratifying the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Official Gazette of the Republic of Slovenia, No. 11/94 – International Treaties, No. 3/94) in Article 3 the wording "science and technology" shall be replaced by wording "justice".

Entry into Force

Article 117

This Act shall enter into force on 1 January 2005.

No. 210-01/89-3/25
Ljubljana, 15 July 2004
EPA 1228-III

President
of the National Assembly
of the Republic of Slovenia
Feri Horvat (signed)

.

Appendix 1

CONSTITUTION OF THE REPUBLIC OF SLOVENIA[33]

Article 38

(**Protection of Personal Data**)

The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.

The collection, processing, purpose of use, supervision and protection of the secrecy of personal data shall be provided by statute.

Everyone has the right of access to the collected personal data that relate to him and the right to judicial protection in the event of abuse of such data.

Appendix 2

The English language translation of the text of the Information Commissioner Act below is provided for information only and confers no rights nor imposes any obligations on anyone. Only the official publication of the Act in Slovene language, as published and promulgated in the Official Gazette of the Republic of Slovenia, is authentic. This translation was prepared by the Office of the Information Commissioner.

INFORMATION COMMISSIONER ACT[34]

I. GENERAL PROVISIONS

Article 1

(1) With this Act an Information Commissioner (hereinafter: Information Commissioner) is established and his duties and powers defined.

(2) This Act implements into the Slovenian legal order the Directive 95/46/EC of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data from 24 October 1995.

[33] Official Gazette of the Republic of Slovenia, Nos. 33/91-I, 42/97, 66/2000, 24/2003, 69/2004, 68/2006 and 47/2013. Constitution of the Republic of Slovenia is in Slovene language: "Ustava Republike Slovenije".
[34] Official Gazette of the Republic of Slovenia, Nos. 113/2005 and 51/2007-ZustS-A. Information Commissioner Act is in Slovene language: "Zakon o Informacijskem pooblaščencu".

Article 2

(1) The Information Commissioner is an autonomous and independent state body, competent for:
- deciding on the appeal against the decision with which a body refused or dismissed the applicant's request for access or violated the right to access or re-use of public information in some other way, and within the frame of appellate proceedings also for supervision over implementation of the Act regulating the access to public information and regulations adopted there under,
- **inspection supervision over implementation of the statute and other regulations, regulating protection or processing of personal data or the transfer of personal data from Slovenia, as well as carrying out other duties, defined by these regulations,**
- **deciding on the appeal of an individual when the data controller refuses his request for data, extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the statute regulating personal data protection.**

(2) The Information Commissioner is a minore offence body, competent for supervision over this Act and the statute regulating personal data protection.

(3) The Information Commissioner has the following competencies:
- **organizes and manages the work of all employees, including the national supervisors for personal data protection;**
- carries out other competencies of the head of the state body;
- conducts supervision in accordance with the statute regulating personal data protection.

Article 3
(Meaning and renaming of terms)

(1) Bodies under this Act are state bodies, local government bodies, public agencies, public funds and other entities of public law, public powers holders and public service contractors (hereinafter: "the bodies").

(2) The official of the body according to this Act is an official, competent for transmission of public information or the head of the body.

(3) When another statute or regulation uses terms "Chief National Supervisor", "National supervisory body for personal data protection" or "Commissioner for Access to Public Information" these terms mean "Information Commissioner".

Article 4

(1) The seat of Information Commissioner is in Ljubljana.

(2) Information Commissioner establishes his organizational structure with standing orders and other general acts.

Article 5
(Budgetary funds)

Funds for Information Commissioner's operation are provided from the Budget of the Republic of Slovenia and shall be determined by the National Assembly of the Republic of Slovenia on proposal of the Information Commissioner.

2. Appointment and position of the Information Commissioner

Article 6
(Appointment of the Information Commissioner)

(1) Information Commissioner is appointed by the National Assembly of the Republic of Slovenia on proposal of the President of the Republic of Slovenia.

(2) For the appointment as Information Commissioner, a person must fulfil the following conditions:
- be a citizen of the Republic of Slovenia;
- hold a university degree;
- have at least five years of working experience;
- must not have been convicted by a final decision of a criminal offence punishable by an unconditional punishment of deprivation of liberty.

(3) Information Commissioner is appointed for a five year's term and can be reappointed once.

Article 7

(Status of the Information Commissioner and his dismissal)

(1) Information Commissioner has the status of state functionary.

(2) Information Commissioner may be subject to early dismissal by the National Assembly of the Republic of Slovenia only if:
- he himself so demands,
- if he no longer fulfils the conditions for execution of the function determined in the Article 6(2) of this Act.
- if he becomes permanently incapable of performing his function,
- if he neglects to execute his powers in accordance with the Law and Constitution.

(3) The procedure for the dismissal of the Information Commissioner shall be started on proposal of the president of the Republic of Slovenia.

(4) With regard to incompatibility of the Information Commissioner's function with other functions and activities the Human Rights Ombudsman Act applies by analogy.

3. National Supervisors for personal data protection and expert staff of the Information Commissioner

Article 8

(National Supervisor)

(1) Information Commissioner employs National Supervisors for personal data protection (hereinafter: Supervisors).

(2) A person to be appointed as Supervisor must hold a university degree; have at least five years of working experience and a certificate of professional examination for the position of inspector pursuant to the Act governing inspections.

(3) Supervisors have the position, rights and obligations, as determined for inspectors by Act governing inspections and Act governing civil servants.

(4) Supervisors are appointed by Information Commissioner in accordance with the Civil Servants Act.

(5) During the execution of duties of supervision and other duties within the frame of the Act on personal data protection supervisors are autonomous in accordance with their mandate and operate within the frame of constitution and legislation.

(6) While performing duties, which do not include supervision, they are bound by Information Commissioner's written instructions.

Article 9

(Expert staff of the Information Commissioner)

Information Commissioner has an expert and administrative-technical staff.

4. Procedure before the Information Commissioner

Article 10
(Acquiring requested information and documents in cases of access to public information)

(1) If necessary to deal with a complaint, the official of the body must immediately send to the Information Commissioner on his demand the documents, dossiers, registers, records or other documentary material, requested by the applicant. Within the frame of his competency, the Information Commissioner can also view a tax secret.

(2) If, when dealing with a complaint in a case of access to public information the Information Commissioner suspects that the first level body holds the requested information, but does not entirely or partially reveal it to the Information Commissioner, the Commissioner can use powers in accordance with the Act governing inspections.

(3) If the body does not initiate an administrative dispute against the Information Commissioner's decision, it must in accordance with the decision transmit the requested document, file, dossier, register, record or documentary material to the applicant.

(4) Procedures in an administrative dispute against the decision or procedural conclusion issued by the Information Commissioner are urgent and privileged.

Article 11

(Procedural acts in cases of access to public information)

Information Commissioner can conclude a procedural act in case of access to public information without the presence of the party, requesting access to public information, or the person with rights and obligations of a party, if such conduct is necessary for prevention of access to requested information prior to the Information Commissioner's final decision.

Article 12

(File examination in cases of access and re-use of public information)

(1) The parties' right to examine documents in cases of access to information according to the Act governing the general administrative procedure excludes the examination of the requested document and other documents of the case, which could reveal or point to the contents of the requested information.

(2) After the final decision of the Information Commissioner the parties' right referred to in the previous paragraph of this Article includes the examination of the requested document within the frame allowed for, by the final decision of the Information Commissioner.

~~**Article 13**~~

~~**(Competencies with regard to regulations)**~~

~~Information Commissioner can file to the Constitutional Court of the Republic of Slovenia a request for constitutional review of a statute, of other regulations and general acts, adopted to perform public powers, in case of questions of constitutionality and legality in connection with a procedure being dealt with.~~

[Repealed by the Act on Changes and Amendments to the Constitutional Court Act, Official Gazette of the RS, No. 51/2007. This provision on direct access to the Constitutional Court was transferred into Article 23.a, paragraph 1, item 6 of the Constitutional Court Act. See Appendix 3.]

Article 14

(Reports of the Information Commissioner)

(1) Information Commissioner transmits an Annual Report on his work to the National Assembly at the latest on 31 May for the previous year and publishes the report on his web site.

(2) The annual report consists of data on previous year's activities as well as estimates and recommendations in the area of personal data protection and access to public information.

5. Penal provisions

Article 15

(Liability for minor offences)

(1) A fine in range of SIT 100.000 to SIT 250.000 will be imposed upon an official responsible for a violation, with which according to the provision of Article 10(1) of this Act, while delivering the applicant's appeal, in spite so requested, the official fails to transfer to the Information Commissioner the demanded document, case, dossier, register, record or documentary material, although they are in the bodies' possession.

(2) A fine in range of SIT 100.000 to SIT 250.000 will be imposed upon an official responsible for a violation, when according to the provision of Article 10(3) of this Act, in spite of the Information Commissioner's decision, the official fails to transfer the required document, case, dossier, register, record or documentary material to the applicant.

(3) A fine in range of SIT 100.000 to SIT 250.000 will be imposed upon a responsible official of the data controller, who in spite of the Information Commissioner's decision on a case of applicant's appeal from point 3 of Article 2(1) of this Act, fails to assure the applicant the right defined in point 3 of Article 2(1).

6. Transitional and final provisions

Article 16

(Expiry of validity)

On a day of entry into force of this Act the provisions of Articles 38 to 46, 57 and 104, 108 to 110 of the Personal Data Protection Act (Official Gazette, No. 86/04 – ZVOP-1) and provisions of Articles 28 to 30 of the Act on Access to Information of Public Character (Official Gazette, Nos. 24/03 and 61/05 – ZDIJZ) cease to be valid.

Article 17

(Continuation of work)

With the entry into force of this Act the Commissioner for Access to Information of Public Character continues to perform his duties as Information Commissioner until the expiry of his term of appointment as the Commissioner for access to public information.

Article 18

(Take over of employees and archives)

(1) Information Commissioner takes over Inspectors and other employees who, on the day of start of functioning of the Information Commissioner, perform their duties within the Inspectorate for Personal Data Protection of the Republic of Slovenia, together with the appurtenant equipment and resources.

(2) Information Commissioner takes over all pending cases, archives, and records, kept by Inspectorate for Personal Data Protection of the Republic of Slovenia.

Article 19

(Information Commissioner's salary)

Until the entry into validity of the ordinance governing the salaries of holders of public functions, the Information Commissioner's salary is determined according to the salary of the President of the National Review Commission.

Article 20

(Entry into validity)

This Act shall enter into validity on the 15th day following its publication in the Official Gazette of the Republic of Slovenia.[35]

The English language translation of the text of the Information Commissioner Act above is provided for information only and confers no rights nor imposes any obligations on anyone. Only the official publication of the Act in Slovene language, as published and promulgated in the Official Gazette of the Republic of Slovenia, is authentic. This translation was prepared by the Office of the Information Commissioner.

Appendix 3

CONSTITUTIONAL COURT ACT[36]

Article 23.a

(1) The procedure for the review of the constitutionality or legality of regulations or general acts issued for the exercise of public authority can be initiated by a request submitted by:
- the National Assembly;

[35] The Information Commissioner Act was published in the Official Gazette of the Republic of Slovenia, No. 113/2005 on 16 December 2005 and entered into force on 31 December 2005.
[36] Official Gazette of the Republic of Slovenia, Nos. 15/94, 64/01 – ZPKSMS, 51/2007, 64/2007 – Officially Consolidated Text and 109/2012. Constitutional Court Act is in Slovene language: "Zakon o ustavnem sodišču".

- one third of the deputies;
- the National Council;
- the Government;
- the Human Rights Ombudsman if he deems that a regulation or general act issued for the exercise of public authority inadmissibly interferes with human rights or fundamental freedoms;
- the Information Commissioner, provided that a question of constitutionality or legality arises in connection with a procedure he is conducting;
- the Bank of Slovenia or the Court of Audit, provided that a question of constitutionality or legality arises in connection with a procedure they are conducting;
- the State Prosecutor General, provided that a question of constitutionality arises in connection with a case the State Prosecutor's Office is conducting;
- representative bodies of local communities, provided that the constitutional position or constitutional rights of a local community are interfered with;
- representative associations of local communities, provided that the rights of local communities are threatened;
- national representative trade unions for an individual activity or profession, provided that the rights of workers are threatened.

(2) The applicants referred to in the preceding paragraph may not submit a request to initiate the procedure for the review of the constitutionality or legality of regulations and general acts issued for the exercise of public authority which they have adopted by themselves.

Appendix 4

CRIMINAL CODE[37]

Abuse of Personal Data
Article 143

(1) Whoever publishes or transmits for publication personal data processed without the basis of the statute or the personal consent of the individual to whom the personal data relate, that are processed on the basis of statute or with the personal consent of the individual,

shall be punished by a fine or by imprisonment of up to one year.

(2) Whoever breaks into a computer database in order to acquire personal data for his or a third person's use shall be punished in accordance with the preceding paragraph.

(3) Whoever publishes on the World Wide Web or publishes in another manner or enables another person to publish personal data of victims of criminal offences, victims of violation of rights and liberties, protected witnesses, which are contained in judicial records of court

[37] Official Gazette of the Republic of Slovenia, Nos. 55/2008, 66/2008 – correction, 39/2009, 91/2011 and 50/2012 – Officially Consolidated Text. Criminal Code is in Slovene language: "Kazenski zakonik".

proceedings, in which the presence of the public or witness identification or protected witnesses and personal records thereof related to the court proceeding was not allowed according to the statute or court decision, on the basis of which these persons may be identified or are identifiable,

shall be punished by imprisonment of up to three years.

(4) Whoever assumes the identity of another person or, by processing his personal data, exploits his or her rights, gains proceeds or non-pecuniary benefits or adversely affects his personal dignity,

shall be punished by imprisonment from three months up to three years.

(5) Whoever commits the offence referred to in paragraph 1 of this Article by trnasminitting for publication or publishing sensitive personal data,

shall be punished by imprisonment of up to two years.

(6) If any offence from the preceding paragraphs of this Article is committed by an official person through the abuse of office or official authority,

he shall be punished by imprisonment of up to five years.

(7) The prosecution under paragraph 4 of this Article shall be initiated upon a motion.

Appendix 5

OBLIGATIONS CODE[38]

Request to Cease Infringement of Personality Rights

Article 134

(1) All persons shall have the right to request the court or any other relevant authority to order that action that infringes the inviolability of the human person, personal and family life or any other personality right be ceased, that such action be prevented or that the consequences of such action be eliminated.

[38] Official Gazette of the Republic of Slovenia, Nos. 83/2001, 32/2004 – Authentic Interpretation of Article 195, 28/2006 - Decision of the Constitutional Court, 40/2007 and 97/2007 – Officially Consolidated Text. Obligations Code is in Slovene language: "Obligacijski zakonik".

(2) The court or other relevant authority may order that the violator cease such action, with failure to do so resulting in the mandatory payment of a monetary sum to the person affected, levied in total or per time unit.

Reimbursement of Material Damage in Case of Defamation or Calumny

Article 177

(1) Any person that defames another or asserts or disseminates untrue statements on the past, knowledge or capability of another, even though the former knows or should have known that they were untrue, and thereby inflicts material damage on the latter must reimburse such damage.

(2) However any person that reports anything untrue about another without knowing that such was untrue shall not be liable for the damage inflicted if there was a serious interest in so doing for the former or the person to whom the report was made.

Publication of Judgement or Correction

Article 178

In a case of the infringement of a personality right the court may order the publication of the judgement or a correction at the injurer's expense or order that the injurer must retract the statement by which the infringement was committed or do anything else through which it is possible to achieve the purpose achieved via compensation.

Monetary Compensation

Article 179

(1) Just monetary compensation independent of the reimbursement of material damage shall pertain to the injured party for physical distress suffered, for mental distress suffered owing to a reduction in life activities, disfigurement, the defamation of reputation or honour, the truncation of freedom or a personality right, or the death of a close person, and for fear, if the circumstances of the case, particularly the level and duration of distress and fear, so justify, even if there was no material damage.

(2) The amount of compensation for non-material damage shall depend on the importance of the good affected and the purpose of the compensation, and may not support tendencies that are not compatible with the nature and purpose thereof.

ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data

This is an unofficial translation that has been updated according to the changes operated in the Act after the Sentence 292/200 of the Spanish Constitutional Court

Please note that the only legally binding text
is that published in the Spanish Official Journal

I. General provisions

OFFICE OF THE HEAD OF STATE

23750 ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data.

JUAN CARLOS I
KING OF SPAIN

To whom it may concern.
Know ye that Parliament has passed, and I approve, the following Organic Law.

TITLE I

General provisions

Article 1. *Subject*

This Organic Law is intended to guarantee and protect the public liberties and fundamental rights of natural persons, and in particular their personal and family privacy, with regard to the processing of personal data.

Article 2. *Scope*

1. This Organic Law shall apply to personal data recorded on a physical support which makes them capable of processing, and to any type of subsequent use of such data by the public and private sectors.
This Organic Law shall govern any processing of personal data:

a) When the processing is carried out on Spanish territory as part of the activities of an establishment belonging to the person responsible for the processing.
b) When the person responsible for the processing is not established on Spanish territory but is subject to Spanish law pursuant to the norms of public international law.
c) When the person responsible for the processing is not established on the territory of the European Union and is using for the processing means situated on Spanish territory, unless such means are used solely for transit purposes.

2. The system of protection of personal data laid down by this Organic Law shall not apply to:

a) Files maintained by natural persons in the exercise of purely personal or household activities.
b) Files subject to the legislation on the protection of classified materials.
c) Files established for the investigation of terrorism and serious forms of organised crime. However, in such cases, the person responsible for the file shall previously inform the Data Protection Agency of its existence, its general characteristics and its purpose.

3. The following processing of personal data shall be governed by the specific provisions, and by any special provisions, of this Organic Law:

a) Files regulated by the legislation on the electoral system.
b) Those used solely for statistical purposes and protected by central or regional government legislation on public statistical activities.
c) Those intended for the storage of the data contained in the personal assessment reports covered by the legislation on the personnel regulations of the armed forces.
d) Those contained in the Civil Register and the Central Criminal Register.
e) Thos deriving from images and sound recorded by videocameras for the security forces in accordance with the relevant legislation.

Article 3. *Definitions*

The following definitions shall apply for the purposes of this Organic Law:

a) Personal data: any information concerning identified or identifiable natural persons.
b) File: any structured set of personal data, whatever the form or method of its creation, storage organisation and access.
c) Processing of data: operations and technical processes, whether or not by automatic means, which allow the collection, recording, storage, adaptation, modification, blocking and cancellation, as well as assignments of data resulting from communications, consultations, interconnections and transfers.
d) Controller: natural or legal person, whether public or private, or administrative body which determines the purpose, content and use of the processing.
e) Data subject: the natural person who owns the data undergoing the processing referred to in (c) above.
f) Dissociation procedure: any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person.
g) Processor: the natural or legal person, public authority, service or any other body which alone or jointly with others processes personal data on behalf of the controller.
h) Consent of the data subject: any free, unequivocal, specific and informed indication of his wishes by which the data subject consents to the processing of personal data relating to him.
i) Assignment or communication of data: any disclosure of data to a person other than the data subject.
j) Sources accessible to the public: those files which can be consulted by anyone, which are not subject to restrictive legislation, or which are subject only to payment of a consultation fee. Only the following shall be considered to be sources accessible to the public: the publicity register, telephone directories subject to the conditions laid down in the relevant regulations, and the lists of persons belonging to professional associations containing only data on the name, title, profession, activity, academic degree, address and an indication of his membership of the association. Newspapers, official gazettes and the media shall also be considered sources with public access.

TITLE II

Principles of data protection

Article 4. *Quality of the data*

1. Personal data may be collected for processing, and undergo such processing, only if they are adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which they were obtained.
2. Personal data subjected to processing may not be used for purposes incompatible with those for which they were collected. Further processing of the data for historical, statistical or scientific purposes shall not be considered incompatible.
3. Personal data shall be accurate and updated in such a way as to give a true picture of the current situation of the data subject.
4. If the personal data recorded prove to be inaccurate, either in whole or in part, or incomplete, shall be erased and officially replaced by the corresponding rectified or supplemented data, without prejudice to the rights granted to data subjects in Article 16.
5. Personal data shall be erased when they have ceased to be necessary or relevant for the purpose for which they were obtained or recorded.
They shall not be kept in a form which permits identification of the data subject for longer than necessary for the purposes for which they were obtained or recorded.
On a regular basis, the procedure shall be determined by which, exceptionally, it is decided to keep the entire set of particular data, in accordance with the specific legislation, because of their historical, statistical or scientific value.
6. Personal data shall be stored in a way which permits the right of access to be exercised, unless lawfully erased.
The collection of data by fraudulent, unfair or illicit means is prohibited.

Article 5. *Right of information in the collection of data*

1. Data subjects from who personal data are requested must previously be informed explicitly, precisely and unequivocally of the following:

a) The existence of a file or personal data processing operation, the purpose of collecting the data, and the recipients of the information.
b) The obligatory or voluntary nature of the reply to the questions put to them.
c) The consequences of obtaining the data or of refusing to provide them.
d) The possibility of exercising rights of access, rectification, erasure and objection.
e) The identity and address of the controller or of his representative, if any.

Where the controller is not established on the territory of the European Union, and he is using for the processing means situated on Spanish territory, he must, unless these means are being used for transit purposes, designate a representative in Spain, without prejudice to any action which may be taken against the controller himself.
2. Where questionnaires or other forms are used for collection, they must contain the warnings set out in the previous paragraph in a clearly legible form.

3. The information set out in subparagraphs (b), (c) and (d) of paragraph 1 shall not be required if its content can be clearly deduced from the nature of the personal data requested or the circumstances in which they are obtained.
4. Where the personal data have not been obtained from the data subject, he must be informed explicitly, precisely and unequivocally by the controller or his representative within three months from the recording of the data - unless he has been informed previously - of the content of the processing, the origin of the data, and the information set out in (a), (d) and (e) of paragraph 1 of this Article.
5. The provisions of the preceding paragraph shall not apply where explicitly provided for by law, when the processing is for historical, statistical or scientific purposes, or when it is not possible to inform the data subject, or where this would involve a disproportionate effort in the view of the Data Protection Agency or the corresponding regional body, in view of the number of data subjects, the age of the data and the possible compensatory measures.
The provisions of the preceding paragraph shall also not apply where the data come from sources accessible to the public and are intended for advertising activity or market research, in which case each communication sent to the data subject shall inform him of the origin of the data, the identity of the controller and the rights of the data subject.

Article 6. *Consent of the data subject*

1. Processing of personal data shall require the unambiguous consent of the data subject, unless laid down otherwise by law.
2. Consent shall not be required where the personal data are collected for the exercise of the functions proper to public administrations within the scope of their responsibilities; where they relate to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and are necessary for its maintenance or fulfilment; where the purpose of processing the data is to protect a vital interest of the data subject under the terms of Article 7(6) of this Law, or where the data are contained in sources accessible to the public and their processing is necessary to satisfy the legitimate interest pursued by the controller or that of the third party to whom the data are communicated, unless the fundamental rights and freedoms of the data subject are jeopardised.
3. The consent to which the Article refers may be revoked when there are justified grounds for doing so and the revocation does not have retroactive effect.
4. In the cases where the consent of the data subject is not required for processing personal data, and unless provided otherwise by law, the data subject may object to such processing when there are compelling and legitimate grounds relating to a particular personal situation. In such an event, the controller shall exclude the data relating to the data subject from the processing.

Article 7. *Data with special protection*

1. In accordance with the provisions of Article 16(2) of the Constitution, nobody may be obliged to state his ideology, religion or beliefs.
If, in relation to such data, the consent referred to in the following paragraph is sought, the data subject shall be warned of his right to refuse such consent.
2. Personal data which reveal the ideology, trade union membership, religion and beliefs may be processed only with the explicit and written consent of the data subject. Exceptions shall be files maintained by political parties, trade unions, churches, religious confessions or communities, and

associations, foundations and other non-profit-seeking bodies with a political, philosophical, religious or trade-union aim, as regards the data relating to their associates or members, without prejudice to the fact that assignment of such data shall always require the prior consent of the data subject.
3. Personal data which refer to racial origin, health or sex life may be collected, processed and assigned only when, for reasons of general interest, this is so provided for by law or the data subject has given his explicit consent.
4. Files created for the sole purpose of storing personal data which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin or sex life remain prohibited.
5, Personal data on criminal or administrative offences may be included in files of the competent public administrations only under the circumstances laid down in the respective regulations.
6. Notwithstanding the provisions of the preceding paragraphs, the personal data referred to in paragraphs 2 and 3 of this Article may be processed when such processing is necessary for purpose of preventive medicine or diagnosis, the provision of medical care or treatment, or the management of health-care services, provided such data processing is effected by a health professional subject to professional secrecy or by another person also subject to an equivalent obligation of secrecy.
The data referred to in the preceding subparagraph may also be processed when this is necessary to safeguard the vital interests of the data subject or another person in the event that the data subject is physically or legally incapable of giving his consent.

Article 8. *Data on health*

Without prejudice to the provisions of Article 11 on assignment, public and private health-care institutions and centres and the corresponding professionals may process personal data relating to the health of persons consulting them or admitted to them for treatment, in accordance with the provisions of the central or regional government legislation on health care.

Article 9. *Data security*

1. The controller or, where applicable, the processor shall adopt the technical and organisational measures necessary to ensure the security of the personal data and prevent their alteration, loss, unauthorised processing or access, having regard to the state of the art, the nature of the data stored and the risks to which they are exposed by virtue of human action or the physical or natural environment.
2. No personal data shall be recorded in files which do not meet the conditions laid down by rules regarding their integrity and security, as well as the rules governing the processing centres, premises, equipment, systems and programs.
3. Rules shall be laid down governing the requirements and conditions to be met by the files and the persons involved in the data processing referred to in Article 7 of this Law.

Article 10. *Duty of secrecy*

The controller and any persons involved in any stage of processing personal data shall be subject to professional secrecy as regards such data and to the duty to keep them. These obligations shall continue even after the end of the relations with the owner of the file or, where applicable, the person responsible for it.

Article 11. *Communication of data*

1. Personal data subjected to processing may be communicated to third persons only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject.
2. The consent required under the previous paragraph shall not be required:
a) when the transfer is authorised by a law.
b) when the data have been collected from publicly accessible sources.
c) when the processing corresponds to the free and legitimate acceptance of a legal relationship whose course, performance and monitoring necessarily involve the connection between such processing and files of third parties. In that case, communication shall be legitimate to the extent of the purpose justifying it.
d) when the communication to be effected is destined for the Ombudsman, the Office of Public Prosecutor, judges, courts or the Court of Auditors in the exercise of the functions assigned to them. Not shall consent be required when the communication is destined to regional government authorities with functions analogous to the Ombudsman or the Court of Auditors.
e) when the transfer is between public administrations and concerns the retrospective processing of the data for historical, statistical or scientific purposes.
f) when the transfer of personal data on health is necessary for resolving an emergency which requires access to a file or for conducting epidemiological studies within the meaning of central or regional government health legislation.
3. Consent for the communication of personal data to a third party shall be null and void when the information given to the data subject does not enable him to know the purpose for which the data whose communications is authorised will be used or the type of activity of the person to whom it is intended to communicate them.
4. Consent for the communication of personal data may also be revoked.
5. The person to who personal data are communicated is obliged, by the mere fact of the communication, to abide by the provisions of this Law.
6. If the communication is preceded by a depersonalisation procedure, the provisions of the preceding paragraphs shall not apply.

Article 12. *Access to data on behalf of third parties*

1. Access to data by a third party shall not be considered communication of data when such access is necessary for the provision of a service to the data controller.
2. Processing on behalf of third parties shall be regulated in a contract which must be in writing or in any other form which allows its performance and content to be assessed, it being expressly laid down that the processor shall process the data only in accordance with the instructions of the controller, shall not apply or use them for a purpose other than that set out in the said contract, and shall not communicate them to other persons even for their preservation.
The contract shall also set out the security measures referred to in Article 9 of this Law, which the processor is obliged to implement.
3. Once the contractual service has been provided, the personal data must be destroyed or returned to the controller, together with any support or documents contain personal data processed.
4. If the processor uses the data for another purpose, communicates them or uses them in a way not in accordance with the terms of the contract, he shall also be considered as the controller and shall be personally responsible for the infringements committed by him.

TITLE III

Rights of persons

Article 13. *Challenging assessments*

1. Citizens have the right not to be subject to a decision with legal consequences for them, or which significantly affects them, and which is based processing of data intended to assess certain aspects of their personality.
2. The data subject may challenge administrative acts or private decisions which involve an assessment of his behaviour, the only basis for which is the processing of personal data which provides a definition of his characteristics or personality.
3. In that case, the data subject shall have the right to obtain information from the controller on the assessment criteria and program used in the processing on the basis of which the decision containing the act was adopted.
4. An assessment of the behaviour of citizens based on data processing shall have conclusive force only at the request of the data subject.

Article 14. *Right to consult the General Data Protection Register*

Anyone may consult the General Data Protection Register to learn about the existence of personal data, their purpose and the identity of the controller. The General Register shall be open to public consultation free of charge.

Article 15. *Right of access*

1. The data subject shall have the right to request and obtain free of charge information on his personal data subjected to processing, on the origin of such data and on their communication or intended communication.
2. The information may be obtained by simply displaying the data for consultation or by indicating the data subjected to processing in writing, or in a copy, fax or photocopy, whether certified a true copy or not, in legible and intelligible form, and without using keys or codes which require the use of specific devices.
3. The right of access referred to in this Article may be exercised only at intervals of not less than twelve months, unless the data subject can prove a legitimate interest in doing so, in which case it may be exercised before then.

Article 16. *Right of rectification or cancellation*

The controller shall be obliged to implement the right of rectification or cancellation of the data subject within a period of ten days.
2. Rectification or cancellation shall apply to data whose processing is not in accordance with the provisions of this Law and, in particular, when such data are incorrect or incomplete.
3. Cancellation shall lead to the data being blocked and maintained solely at the disposal of the public administrations, judges and courts, for the purpose of determining any liability arising from the processing, and for the duration of such liability. On expiry of such liability, they shall be deleted.

4. If the data rectified or cancelled have previously been communicated, the controller shall notify the person to whom they have been communicated of the rectification or cancellation. If the processing is being maintained by that person, he shall also cancel the data.
5. Personal data shall be kept for the periods set out in the relevant provisions or, where applicable, in the contractual relations between the person or body responsible for the processing ("the controller") and the data subject.

Article 17. *Objection, access, rectification or cancellation procedure*

1. The procedures for exercising the right of objection, access, rectification and cancellation shall be established by regulation.
2. No consideration shall be demanded for the exercise of the rights of objection, access, rectification or cancellation.

Article 18. *Supervision of rights*

1. Acts contrary to the provisions of this Law may be the subject of complaints by data subjects to the Data Protection Agency in the form laid down by regulation.
2. A data subject who is denied, either wholly or partially, the exercise of the rights of objection, access, rectification or cancellation, may bring this to the attention of the Data Protection Agency or, where applicable, to the competent body in each Autonomous Community, which must decide on the admissibility or inadmissibility of the denial.
3. The maximum period within which a decision on the ownership of data must be reached shall be six months.
4. An appeal may be lodged against the decisions of the Data Protection Agency.

Article 19. *Right to damages*

1. Data subjects who, as a result of failure to comply with the provisions of this Law on the part of the controller or processor, suffer damage to their possessions or rights, shall have the right to damages.
2. Where the files are in public ownership, liability shall be established in accordance with the legislation regulating the liability of public administrations.
3. In the case of files in private ownership, the case shall be heard by the civil courts.

TITLE IV

Sectoral provisions

CHAPTER I

Files in public ownership

Article 20. *Creation, modification or deletion*

1. Files of the public administrations may only be created, modified or deleted by means of a general provision published in the *Boletín Oficial del Estado* or in the corresponding official gazette.

2. The provisions for the creation or modification of files must indicate:

a) The purpose of the file and its planned use.
b) The persons or bodies on which it is planned to obtain personal data or which they are obliged to submit data.
c) The procedure for collecting the personal data.
d) The basic structure of the file and a description of the personal data included in it.
e) The intended transfers of personal data and, where applicable, the intended transfers of data to third countries.
f) The officials in the administrations responsible for the file.
g) The services or units with which the rights of access, rectification, cancellation and objection may be exercised.
h) The security measures, indicating the basic, medium or high level required.

3. The provisions on the deletion of files shall lay down the fate of the files or, where applicable, the timetables to be adopted for their destruction.

Article 21. *Communication of data between public administrations*

1. Personal data collected or drawn up by public administrations in the performance of their tasks shall not be communicated to other public administrations for the exercise of different powers or powers relating to other matters unless the communication is for the purpose of subsequent processing for historical, statistical or scientific purposes.
2. Personal data which a public administration obtains or draws up on behalf of another administration may be communicated.
3. Notwithstanding the provisions of Article 11.2.b), communication of data obtained from sources accessible to the public shall apply to files in private ownership only with the consent of data subject or when a law stipulates otherwise.
4. In the cases provided for in paragraphs 1 and 2 of this Article, the consent of the data subject referred to in Article 11 of this Law shall not be required.

Article 22. *Files of the security forces*

1. The files created by the security forces and containing personal data which, because they were collected for administrative purposes, must be recorded permanently, shall be subject to the general rules of this Law.
2. Collection and processing, for police purposes, of personal data by the security forces without the consent of the data subjects shall be limited to those cases and categories of data necessary for the prevention of a genuine threat to public safety or for the suppression of crime; such data shall be stored in special files established for the purpose, which must be classified according to their degree of reliability.
3. The data referred to in paragraphs 2 and 3 of Article 7 may be collected and processed only in cases in which it is absolutely essential for the purposes of a specific investigation, without prejudice to checks on the legality of the administrative action or the obligation to consider any applications made by the data subjects falling within the remit of the bodies responsible for the administration of justice.
4. Personal data stored for police purposes shall be cancelled when they are not necessary for the investigations for the purposes of which they were stored.

To this end, special consideration shall be given to the age of the data subject and the nature of the data stored, the need to maintain the data until the conclusion of a specific investigation or procedure, a final judgment, and in particular an acquittal, a pardon, rehabilitation and the expiry of liability

Article 23. *Exceptions to the rights of access, rectification and cancellation*

1. The controllers of files containing the data referred to in paragraphs 2, 3 and 4 of the preceding Article may deny access, rectification or cancellation in the light of the risks which might arise for the defence of the state or public safety, the protection of the rights and liberties of third parties, or for the needs of investigations under way.
2. Controllers of files in the public finance sector may also deny exercise of the rights referred to in the previous paragraph when this impede administrative actions aimed at ensuring fulfilment of tax obligations, and particularly when the data subject is under investigation.
3. A data subject who is denied, either wholly or partially, exercise of the rights referred to in the preceding paragraphs may bring this to the notice of the Director of the Data Protection Agency, or of the competent body in each Autonomous Community in the case of files maintained by its own police forces, or the tax authorities of the Autonomous Communities, which must establish the admissibility or inadmissibility of the denial.

Article 24. *Other exceptions to the rights of data subjects*

The provisions of paragraphs 1 and 2 of Article 5 shall not apply to the collection of data when informing the data subject would affect national defence, public safety or the prosecution of criminal offences.

CHAPTER II

Files in private ownership

Article 25. *Creation*

Files in private ownership containing personal data may be created when it is necessary for the success of the legitimate activity and purpose of the person, undertaking or body owning them and the guarantees laid down by this Law for the protection of persons are respected.

Article 26. *Notification and entry in the register*

1. Any person or body creating files of personal data shall first notify the Data Protection Agency,
2. Detailed rules shall be established for the information to be contained in the notification, amongst which must be the name of the controller, the purpose of the file, its location, the type of personal data contained, the security measures, with an indication of whether they are of basic, medium or high level, any transfers intended and, where applicable, ant intended transfers of data to third countries.
3. The Data Protection Agency must be informed of any changes in the purpose of the computer file, the controller and the address of its location.
4. The General Data Protection Register shall enter the file if the notification meets the requirements.
If this is not the case, it may ask for the missing data to be provided or take remedial action.
5. If one month has passed since submitting the application for entry without the Data Protection Agency responding, the computer file shall, for all accounts and purposes, be considered entered in the Register.

Article 27. *Communication of transfers of data*

1. When making the first transfer of data, the controller must communicate this to the data subjects, also indicating the purpose of the file, the nature of the data transferred and the name and address of the transferee.
2. The obligation set out in the preceding paragraph shall not apply in the case provided for in paragraphs 2.c), d) and e) and 6 of Article 11, nor when the transfer is forbidden by law.

Article 28. *Data included in sources accessible to the public*

1. Personal data contained in the publicity register or in the lists of persons belonging to professional associations referred to in Article 3.j) of this Law must be limited to those that are strictly necessary to fulfil the purpose for which each list is intended. The inclusion of additional data by the bodies responsible for maintaining these sources shall require the consent of the data subject, which may be revoked at any time.
2. Data subjects shall have the right to require the body responsible for maintaining the lists of professional associations to indicate, free of charge, that their data may not be used for the purposes of publicity or market research.
Data subjects shall have the right to have all the personal data contained in the publicity register excluded, free of charge, by the bodies entrusted with maintaining those sources.
A reply to the application for exclusion of the unnecessary information or for inclusion of the objection to the use of the data for the purposes of publicity or distance selling must be given within ten days in the case of information provided via telematic consultation or communication, and in the following edition of the list regardless of the medium on which it is published.
3. Publicly accessible sources published in the form of a book or on any other physical support shall cease to be an accessible source when the new edition is published.
If an electronic version of the list is obtained by telematic means, it shall cease to be a publicly accessible source within one year from the moment it was obtained.
4. Data contained in guides to telecommunications services available to the public shall be governed by the relevant legislation.

Article 29. *Provision of information services on creditworthiness and credit*

1. Providers of information services on creditworthiness and credit may process only personal data obtained from registers and sources accessible to the public and set up for that purpose or based on information provided by the data subject or with his consent.
2. Processing is also allowed of personal data relating to the fulfilment or non-fulfilment of financial obligations provided by the creditor or by someone acting on his behalf. In such cases the data subjects shall be informed, within a period of thirty days from the recording, of those who have recorded personal data in files, with a reference to the data included, and they shall be informed of their right to request information on all of them under the conditions laid down by this Law.
3. In the cases referred to in the two paragraphs above, and at the request of the data subject, the data controller shall communicate to him the data, together with any assessments and appreciations made about him during the previous six months and the name and address of the person or body to whom the data have been disclosed.
4. Only those personal data may be recorded and transferred which are necessary for assessing the economic capacity of the data subjects and which, in the case adverse data, do not go back for more than six years, always provided that they give a true picture of the current situation of the data subjects.

Article 30. *Processing for the purpose of publicity and market research*

1. Those involved in compiling addresses, disseminating documents, publicity, distance selling, market research or other similar activities shall use names and addresses or other personal data when they feature in sources accessible to the public or when they have been provided by the data subjects themselves or with their consent.
2. When the data come from sources accessible to the public, in accordance with the provisions of the second paragraph of Article 5.5 of this Law, each communication sent to the data subject shall indicate the origin of the data and the identity of the controller, as well as the rights available to the data subject.
3. In exercising the right of access, data subjects shall have the right to know the origin of their personal data and the rest of the information referred to in Article 15.
4. Data subjects shall have the right to object, upon request and free of charge, to the processing of the data concerning them, in which case they shall be deleted from the processing and, at their mere request, the information about them contained in the processing shall be cancelled.

Article 31. *Publicity register*

1. Those intending to be involved, either permanently or occasionally, in compiling addresses, disseminating documents, publicity, distance selling, market research or other similar activities, may request from the National Statistical Institute or the equivalent bodies in the Autonomous Communities a copy of the publicity register comprising data on the surnames, forenames and domiciles contained in the electoral roll.
2. Each publicity register list shall be valid for one year. Thereafter, the list shall lose its validity as a publicly accessible source.

3. The procedures by which data subjects may request not to be included in the publicity register shall be governed by regulation. Amongst these procedures, which shall be free of charge for the data subjects, shall be the census document. Every quarter, an updated list of the publicity register shall be published, leaving out the names and addresses of those who have asked to be excluded.
4. A consideration may be required for providing the above list on a digital medium.

Article 32. *Standard codes of conduct*

1. By means of sectoral agreements, administrative agreements or company decisions, publicly and privately-owned controllers and the organisations to which they belong may draw up standard codes of conduct laying down the organisation conditions. The operating rules, the applicable procedures, the safety standards for the environment, programs and equipment, the obligations of those involved in the processing and use of personal information, as well as the guarantees, within their remit, for exercising the rights of the individual in full compliance with the principles and provisions of this Law and its implementing rules.
2. These codes may or may not contain detailed operational rules for each particular system and technical standards for their application.
If these codes are not incorporated directly into the code, the instructions or orders for drawing them up must comply with the principles laid down in the code.
3. The codes must be in the form of codes of conduct or of good professional practice, and must be deposited or entered in the General Data Protection Register and, where appropriate, in the registers set up for this purpose by the Autonomous Communities, in accordance with Article 41. The General Data Protection Register may refuse entry when it considers that the code does not comply with the legal and regulatory provisions on the subject. In such a case, the Director of the Data Protection Agency must require the applicants to make the necessary changes.

TITLE V

International movement of data

Article 33. *General rule*

1. There may be no temporary or permanent transfers of personal data which have been processed or which were collected for the purpose of such processing to countries which do not provide a level of protection comparable to that provided by this Law, except where, in addition to complying with this Law, prior authorisation is obtained from the Director of the Data Protection Agency, who may grant it only if adequate guarantees are obtained.
2. The adequacy of the level of protection afforded by the country of destination shall be assessed by the Data Protection Agency in the light of all the circumstances surrounding the data transfer or category of data transfer. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question, the content of the reports by the Commission of the European Union, and the professional rules and security measures in force in those countries.

Article 34. *Derogations*

The provisions of the preceding paragraph shall not apply where:

a) The international transfer of personal data is the result of applying treaties or agreements to which Spain is a party.
b) The transfer serves the purposes of offering or requesting international judicial aid.
c) The transfer is necessary for medical prevention or diagnosis, the provision of health aid or medical treatment, or the management of health services.
d) Where the transfer of data is related to money transfers in accordance with the relevant legislation.
e) The data subject has given his unambiguous consent to the proposed transfer.
f) The transfer is necessary for the performance of a contract between the data subject and the controller or the adoption of precontractual measures taken at the data subject's request.
g) The transfer is necessary for the conclusion or performance of a contract concluded, or to be concluded, in the interest of the data subject, between the controller and a third party.
h) The transfer is necessary or legally required to safeguard a public interest. A transfer requested by a tax or customs authority for the performance of its task shall be considered as meeting this condition.
i) The transfer is necessary for the recognition, exercise or defence of a right in legal proceedings.
j) The transfer takes place at the request of a person with a legitimate interest, from a public register, and the request complies with the purpose of the register.
k) The transfer takes place to a Member State of the European Union or to a country which the Commission of the European Communities, in the exercise of its powers, has declared to ensure an adequate level of protection.

TITLE VI

Data Protection Agency

Article 35. *Nature and legal status*

1. The Data Protection Agency is a body under public law, with its own legal personality and unlimited public and private legal capacity, which acts fully independently of the public administrations in the performance of its tasks. It shall be governed by the provisions of this Law and in a Statute of its own to be approved by the Government.
2. In the exercise of its public functions, and until such time as this Law and its implementing provisions are adopted, the Data Protection Agency shall act in conformity with Law 301992 of 26 November on the Legal Status of Public Administrations and the Common Administrative Procedure. Its acquisitions of assets and contracts shall be governed by private law.
3. The posts in the bodies and services belonging to the Data Protection Agency shall be filled by officials of the public administrations and by staff recruited to this end, in accordance with the functions assigned to each post. The staff is obliged to keep secret any personal data of which they acquire knowledge in the performance of their task.
4. For the performance of its tasks, the Data Protection Agency shall have the following assets and resources:

a) The annual appropriations from the General Government Budget.

b) The goods and assets making up its resources, and any interest from them.
c) Any other resources legally assigned to it.

5. Each year the Data Protection Agency shall draw up and approve the corresponding preliminary draft budget and send it to the Government for incorporation, with due regard to its independence, into the General Government Budget.

Article 36. *The Director*

1. The Director of the Data Protection Agency manages and represents the Agency. He shall be appointed from amongst the members of the Consultative Council, by Royal Decree, for a period of four years.
2. He shall exercise his functions fully independently and objectively and shall not be subject to any instructions thereby.
The Director shall in all cases take note of any proposals the Consultative Council may make to him in the exercise of its functions.
3. The Director of the Data Protection Agency may be removed from office before the end of the period set out in paragraph 1 only at his own request or on the instructions of the Government, after an investigation in which the other members of the Consultative Council must be consulted, for serious infringement of his obligations, inability to exercise his functions, incompatibility or conviction for a criminal offence.
4. The Director of the Data Protection Agency shall be considered as occupying a senior post and shall be governed by the special services régime if he was previously exercising a pubic function. If a member of the judicial or tax career bracket is appointed to the post, he shall also be governed by the special services administrative régime.

Article 37. *Functions*

The functions of the Data Protection Agency are as follows:

a) To ensure compliance with the legislation on data protection and ensure its application, in particular as regards the rights of information, access, rectification, objection and cancellation of data.
b) To issue the authorisations provided for in the Law or in its regulatory provisions.
c) To issue, where applicable, and without prejudice to the remits of other bodies, the instructions needed to bring processing operations into line with the principles of this Law.
d) To consider the applications and complaints from the data subjects.
e) To provide information to persons on their rights as regards the processing of personal data.
f) To require controllers and processors, after having heard them, to take the measures necessary to bring the processing operations into line with this Law and, where applicable, to order the cessation of the processing operation when the cancellation of the files, when the operation does not comply with the provisions of the Law.
g) To impose the penalties set out in Title VII of this Law.
h) To provide regular information on the draft general provisions set out in this Law.
i) To obtain from the data controllers any assistance and information it deems necessary for the exercise of its functions.
j) To make known the existence of files of personal data, to which end it shall regularly publish a list of such files with any additional information the Director of the Agency deems necessary.

k) To draw up an annual report and submit it to the Ministry of Justice.
l) To monitor and adopt authorisations for international movements of data, and to exercise the functions involved in international cooperation on the protection of personal data.
m) To ensure compliance with the provisions laid down by the Law on Public Statistics with regard to the collection of statistical data and statistical secrecy, to issue precise instructions, to give opinions on the security conditions of the files set up for purely statistical purposes, and to exercise the powers referred to in Article 46.
n) Any other functions assigned to it by law or regulation.

Article 38. *Consultative Council*

The Director of the Data Protection Agency shall be assisted by a Consultative Council made up of the following members:

One member of the Congress of Deputies, proposed by the Congress.
One member of the Senate, proposed by the Senate.
One member of the central administration, proposed by the Government.
One member of the local administration, proposed by the Spanish Federation of Municipalities and Provinces.
One member of the Royal Academy of History, proposed by the Academy.
One expert in the field, proposed by the Supreme Council of Universities.
A representative of users and consumers, to be selected according to a method to be laid down by regulation.
One representative of each Autonomous Community which has set up a data protection agency on its territory, to be proposed in accordance with the procedure laid down by the Autonomous Community concerned.
One representative of the private file sector, to be proposed according to the procedure laid down by regulation.

The Consultative Council shall operate in accordance with the regulations laid down for that purpose.

Article 39. *The General Data Protection Register*

1. The General Data Protection Register is a body incorporated into the Data Protection Agency.
2. The following shall be entered in the General Data Protection Register:

a) Files owned by the public administrations.
b) Files in private ownership.
c) The authorisations referred to in this Law.
d) The codes of conduct referred to in Article 32 of this Law.
e) Data relating to files which are necessary for the exercise of the rights of information, access, rectification, cancellation and objection.

3. The procedures for entering the files in public and private ownership in the General Data Protection Register, the content of the entry, its modification, cancellation, complaints and

appeals against the corresponding decisions, and other related matters, shall be laid down by regulation.

Article 40. *Powers of inspection*

1. The supervisory authorities may inspect the files referred to in this Law and obtain any information they require for the performance of their tasks.
To this end, they may require the disclosure or transmission of documents and data and examine them at their place of storage, inspect the hardware and software used to process the data, and obtain access to the premises on which they are located.
2. In the performance of their tasks, the officials carrying out the inspection referred to in the preceding paragraph shall be deemed to be a public authority.
They shall be obliged to keep secret any information acquired in the exercise of the aforementioned functions, even after they have ceased to exercise them.

Article 41. *Corresponding bodies of the Autonomous Communities*

1. The functions of the Data Protection Agency set out in Article 37, with the exception of those referred to in paragraphs j), k) and l), and in paragraphs f) and g) as regards international transfers of data, as well as in Articles 46 and 49 relating to its specific powers, shall, when they concern files of personal data created and administered by the Autonomous Communities and by local government within its territory, be exercised by the corresponding bodies in each Community, which shall be deemed to be supervisory authorities guaranteed full independence and objectivity in the performance of their task.
2. The Autonomous Communities may create and maintain their own registers of files for the exercise of the powers assigned to them.
3. The Director of the Data Protection Agency may regularly meet the corresponding bodies in the Autonomous Communities for the purposes of institutional cooperation and coordination of the criteria or operating procedures. The Director of the Data Protection Agency and the corresponding bodies in the Autonomous Communities may ask each other for the information needed for the exercise of their functions.

Article 42. *Files of the Autonomous Communities for which the Agency has sole responsibility*

1. When the Director of the Data Protection Agency establishes that the maintenance or use of a particular file of the Autonomous Communities contravenes any provision of this Law for which it has sole responsibility, he may require the corresponding administration to adopt the corrective measures specified by him within the period laid down by him.
2. If the public administration in question does not comply with the requirement, the Director of the Data Protection Agency may challenge the decision taken by that administration.

TITLE VII

Infringements and penalties

Article 43. *Controllers*

1. Controllers and processors shall be subject to the penalties set out in this Law.
2. In the case of files for which the public administrations are responsible, the provisions of Article 46(2) shall apply to the procedure and penalties.

Article 44. *Types of infringement*

1. Infringements shall be classified as minor, serious and very serious.
2. The following shall be minor infringements:

a) Failure to respond, for formal reasons, to a request by a data subject for the rectification or cancellation of personal data subject to processing, when that request is justified in law.
b) Failure to provide the information requested by the Data Protection Agency in the exercise of the functions assigned to it by law, with regard to non-substantive aspects of data protection.
c) Failure to request the entry of the file of personal data in the General Data Protection Register, where this does not amount to a serious infringement.
d) Collection of personal data on data subjects without providing them with the information set out in Article 5 of this Law.
e) Failure to respect the duty of secrecy set out in Article 10 of this Law, where this does amount to a serious infringement.

3. The following shall be serious infringements:

a) Creating files in public ownership, or initiating the collection of personal data for such files, without the authorisation published in the *Boletín Oficial del Estado* or the corresponding official gazette.
b) Creating files in private ownership, or initiating the collection of data for such files, for purposes other than the legitimate purposes of the undertaking or body.
c) Collecting personal data without obtaining the explicit consent of the data subjects, where this has to be obtained.
d) Processing personal data or subsequently using them in infringement of the principles and guarantees laid down in this Law, and failure to respect the protection laid down by the implementing provisions, where this does not amount to a very serious infringement.
e) Preventing or hindering the exercise of the rights of access and objection, and refusing to provide the information asked for.
f) Maintaining incorrect personal data or failure to rectify or cancel such data when legally obliged if the citizens' rights protected by this Law are affected
g) Breach of the duty of secrecy for personal data incorporated into files containing data on the commission of administrative or criminal offences, public finance, financial services, provision of creditworthiness and credit services, as well as other files containing a set of personal data sufficient to obtain an assessment of the personality of the individual.
h) Maintaining files, premises, programs or hardware containing personal data without the security required by regulations.
i) Failure to send the Data Protection Agency the notifications laid down in this Law or in its implementing provisions, and not providing it, on time, with any documents and information due to it or which it may require to that end.
j) Impeding inspections.
k) Failure to enter a file of personal data in the General Data Protection Register when this has been required by the Director of the Data Protection Agency.

l) Failure to comply with the duty of information laid down in Articles 5, 28 and 29 of this Law, when the data have been obtained from a person other than the data subject.

4. The following shall be very serious infringements:

a) The misleading or fraudulent collection of data.
b) Communication or transfer of personal data other than in cases where these are allowed.
c) Obtaining and processing the personal data referred to in paragraph 2 of Article 7 without the explicit consent of the data subject; obtaining and processing the data referred to in paragraph 3 of Article 7 when not covered by a law or when the data subject has not given his explicit consent, or breaching the prohibition contained in paragraph 4 of Article 7.
d) Failure to cease the illegitimate use of personal data processing operations when required to do so by the Director of the Data Protection Agency or by the persons owning the rights of access.
e) The temporary or final transfer of personal data which have been subjected to processing, or which have been collected for such processing, to countries which do not provide a comparable level of protection, without the authorisation of the Director of the Data Protection Agency.
f) Processing personal data illegally or in breach of the principles and guarantees applying to them, when this prevents or infringes the exercise of fundamental rights.
g) Breach of the duty to maintain the secrecy of the personal data referred to in paragraphs 2 and 3 of Article 7, as well as of data obtained for police purposes without the consent of the data subjects.
h) Systematically impeding or failing to comply with the exercise of the rights of access, rectification, cancellation or objection.
i) Systematic failure to comply with the duty to notify the inclusion of personal data in a file.

Article 45. *Penalties*

1. Minor infringements shall be punished by a fine of Ptas 100 000 to 10 000 000.
2. Serious infringements shall be punished by a fine of Ptas 10 000 000 to 50 000 000.
3. Very serious infringements shall be punished by a fine of Ptas 50 000 000 to 100 000 000.
4. The amount of the penalties shall be graded taking account the nature of the personal rights involved, the volume of the processing operations carried out, the profits gained, the degree of intentionality, repetition, the damage caused to the data subjects and to third parties, and any other considerations of relevance in determining the degree of illegality and culpability of the specific infringement.
5. If, in the light of the circumstances, there is a qualified diminution of the culpability of the offender or of the illegality of the action, the body applying the penalties shall determine the amount of the penalty by applying the scale for the category of penalties immediately below that for the actual case in question.
6. In no case shall a penalty be imposed which is higher than that laid down in the Law for the category covering the infringement to be punished.
7. The Government shall regularly update the amount of the penalties in accordance with changes in the price indices.

Article 46. *Infringements by public administrations*

1. When the infringements referred to in Article 44 are committed in files for which the public administrations are responsible, the Director of the Data Protection Agency shall issue a decision setting out the measures to be adopted to terminate or correct the effects of the infringement. This decision shall be notified to the data controller, the body to which he is responsible, and to the data subjects, if any.
2. The Director of the Agency may also propose that disciplinary proceedings be initiated. The procedure and penalties to be applied shall be those laid down in the legislation on disciplinary proceedings in public administrations.
3. Decisions on the measures and proceedings referred to in the preceding paragraphs shall be communicated to the Agency.
4. The Director of the Agency shall communicate to the Ombudsman the proceedings and decisions taken within the terms of the preceding paragraphs.

Article 47. *Time limits*

1. The time limits for pursuing infringements shall be three years for very serious infringements, two years for serious infringements and one year for minor infringements.
2. The time limits shall start to run on the day on which the infringement was committed,
3. The time limits shall be interrupted when the person concerned is informed of the initiation of the infringement procedure, and the time limit shall recommence if the procedure is held up for more than six months for reasons for which the alleged offender cannot be held responsible.
4. Penalties imposed for very serious infringements shall expire after three years, those imposed for serious infringements after two years, and those imposed for minor infringements after one year.
5. The time limits for penalties shall start to run from the day after the decision imposing the penalty comes into force.
6. The time limits shall be interrupted when the person concerned is informed of the initiation of the execution procedure, and shall recommence if the procedure is held up for more than six months for reasons for which the offender cannot be held responsible.

Article 48. *Penalty procedure*

1. The procedure for determining infringements and imposing the penalties referred to in this Title shall be laid down by regulation.
2. The decisions of the Data Protection Agency or the corresponding body in the Autonomous Community shall exhaust the administrative procedure.

Article 49. *Power to immobilise files*

In cases of very serious infringement, involving the use or illicit transfer of personal data in which the exercise of the rights of citizens and the free development of the personality guaranteed by the Constitution and the laws are seriously impeded or otherwise affected, the Director of the Data Protection Agency may, in addition to imposing a penalty, require the controllers of files personal data in both public and private ownership to terminate the use or illicit transfer of the data. If there is no response to this requirement, the Data Protection Agency may, on the basis of a reasoned decision, immobilise such files for the sole purpose of restoring the rights of the data subjects.

First additional provision. *Existing files*

Files and computer processing operations, whether or not entered in the General Data Protection Register, must comply with this Organic Law within three years of its entry into force. Within this period, files in private ownership must be communicated to the Data Protection Agency, and the public administrations responsible for files in public ownership must approve the relevant provision regulating the files or adapt the existing provision.
In the case of files and data processing operations which are not computerised, compliance with this Organic Law and the obligation in the preceding paragraph must be achieved within twelve years from 24 October 1995, without prejudice to the exercise of the rights of access, rectification and cancellation by the data subjects.

Second additional provision. *Population files and registers of public administrations*

1. Central Government and the administrations of the Autonomous Communities may request from the National Statistical Institute, without the consent of the data subject, an updated copy of the file comprising data on the surname, forenames, domicile, sex and date of birth contained in the municipal censuses of inhabitants and the electoral roll for the territories in which they exercise their powers, for the creation of population files or registers.
2. The purpose of the population files or registers shall be communication between the various bodies in each public administration and data subjects resident in the respective territories, in relation to the legal and administrative relations deriving from the respective remits of the public administrations.

Third additional provision. *Processing of files from the repealed Laws on Vagrants and Malefactors and on Riskiness and Social Rehabilitation*

The files specifically established under the repealed Laws on Vagrants and Malefactors and on Riskiness and Social Rehabilitation, and containing data of whatever sort which might affect the security, reputation, privacy or image of individuals, may not be consulted without the explicit consent of the data subjects or unless fifty years have passed since their date of collection.
In the latter case, the Central Government shall, unless there is proof of the death of the data subjects, make the documentation available to requesters after deleting from it the data referred to in the preceding paragraph using the technical procedures appropriate to each case.

Fourth additional provision. *Amendment to Article 112.4 of the General Law on Taxation*

> "4. The processed personal data which must be transferred to the tax authorities in accordance with the provisions of Article 111, of the preceding paragraphs of this Article, or of other rules of equal standing, shall not require the consent of the data subject. The provisions of paragraph 1 of Article 21 of the Organic Law on Personal Data relating to public administrations shall also not apply to such matters."

Fifth additional provision. *Remit of the Ombudsman and similar regional government bodies*

The provisions of this Organic Law are without prejudice to the remit of the Ombudsman and the similar bodies in the Autonomous Communities.

Sixth additional provision. *Amendment to Article 24.3 on the Law on the Regulation and Supervision of Private Insurances*

Article 24.3, second paragraph, of Law 30/1995 of 8 November, on the Regulation and Supervision of Private Insurances, is amended as follows:

> "Insurance bodies may create joint files containing personal data for the settlement of accident claims and for actuarial statistical collaboration aimed at establishing rates of premiums and the selection of risks, and for drawing up studies on insurance techniques. The transfer of data to such files shall not require the prior consent of the data subject, but the possible transfer of his personal data for the purposes indicated must be communicated to the data subject, together with an explicit indication of the data controller, so that the rights of access, rectification and cancellation laid down by law may be exercised.
> Joint files may also be created without the consent of the data subject for the purpose of preventing insurance fraud. However, it will be necessary in such cases to make known to the data subject, when the data are first introduced, who is responsible for the file and the ways in which the rights of access, rectification and cancellation may be exercised.
> In all cases, data relating to health may be subjected to processing only with the explicit consent of the data subject."

First transitional provision. *Processing operations under international agreements*

The Data Protection Agency shall be the body responsible for the protection of natural persons as regards the processing of personal data, with respect to the processing operations set up under any international agreement to which Spain is a signatory and which assigns this power to a national supervisory authority, unless a different authority is set up for this task in implementation of the agreement.

Second transitional provision. *Use of the publicity register*

The procedures for drawing up the publicity register, for objecting to being entered in it, for making it available to requesters, and for monitoring the lists disseminated, shall be governed by regulation. The regulation shall lay down the time limits for implementation of the publicity register.

Third transitional provision. *Continuation in force of existing rules*

Until such time as the arrangements set out in first final provision of this Law come into force, the existing regulatory rules shall continue in force with their own ranking, and in particular Royal Decrees 428/1993 of 26 March, 1332/1994 of 20 June, and 994/1999 of 11 June, unless they are in conflict with this Law.

Single repealing provision. *Repeal of rules*

Organic Law 5/1992 of 29 October regulating the computer processing of personal data is hereby repealed.

First final provision. *Authorisation for regulatory development*

The Government shall approve or amend the regulatory provisions necessary for the application and further development of this Law.

Second final provision. *Precepts with the character of ordinary law*

Titles IV, VI - except for the last indent of paragraph 4 of Article 36 - and VII of this Law, the fourth additional provision, the first transitional provision, and the first final provision, shall have the character of ordinary law.

Third final provision. *Entry into force*

This Law shall enter into force one month after its publication in the *Boletín Oficial del Estado*.

Therefore
I order all Spaniards, individuals and authorities, to uphold this Organic Law and to ensure that it is upheld.

Madrid, 13 December 1999.

JUAN CARLOS R.

The Prime Minister
JOSÉ MARÍA AZNAR LÓPEZ

DATA PROTECTION AGREEMENT for "RELAXED CARE"

between the Parties of the Consortium Agreement "Relaxed Care" as listed in the signature pages.

The Parties have foreseen in the Ethical Manual of the funded AAL Project Relaxed Care to safeguard the personal data of participant through a separate agreement also to fulfill the obligations according to several data protection legislations since all data and information collected within the RelaxedCare project must be handled in accordance with the respective national data protection regulations of Austria, Sweden and Switzerland. In addition to these national data protection regulations, directive 95/46/EC of the European Parliament (Ref.3: Directive 95/46/EC) applies in its latest version. Therefore the Parties of Relaxed Care agree:

1. Definition

1.1. **Data** shall refer to personal data and shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

1.2. **Agreement** shall refer to this Data Protection Agreement.

1.3. **Consortium Agreement** shall refer to the Consortium Agreement "Relaxed Care" signed by the Coordinator on the 4th of April 2013.

1.4. **Controller** shall mean the Party transferring Data for the implementation of the Project.

1.5. **Coordinator** shall mean the AIT Austrian Institute of Technology GmbH.

1.6. **Party or Parties** shall mean all or one Party of the Consortium Agreement.

1.7. **Processor** shall be the Party receiving and using the Data in the Project.

1.8. **Project** shall refer to the Project "Relaxed Care" as described in the Annexes of the Consortium Agreement

2. Object of the Agreement

The Parties will divulge and receive Data for the implementation of the Project. To observe the Data protection regulations to which the Parties are subject to, the Parties agree on the following stipulation which is to be seen as completing the Consortium Agreement with regards to DATA and not substituting any regulations therein.

3. Obligation of the Processor

3.1. The Controller warrants that the processing, including the transfer itself, of the Data has been and, up to the moment of transfer, will continue to be carried out in accordance with the relevant

provisions of the applicable data protection legislation in which the Controller is established and does not violate the relevant provisions of that legislation. The Controller further warrants that he is able to respond in a reasonable time and to the extent reasonably possible to enquires for the applicable supervision authority on the procession of Data and to enquiries form the Data subjects concerning the processing of his personal Data by the Controller.

3.2. The Processor shall implement the appropriate technical and organizational measures to protect Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, abuse, and against all other unlawful forms of processing.

3.3. Should special measures be needed for certain data the Controller shall inform the Processor at the latest with the transfer of the Data.

3.4. The Processor warrants that he is able to respond in a reasonable time and to the extent reasonably possible to enquire for the applicable supervision authority on the procession of Data and to enquiries form the Data subjects concerning the processing of his personal Data by the Controller.

3.5. The processor is required to make sure data is erased locally at the time the processing ends after agreement with the controller and only after the controller confirms. The processor and the controller must agree on an acceptable data erasure method. If requested the processor must send a written statement, stating that data has been erased, including used erasure method and shall delete any and all data immediately after information of the Controller.

3.6. The Processor shall at the controller's request provide the controller with sufficient information for the Controller to be able to ensure the processor's compliance with the mentioned technical and organizational measures.

3.7. It is the Processors duty to make sure that the demanded security measures are in place and kept. By mutual agreement this can be accomplished by security audits or documentation of policy and procedures

3.8. Processing of personal data may not take place in ad hoc places of work (working places at home). If processing of confidential and sensitive personal data, as a rare exception must take place in ad hoc places of work (working places at home) the Processor must comply with the applicable legal demands regarding protection of personal data among these ensuring that the protection of the personal data is sufficient as an example by way of intense coding or digital signature.

3.9. The Controller must be informed, if the Processor uses a subcontractor. It is the responsibility of the Processor to make sure the subcontractor follows the Controllers rules of safe storage and handling of data. In the event the Processor decides to switch subcontractor or enter into a contract with a subcontractor, Controller must be notified no later than one month prior to the change.

3.10. All data processing and handling are under the jurisdiction of the law applicable to this Data in the place it is being processed, meaning until the transfer under the laws of the Controller and after transfer the laws of the Processor. In case of conflict the rules and regulation of the applicable protection act will be enforced by the Controller.

4. Duration and Termination of the Agreement

This Agreement shall enter into force with the signature of the Coordinator and shall end 3 years after the end of the Project.

5. Miscellaneous

5.1. This document comprises any and all agreements entered into by and between the Parties with regards to Data. Except for the Consortium Agreement with regards to confidentiality and intellectual property regulations in regards to Data there are no written or oral ancillary agreements. Modifications of or amendments to this Agreement shall only be valid, including modifications of or amendments to this provision, if implemented by written agreement duly signed by all Parties.

5.2. Any disputes arising out of this Agreement shall be decided by the same Courts as the Consortium Agreement.

5.3. Should any provisions of this agreement be or become wholly or partly invalid or unenforceable, this shall not affect the validity or enforceability of the remaining provisions. In this event, the invalid or unenforceable provision shall be substituted by such valid/enforceable provision, which comes as close as possible to the legal and economic purposes pursued by the Parties with such invalid/unenforceable provision.

5.4. This agreement shall be governed in its entirety by the Belgium laws. This includes disputes on its conclusion, binding effect, amendment and legal consequences of this agreement.

SIGNATURES

1. Authorised to sign on behalf of

AIT Austrian Institute of Technology GmbH

Signature

2. Authorised to sign on behalf of

Hochschule Luzern Technik & Architektur, CEESAR – iHomeLab

Signature

Name	Title
Alexander Klapproth	Professor

3. Authorised to sign on behalf of

50plus GmbH

Signature

Name Title

4. Authorised to sign on behalf of

New Design University

Signature

Name	Title
Sandra Dittenberger	Professor

5. Authorised to sign on behalf of

Mobili

Signature

Name Title

6. Authorised to sign on behalf of

Eichenberger-Szenographie

Signature

Name Title
Ralph Eichenberger

7. Authorised to sign on behalf of

Ibernex

Signature

Name Title

8. Authorised to sign on behalf of

Soultank AG

Signature

Name	Title
Marcel B.F. Uhr	Dr. sc. techn. ETH

9. Authorised to sign on behalf of

Schweizerisches Rote Kreuz Luzern

Signature

Name	Title
Erica Züst	Chairwoman SRK Luzern