235.1

National Law Gazette of The Principality of Liechtenstein

2018 No. 272 issued on December 7, 2018

Data Protection Act

of October 4, 2018

I herewith consent to the following resolution passed by the Landtag of the Principality of Liechtenstein:

I. General Regulations

A. Purpose, Scope and Terminology

Article 1

Purpose

- 1) This Act aims at the protection of personality rights and the fundamental freedoms of natural persons when processing their personal data.
- 2) It also aims at:
- a) the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (ABI. L 119, dated 4 May 2016, page 1);
- b) the implementation of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (ABI L. 119, dated 4 May 2016, page 89).

3) The version of the legislation in force as set out in paragraph 2 results from the publication of the resolutions of the EEA Joint Committee as well as the treaties regarding the development of the Schengen acquis as published in the National Law Gazette of the Principality of Liechtenstein ("Liechtensteinisches Landesgesetzblatt") pursuant to Article 3 lett. c and k of the Act on the publication of national legislation ("Kundmachungsgesetz").

Article 2

Scope

- 1) This Act shall apply to the processing of personal data by public bodies. For non-public bodies, this Act shall apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system with the exception of processing personal data by a natural person in the course of a purely personal or domestic activity.
- 2) Special legal provisions regarding data protection take precedence over the provisions set out in this Act. If such legislation does not regulate or not conclusively regulate a matter, the provisions set out in this Act shall apply in a subsidiary manner. The obligation to maintain professional or official secrecy remains unaffected.
- 3) This Act shall apply to public bodies. It shall apply to non-public bodies if:
- a) the controller or processor is processing data in Liechtenstein;
- b) the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in Liechtenstein; or
- c) the controller or processor does not have an establishment in the EEA but falls within the scope of Regulation (EU) 2016/679.

Provided that this Act is not applicable pursuant to sentence 2, only Articles 9 to 20 and 39 to 44 shall apply to the controller or processor.

- 4) For the processing of personal data by public bodies which do not fall within the scope of activities as set out in Regulation (EU) 2016/679 and Directive (EU) 2016/680, Regulation (EU) 2016/679 and Chapter I and II of this Act shall apply if not regulated otherwise in this Act or any other legal provision.
- 5) This Act shall not apply to:
- a) debates held in Parliament and its Commissions as well as the Judge Appointment Board;
- b) pending civil proceedings and administrative procedures;
- c) proceedings pending before the Constitutional Court;
- d) activities of the Financial Audit Office.

6) This Act shall not apply where the law of the European Economic Area, in particular Regulation (EU) 2016/679, directly applies.

Article 3

Definitions

- 1) For the purpose of this Act:
- a) "public bodies" means:
- 1. organs of the state, municipalities, corporations, foundations and public-law institutions;
- 2. non-public bodies as far as they carry out tasks in the public interest conferred upon them;
- b) "non-public bodies" means:
- 1. natural and legal persons, societies and other associations established under private law unless they are covered by lett. a (2).
- 2. Public bodies pursuant to lett. a (1) if they operate commercially.
- 2) The terms used in this Act to refer to persons and functions are understood as applying to both male and female.

B. Legal basis for processing personal data

Article 4

Processing of personal data by public bodies

The processing of personal data by public bodies is lawful if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 5

Video surveillance of publicly accessible areas

- 1) The surveillance of publicly accessible areas with optical-electronic-equipment (video surveillance) shall be permitted only
- a) as far as it is necessary:
- 1. for public bodies to perform their tasks;
- 2. to exercise the right to determine who shall be allowed or denied access or

- 3. to safeguard legitimate interests for specifically defined purposes; and
- b) if there is nothing to indicate legitimate overriding interests of the data subjects.
- 2) The protection of life, health or freedom is considered a particularly important interest of persons present in the following areas, locations or facilities:
- a) large publicly accessible facilities, such as sport facilities, places of gathering and entertainment, shopping centers and car parks; or
- b) vehicles and large publicly accessible facilities of public transport.
- 3) The operation of a video surveillance system as well as the name and contact details of the controller shall be made known as early as possible by appropriate measures.
- 4) The storage or use of data collected according to paragraphs 1 and 2 shall be permitted if it is necessary to achieve the purposes for which such data has been collected and there is no indication of legitimate overriding interests of the data subjects. Paragraph 2 shall apply accordingly. For any other purpose, they may only be further processed to the extent necessary to avert threats to state or public security, to avert serious danger to life, limb, freedom or property, or to prosecute criminal offenses or to safeguard evidence; in the latter cases the National Police can demand the transfer of any data collected.
- 5) If data collected through video surveillance are attributed to a particular person, that person shall be informed of the processing according to Articles 13 and 14 of Regulation (EU) 2016/679. Article 32 shall apply accordingly.
- 6) The data shall be deleted immediately if they are no longer needed for the intended purpose or if the data subject's legitimate interests stand in the way of any further storage.
- 7) The use of video surveillance shall be notified to the Data Protection Authority prior to its implementation. Live video streaming without the possibility of recording or further processing are not subject to prior notification. The Government regulates further details in an ordinance.
- 8) Any person who intentionally violates the notification obligation according to paragraph 7 will be fined by the Data Protection Authority up to 5'000 Swiss Francs. Article 40 (3) to (6) shall apply accordingly.

C. Data Protection Officers of public bodies

Article 6

Designation

- 1) Public bodies shall designate a data protection officer. This shall apply likewise to public bodies as defined in Article 3 paragraph 1 lett. b no. 2.
- 2) A single data protection officer may be designated for several public bodies, taking into account their organizational structure and size.

- 3) The data protection officer shall be designated on the basis of his or her professional qualifications and, in particular, expert knowledge of data protection law and practice and the ability to fulfill the tasks referred to in Article 8.
- 4) The data protection officer may be an employee of the public body or act on the basis of a service agreement.
- 5) The public body shall publish the contact details of the data protection officer and also notify these details to the Data Protection Authority.

Article 7

Position

- 1) The public body shall ensure that the data protection officer is properly and in a timely manner involved in all matters concerning the protection of personal data.
- 2) The public body shall support the data protection officer in the fulfillment of his or her tasks as set out in Article 8 by providing the required resources as well as access to personal data and processing operations and by providing the resources required to maintain his or her expert knowledge.
- 3) The public body shall ensure that the data protection officer does not receive instructions on how to fulfill his or her tasks. The data protection officer reports directly to the head of the respective public body. The data protection officer shall not be dismissed or disadvantaged by the public body for performing his or her tasks.
- 4) The dismissal of the data protection officer is subject to Article 24 of the Civil Servants Act.
- 5) Data subjects may seek advice from the data protection officer regarding any questions related to the processing of their personal data and the exercise of their rights pursuant to Regulation (EU) 2016/679, this Act as well as other laws regarding data protection. The data protection officer is bound by law to maintain confidentiality about the identity of the data subject as well as all circumstances enabling data subjects to be identified, unless he or she is released from this obligation by the data subject.
- 6) If the data protection officer gains knowledge about data for which the head of a public body or any person employed by this body has the right to refuse to give evidence for employment-related reasons, this right shall also apply to the data protection officer and his or her staff members. The person to whom the right to refuse to give evidence applies for employment-related reasons shall decide whether to exercise this right unless it is impossible to effect such a decision in the foreseeable future. Where the right of the data protection officer to refuse to give evidence applies, his or her files and other documents shall not be subject to seizure.

Article 8

Tasks

1) In addition to the tasks set out in Regulation (EU) 2016/679, the data protection officer is responsible

for the following tasks:

- a) Informing and advising the public body and the employees who carry out processing of their obligations pursuant to this Act and other regulations regarding data protection including all laws and regulations implementing Regulation (EU) 2016/680;
- b) Monitoring of compliance with this Act as well as other regulations regarding data protection as well as all laws and regulations implementing Regulation (EU) 2016/680 as well as policies of the public body regarding the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- c) Providing advice as regards the data protection impact assessment and monitoring of its performance pursuant to Article 66;
- d) Cooperating with the Data Protection Authority;
- e) Acting as the contact point for the Data Protection Authority on issues relating to data processing, including the prior consultation referred to in Article 68, and consulting, where appropriate, with regard to any other matter.
- 2) In the case of a data protection officer designated by a court, the tasks set out in paragraph 1 shall not refer to the action of the court acting in its judicial capacity.
- 3) Data protection officers may be assigned other duties and tasks. The official body shall ensure that such duties and tasks do not result in a conflict of interest.
- 4) The data protection officer shall in the performance of his or her tasks give due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

D. Data Protection Authority

Article 9

Position and organization

- 1) The Data Protection Authority is the national supervisory authority pursuant to Article 51 of Regulation (EU) 2016/679 and Article 41 of Directive (EU) 2016/680.
- 2) The Data Protection Authority consists of the Head of the Data Protection Authority and other staff members.
- 3) Unless expressly stated otherwise in Regulation (EU) 2016/679 or this Act, the employment of the Head of the Data Protection Authority and the other staff is subject to the Civil Servants Act.

Article 10

Competences

- 1) The Data Protection Authority shall be responsible for the supervision of the processing of data by public and non-public bodies.
- 2) The Data Protection Authority shall not be responsible for the supervision of:
- a) data processing by the government within the context of their activity;
- b) data processing by courts when acting in their judicial capacity.

Article 11

Independence

- 1) The Data Protection Authority shall be completely independent when performing their tasks and exercising their powers. It shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
- 2) The Data Protection Authority is subject to financial audit by the Financial Audit Office according to the Public Audit Act.

Appointment and termination of employment

Article 12

a) Head of the Data Protection Authority

- 1) The Parliament appoints the Head of the Data Protection Authority on a proposal from the government for a term of six years. The Head of the Data Protection Authority can be re-elected.
- 2) If the employment contract of the Head of the Data Protection Authority ends with the expiration of the contract, the government may extend the employment period of the Head of the Data Protection Authority up to six months until an appropriate substitute is employed.
- 3) The employment of the Head of the Data Protection Authority ends with the expiration of the contract; subject to paragraph 4.
- 4) The employment of the Head of the Data Protection Authority can only be terminated by the government in the following cases:
- a) incapacity for work or to fulfill his or her duties caused by illness or accident; or
- b) compelling reasons for a termination without notice.

Article 13

b) Other personnel of the Data Protection Authority

- 1) All other personnel of the Data Protection Authority are employed by the government on a proposal from the Head of the Data Protection Authority.
- 2) Terms and regulations regarding the reassignment of employees or the termination of employment pursuant to Articles 16 and 18-27 of the Civil Servants Act are applicable to all the other personnel of the Data Protection Authority under the condition that the Head of the Data Protection Authority submits an according request with the government.

Article 14

Rights and duties

- 1) The Head of the Data Protection Authority shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any incompatible occupation, whether gainful or not. The Head of the Data Protection Authority shall not be a Member of Parliament, government, court or another administrative authority or exercise the role of a mayor or a municipal council member of a Liechtenstein municipality. He or she shall resign from such offices at the time of his or her appointment. He or she shall not deliver extra-judicial opinions in exchange for payment.
- 2) The Head of the Data Protection Authority is authorised to refuse to give evidence regarding persons that have entrusted him or her with information as well as regarding the information itself. This shall apply likewise to other personnel of the Data Protection Authority on the condition that the Head of the Data Protection Authority decides on the exercise of this right. The right to refuse to give evidence by the Head of the Data Protection Authority includes the refusal of releasing files or other documents.
- 3) The Head of the Data Protection Authority is obliged to maintain confidentiality regarding matters which he gained knowledge of whilst in office. After termination of his or her employment relationship, the Head of the Data Protection Authority is still obliged to maintain confidentiality. This obligation shall not apply to official communications or to matters which are common knowledge or which by their nature do not require confidentiality. The Head of the Data Protection Authority shall decide at his or her due discretion if and to what extent he or she shall testify in court or in extrajudicial proceedings; if he or she is no longer in office, the approval of the acting Head of the Data Protection Authority is required. This shall not affect the legal obligation to report crimes.
- 4) Articles 84 and 85 of the Tax Act shall not apply to the Head of the Data Protection Authority or other members of staff. This shall not apply if the tax authorities require information for carrying out a procedure related to a tax offence as well as a connected tax procedure for which the prosecution constitutes an overriding public interest, or the provider of the information has deliberately provided false information. If the Data Protection Authority identifies a violation of the data protection provisions, they are authorised to report and notify the data subject accordingly.
- 5) The Head of the Data Protection Authority may testify as a witness unless the testimony would:
- a) be detrimental to the welfare of the state, in particular its security or its relations with other states; or

- b) violate fundamental rights.
- 6) If the testimony according to paragraph 5 concerns pending or completed proceedings which are or could be within the competence of the government, the Head of the Data Protection Authority may only testify after consultation with the government. The government may only deny the testimony if it is to the well-being of the state.
- 7) The Head of the Data Protection Authority issues organizational rules which shall be submitted to the government.

Article 15

Tasks

- 1) In addition to the tasks set out in Regulation (EU) 2016/679, the Data Protection Authority shall have the following tasks:
- a) monitor and enforce the application of this Act as well as other regulations regarding data protection as well as all laws and regulations implementing Directive (EU) 2016/680;
- b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention;
- c) advise the Parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing of personal data;
- d) promote the awareness of controllers and processors of their obligations under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;
- e) upon request, provide information to any data subject concerning the exercise of their rights under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680, and if appropriate, cooperate with the supervisory authorities in other Member States to that end;
- f) handle complaints lodged by a data subject, or by a body, organization or association in accordance with Article 55 of Directive (EU) 2016/680, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
- g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;
- h) to conduct investigations on the application of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680, also on the basis of information received from

another supervisory authority or other public authority;

- i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- k) give advice on the processing operations referred to in Article 68; and
- 1) contribute to the activities of the European Data Protection Board.
- 2) Additionally, within the scope of Directive (EU) 2016/680, the Data Protection Authority shall perform the task pursuant to Article 60.
- 3) To fulfill the tasks as set out in paragraph 1 lett. c, the Data Protection Authority may make recommendations to the national Parliament, one of its commissions, the Government or any other public authority concerning all matters related to the protection of personal data. Upon request of the national Parliament, one of its commissions or the government, the Data Protection Authority shall also investigate data protection matters and incidents at public bodies.
- 4) The Data Protection Authority shall facilitate the submission of complaints referred to in paragraph 1 lett. f by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.
- 5) The services provided by the Data Protection Authority are free of charge for the data subjects. When requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Data Protection Authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The Data Protection Authority may also deny services under these circumstances. The Data Protection Authority shall bear the burden of proof in such cases. The government shall regulate the details in an ordinance.

Article 16

Activity Report

The Data Protection Authority shall produce an annual report on its activities, which may include a list of the types of infringement notified and the types of measures taken in accordance with Article 58 (2) of Regulation (EU) 2016/679. The report shall be submitted to the Parliament and the government and be made available to the public, to the EFTA Surveillance Authority and to the European Data Protection Board.

Article 17

Powers

1) The Data Protection Authority shall have, within the scope of Regulation (EU) 2016/679, the powers referred to in Article 58 of Regulation (EU) 2016/679. If the Data Protection Authority concludes that

there is a breach of data protection regulations or that there are other shortcomings regarding the processing of personal data, the Data Protection Authority shall inform the competent supervisory authority. Before exercising the powers pursuant to Article 58 (2) (b) to (g), (i) and (j) of Regulation (EU) 2016/679, the Data Protection Authority shall give this authority the opportunity to notify its opinion to the controller within a reasonable period. The Data Protection Authority may refrain from giving the opportunity to notify its opinion if an immediate decision has to be made due to imminent danger, reasons of public security or in the public interest, or if it conflicts with compelling public interests. The opinion shall include a brief description of the measures taken on the basis of the information from the Data Protection Authority.

- 2) If the Data Protection Authority concludes that, in data processing for purposes beyond the scope of Regulation (EU) 2016/679, public or non-public bodies have violated this Act or other data protection legislation or there are other shortcomings with their processing or use of personal data, the Data Protection Authority shall notify the controller of the violation. In the case of a public body the Data Protection Authority will additionally inform the government. The Data Protection Authority shall give the controller and in the case of a public body likewise the government the opportunity to notify its opinion within a reasonable period. The Data Protection Authority may refrain from notifying the controller or requesting a statement if the infringement is insignificant or was remedied in the meantime. The statement shall include a brief description of the measures taken on the basis of the information from the Data Protection Authority. The Data Protection Authority may also warn the controller if the intended processing of personal data is likely to violate this Act or any other data protection legislation applying to the respective data processing.
- 3) The powers of the Data Protection Authority shall also extend to:
- a) personal data obtained by public and non-public bodies regarding the contents of and specific circumstances relating to postal communications and telecommunications, and
- b) personal data which are protected by official secrecy, especially tax secrecy pursuant to Article 83 of the Tax Act.
- 4) Public and non-public bodies shall be obligated to provide the Data Protection Authority as well as any persons charged with the monitoring of compliance with data protection legislation by the Data Protection Authority:
- a) after being given due notice by the Data Protection Authority or a responsible person, access to all premises, including to any data processing equipment and means, and to all personal data and all information necessary to perform their tasks; and
- b) any information which is relevant and necessary to fulfill their tasks. In the case of a non-public body, the person who is obliged to provide the information may deny the provision of information if this would expose himself or another person as set out in § 108 (1) of the Code of Criminal Procedure to criminal prosecution. The person concerned shall be informed accordingly.
- 5) When exercising the monitoring activities pursuant to Article 4, the Data Protection Authority shall observe and respect the rights of the public and non-public bodies and third parties.

- 6) The Data Protection Authority advises and provides support to data protection officers and takes into consideration their typical needs. The Data Protection Authority may demand the dismissal of a data protection officer if he or she does not have the expert knowledge needed to perform his or her tasks or if there is a serious conflict of interests as referred to in Article 38 (6) of Regulation (EU) 2016/679.
- 7) The Data Protection Authority shall only process data for tasks relating to its supervisory powers. They may also transfer data to other supervisory authorities. Any further processing going beyond Article 6 (4) of Regulation (EU) 2016/679 is allowed if:
- a) it is obvious that the processing is in the interest of the data subject and there is no reason to believe that the data subject would with regard to that other purpose deny his or her consent;
- b) the processing is necessary to prevent substantial harm to the common good or a threat to public security, defense or national security; or to safeguard substantial concerns of the common good; or
- c) the processing is necessary for the prosecution of crimes, execution or enforcement of punishments or other measures laid down in the Criminal Code as well as measures laid down in the Juvenile Court Act or the enforcement of fines.

E. Representation on the European Data Protection Board and cooperation with other supervisory authorities

Article 18

Representation on the European Data Protection Board

The Data Protection Authority is representing the Principality of Liechtenstein on the European Data Protection Board.

Article 19

Cooperation with other supervisory authorities

Prior to submitting an opinion to supervisory authorities of other EEA member states, the EFTA Surveillance Authority or the European Data Protection Board, the Data Protection Authority informs other national supervisory authorities pursuant to Article 85 and 91 of Regulation (EU) 2016/679 if they are affected by the issue.

F. Legal Remedies

Article 20

Legal Remedies

1) Decisions and orders issued by the Data Protection Authority can be appealed to the Commission for

Administrative Matters within four (4) weeks of receiving the decision.

- 2) Decisions and orders issued by the Commission for Administrative Matters can be appealed to the Administrative Court within four (4) weeks of receiving the decision or order; the Data Protection Authority is also entitled to make use of this legal remedy.
- 3) The Data Protection Authority shall not lift the suspensive effect of decisions and orders issued against other public bodies.

II. Implementing provisions for purposes in accordance with Article 2 of Regulation (EU) 2016/679

A. Legal basis for processing personal data

1. Processing of special categories of personal data and processing for other purposes

Article 21

Processing of special categories of personal data

- 1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data pursuant to Article 9 (1) of Regulation (EU) 2016/679 shall be permitted:
- a) by public and non-public bodies:
- 1. if processing is necessary to exercise the rights derived from the right of social security and social protection and to comply with the related obligations;
- 2. if processing is necessary for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a data subject's contract with a health professional or other persons subject to the obligation of professional secrecy or under their supervision; or;
- 3. if processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; in addition to the measures set forth in paragraph 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with;
- b) by public bodies:
- 1. if processing is urgently necessary for reasons of substantial public interest;
- 2. if processing is necessary to prevent a substantial threat to public security;
- 3. if processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; or

4. if processing is necessary for urgent reasons of defence or to fulfill supra- or intergovernmental obligations of a public body in the field of crisis management or conflict prevention or for humanitarian measures;

and as far as the interests of the controller regarding the data processing referred to in letter b outweigh the interests of the data subjects.

- 2) In the cases of paragraph 1, appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:
- a) technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;
- b) measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
- c) measures to increase awareness of staff involved in processing operations;
- d) designation of a data protection officer;
- e) limiting access to personal data within the controller's or processor's competence;
- f) pseudonymisation of personal data;
- g) encryption of personal data;
- h) measures to ensure the ability, confidentiality, integrity, availability and resilience of systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
- i) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; or
- k) specific rules of procedures which ensure the compliance with this Act as well as Regulation (EU) 2016/679 in case of a transfer or processing for other purposes.

Article 22

Processing of data for other purposes by public bodies

- 1) Public bodies may process personal data for a purpose other than the one for which the data were collected where such processing is necessary for them to perform their duties and if:
- a) it is obvious that the processing is in the interest of the data subject and there is no reason to believe that the data subject would refuse consent if he or she was aware of the other purpose;

- b) information provided by the data subject needs to be verified as there is reason to believe that the information provided is incorrect;
- c) processing is necessary to prevent substantial harm to the common good or a threat to public security, defence or national security; or to safeguard substantial concerns of the common good; or to ensure tax and customs revenues;
- d) processing is necessary for the prosecution of crimes, execution or enforcement of punishments or other measures laid down in the Criminal Code as well as measures laid down in the Juvenile Court Act or the enforcement of fines:
- e) processing is necessary to prevent serious harm to the rights of another person; or
- f) processing is necessary to exercise powers of supervision and monitoring, to conduct audits or organizational analyses of the controller; this includes the processing of data for training or examination purposes by the controller, as long as the legitimate interests of the data subject concerned are not impaired.
- 2) The processing of special categories of personal data pursuant to Article 9 (1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted where the requirements of paragraph 1 are met and an exemption under Article 9 (2) of Regulation (EU) 2016/679 or Article 21 applies.

Article 23

Processing of data for other purposes by non-public bodies

- 1) A non-public body may process personal data for a purpose other than the one for which the data were collected if:
- a) processing is necessary:
- 1. to prevent threats to state or public security or for the prosecution of criminal offences; or
- 2. for the establishment, exercise or defence of legal claims; and
- b) the data subject does not have an overriding interest in not having the data processed.
- 2) The processing of special categories of personal data pursuant to Article 9 (1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted where the requirements of paragraph 1 are met and an exemption under Article 9 (2) of Regulation (EU) 2016/679 or Article 21 applies.

Article 24

Transfer of data by public bodies

- 1) The transfer of personal data by public bodies to public bodies shall be permitted if it is necessary for the transferring body or the third party who receives the data to fulfill their tasks and the conditions are met which would permit processing pursuant to Article 22. A third party who receives the personal data shall process these transferred data only for the purposes for which the data were transferred. The processing of these data for other purposes shall be permitted if the requirements of Article 22 are met.
- 2) The transfer of personal data by public bodies to non-public bodies shall be permitted if:
- a) the transfer is necessary for the transferring body to fulfill its duties and the requirements of Article 22 are met which would allow the processing.
- b) the third party who receives the data presents evidence of a legitimate interest in knowledge of the data to be transferred and the data subject does not have a legitimate interest in not having the data transferred; or
- c) the data are necessary for the establishment, exercise or defense of legal claims
- and the third party has promised the transferring public body that it will only use the data for the purpose for which they were transferred. Processing for other purposes shall be permitted if the transfer according to sentence 1 would be legitimate and the transferring body has agreed.
- 3) The transfer of special categories of personal data pursuant to Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if the requirements of paragraph 1 or 2 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Article 21 applies.

2. Special processing situations

Article 25

Restriction of the right to access or right to information for the media

- 1) The controller may deny, limit or delay the provision of information pursuant to Article 15 of Regulation (EU) 2016/679 regarding the processing of personal data which are to be exclusively published in the editorial part of periodically published media if:
- a) the personal data disclose the source of information;
- b) insight into the drafts of publications would have to be given; or
- c) the free formation of public opinion would be threatened.
- 2) Members of the press may refuse, limit or delay the provision of information pursuant to Article 15 of Regulation (EU) 2016/679 if the processing of personal data is being used exclusively as a personal work aid.

Article 26

Data secrecy

In addition to legal secrecy obligations, a person who processes personal data, or has them processed, shall safeguard personal data he or she was entrusted with or was granted access to in the course of his professional occupation, as far as there is no legal reason for the disclosure of the data.

Article 27

Processing of data for purposes of scientific or historical research and for statistical purposes

- 1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data pursuant to Article 9 (1) of Regulation (EU) 2016/679 shall be permitted without consent of the data subject if the processing is necessary for scientific or historical research purposes or purposes related to statistics and the interests of the controllers outweigh the legitimate interest of the data subject in not processing the data. The controller shall ensure that appropriate and specific measures are taken to safeguard the interests of the data subjects pursuant to Article 21 (2), second sentence.
- 2) For scientific or historical research purposes or purposes related to statistics in the public interest, the controller may process personal data which are not subject to paragraph 1, first sentence if the processing is necessary for these purposes and if:
- a) the data are publicly accessible;
- b) the data are pseudonymised personal data and the controller cannot identify the data subject with legal measures; or
- c) getting consent of the data subject is impossible or involves a disproportionate effort due to the lack of reachability.

Paragraph 1, second sentence shall apply accordingly. Article 4 shall remain unaffected.

- 3) Paragraphs 1 and 2 shall also apply to personal data that the controller has obtained lawfully for other examinations or purposes.
- 4) The rights of data subjects pursuant to Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfillment of the research or statistical purposes. The right to access pursuant to Article 15 of Regulation (EU) 2016/679 shall not apply if the data are required for scientific research and the provision of information would involve a disproportionate effort.
- 5) In addition to the measures set out in Article 21 (2), all personal data which are processed for scientific or historic research purposes or for purposes related to statistics are to be anonymised as soon as the

research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject. Heretofore, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research or statistical purpose.

6) The controller may only publish personal data if the data subject has provided consent or it is indispensable for the presentation of research findings.

Article 28

Processing of data for the purposes of personal, family and genealogical research as well as the maintenance and publication of family chronicles and biographies

The processing of personal data shall be permitted without consent of the data subject if the processing is required for purposes of personal, family or genealogical research as well as the maintenance and publication of family chronicles and biographies. By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data shall be permitted pursuant to Article 9 (1) of Regulation (EU) 2016/679 if the processing is required for these purposes and the interests of the controller outweigh the interests of the data subjects in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Article 21 (2), second sentence.

Article 29

Processing of data for archiving purposes in the public interest

- 1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data pursuant to Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if necessary for archiving purposes in the public interest. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Article 21 (2), second sentence.
- 2) For archiving purposes in the public interest where no personal data can be derived from, the controller may process all personal data which are not subject to paragraph 1, first sentence, if the processing is necessary for these purposes and if:
- a) the data are publicly available;
- b) the data are pseudonymised personal data and the controller cannot relate personal data to an identified or identifiable natural person with legal means; or
- c) getting consent of the data subject is impossible or involves a disproportionate effort due to the lack of reachability.

Paragraph 1, second sentence shall apply accordingly. Article 4 shall remain unaffected.

- 3) Additionally, paragraphs 1 and 2 shall apply accordingly to personal data which were lawfully collected by the controller for other examinations or other purposes.
- 4) The right to access by the data subject pursuant to Article 15 of Regulation (EU) 2016/679 shall not apply if the archival material is not connected to the person's name or no information is given which would enable the archival material to be found with reasonable administrative effort.
- 5) The right to rectification pursuant to Article 16 of Regulation (EU) 2016/679 shall not apply if the personal data are processed for archiving purposes in the public interest. If the data subject disputes the accuracy of the personal data, he or she shall have the opportunity to present his or her version. The responsible archive shall be obligated to add the rectified information to the files.
- 6) The rights pursuant to Article 18 (1) lett. a, b and d, Articles 20 and 21 of Regulation (EU) 2016/679 shall not apply if these rights are likely to render impossible or seriously impair the achievement of the archiving purposes in the public interest, and the exceptions are necessary to fulfill those purposes.

Article 30

Rights of the data subject and powers of the supervisory authorities in the case of secrecy obligations

- 1) With regards to the rights of the data subject pursuant to Articles 14, 15 and 34 of Regulation (EU) 2016/679, the following shall apply:
- a) In addition to the exceptions in Article 14 (5) of Regulation (EU) 2016/679, the obligation to inform the data subject pursuant to Article 14 (1) (4) of Regulation (EU) 2016/679 shall not apply if meeting this obligation would disclose information which:
- 1. is subject to legal confidentiality obligations; or
- 2. by its nature must be kept secret, in particular because of overriding legitimate interests of a third party;
- b) The right of access pursuant to Article 15 of Regulation (EU) 2016/679 shall not apply if access would disclose information which:
- 1. is subject to legal confidentiality obligations; or
- 2. by its nature must be kept secret, in particular because of overriding legitimate interests of a third party;
- c) In addition to the exception in Article 34 (3) of Regulation (EU) 2016/679, the obligation to inform the data subject of a personal data breach according to Article 34 of Regulation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose information which
- 1. is subject to legal confidentiality obligations; or
- 2. by its nature must be kept secret, in particular because of overriding legitimate interests of a third party.

By way of derogation from the exception pursuant to lett. c no. 2, the data subject shall be informed

according to Article 34 of Regulation (EU) 2016/679 if the data subject has an overriding interest in being informed, in particular taking into account the threat of damage.

- 2) If when establishing or in the course of a mandate relationship data of third persons are transferred to persons who are subject to a professional secrecy, the transferring person shall not be obligated to inform the data subject pursuant to Article 13 (3) of Regulation (EU) 2016/679 unless the data subject has an overriding interest in being informed.
- 3) The investigative powers of the Data Protection Authority pursuant to Article 58 (1) lett. e and f of Regulation (EU) 2016/679 shall not apply with regard to persons mentioned in § 121 (1), (3) and (4) of the Liechtenstein Criminal Code or their processors if the exercise of these powers would violate these persons' obligations to secrecy. If the Data Protection Authority in the context of an investigation gains knowledge of data which is subject to professional secrecy pursuant to paragraph 1, the obligation of secrecy shall also apply to the Data Protection Authority.

Article 31

Protection of commercial transactions in the case of scoring and credit reports

- 1) For the purpose of deciding on the creation, execution or termination of a contractual relationship with a natural person, the use of a probability value for certain future action by this person (scoring) shall be permitted only if:
- a) the provisions of data protection law are respected;
- b) the data used for the calculation of the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognised mathematic-statistical procedure;
- c) the data used for the calculation of the probability value does not exclusively contain address data; and
- d) address data are used, the data subject was notified ahead of time of the intended use of these data; this notification shall be documented.
- 2) The use of a probability value calculated by credit reporting agencies to determine a natural person's ability and willingness to pay shall be permitted in the case of including information on claims only as far as the conditions of paragraph 1 are met and only claims concerning a performance owed which has not been rendered on time are considered and
- a) which have been subject of a writ of execution pursuant to Article 1 of the Enforcement Act;
- b) which have been determined pursuant to Article 66 of the Bankruptcy Act and have not disputed at the bankruptcy trial by the debtor;
- c) which are explicitly acknowledged by the debtor;
- d) for which:
- 1. the debtor was notified at least twice in writing after the due date of the claim;

- 2. at least four weeks have elapsed since the first reminder;
- 3. the debtor was previously notified of possible consideration by a credit reporting agency at least in the first reminder; and
- 4. The debtor has not disputed the claim; or
- e) the contractual relationship on which the claim is based, can be terminated without prior notice because of outstanding debts and the debtor was notified of possible consideration by a credit reporting agency.
- 3) The lawfulness of the processing of other data relevant to creditworthiness including the evaluation of possibility values pursuant to general data protection law shall remain unaffected.

B. Rights of the data subject

Article 32

Information obligation when collecting personal data from the data subject

- 1) In addition to the exception in Article 13 (4) of Regulation (EU) 2016/679, the obligation to inform the data subject pursuant to Article 13 (3) of Regulation (EU) 2016/679 shall not apply if the disclosure of information on the further processing:
- a) concerns the further processing of data stored in analogue form, for which the controller directly contacts the data subject through the further processing, the purpose is consistent with the purpose for which the data were collected in accordance with Regulation (EU) 2016/679, the communication with the data subject does not take place in digital form and the interest of the data subject in obtaining the information is considered to be minimal, especially regarding the circumstances of the individual case, in particular with regard to the context in which the data were collected;
- b) concerns a public body and the information would endanger the proper performance of tasks as set out in Article 23 (1) lett. a to e of Regulation (EU) 2016/679 for which the controller is responsible, and the interest of the controller in not providing the information outweigh the interests of the data subject;
- c) would put public security at risk or be in another way detrimental to the welfare of the state and the controller's interests in not providing the information outweigh the interests of the data subject;
- d) would impair the establishment, execution or defence of legal claims and the controller's interests in not providing the information outweigh the interests of the data subject; or
- e) would impair a confidential data transfer to public bodies.
- 2) If information is not provided to the data subject pursuant to paragraph 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject including the provision of information pursuant to Article 13 (1) and (2) of Regulation (EU) 2016/679 to the public in precise, transparent, understandable and easily accessible form and in clear and simple language. The controller shall record in writing the reasons for the non-disclosure of information. Sentences 1 and 2 shall not apply

in cases of paragraph 1, lett. d and e.

3) If the information according to paragraph 1 is omitted due to a temporary obstacle, the controller shall meet the obligation of information taking into consideration the specific circumstances of the processing within a reasonable time period, but no later than two weeks after the obstacle has ceased to exist.

Article 33

Obligation of information when personal data have not been collected from the data subject

- 1) In addition to the exception in Article 14 (5) of Regulation (EU) 2016/679 and Article 30 (1) lett. a, the obligation of information of the data subject according to Article 14 (1), (2) and (4) of Regulation (EU) 2016/679 shall not apply if providing information:
- a) concerns a public body and:
- 1. would impair the proper performance of tasks of the controller pursuant to Article 23 (1) lett. a-e of Regulation (EU) 2016/679; or
- 2. would threaten the public security or order or be in another way detrimental to the state, and therefore, the interest of the data subject in receiving the information must not take precedence;
- b) concerns a non-public body and:
- 1. would impair the establishment, execution or defence of legal claims or the processing includes data from contracts under private law and is intended to prevent harm from criminal offences, unless the data subject has an overriding legitimate interest in receiving the information; or
- 2. the responsible public body has determined with respect to the controller that the disclosure of data would impair public security or order or would be in another way to the disadvantage of the state; in cases of data processing for the purpose of law enforcement, a determination according to the first half-sentence is not required.
- 2) If information is not provided to the data subject pursuant to paragraph 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including the provision of information pursuant to Article 14 (1) and (2) of Regulation (EU) 2016/679 for the public in a precise, transparent, understandable and easily accessible form and in a clear and simple language. The controller shall record in writing the reasons for the non-disclosure of information.
- 3) The provision of information regarding the transfer of personal data by public bodies to the National police for the fulfillment of their tasks to ensure public security requires the approval of the National Police.

Article 34

Right of access by the data subject

- 1) In addition to the exceptions in Article 27 (4), Article 29 (4) and Article 30 (1) lett. b, the data subject's right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if:
- a) the data subject shall not be informed pursuant to Article 33 (1) lett a, b, no. 2 or (3); or
- b) the data:
- 1. were stored only because they may not be erased due to legal or statutory provisions on retention; or
- 2. only serve the purpose of monitoring data protection or safeguarding data,
- and the provision of information would involve a disproportionate effort and appropriate technical and organizational measures make processing for other purposes impossible.
- 2) The reasons for the denial of providing information shall be documented. The data subject shall be informed of the reasons for refusing to provide information, unless in law and in fact on which the decision is based would undermine the intended purpose of refusing to provide the information. Data stored for the purpose of providing information to the data subject and preparing such provision may be processed only for this purpose and for purposes of data protection monitoring; processing for other purposes shall be restricted according to Article 18 of Regulation (EU) 2016/679.
- 3) If a public body does not provide information to the data subject, the data subject may request that the information is to be disclosed to the Data Protection Authority if the government does not conclude that the provision of information would impair the security of the state. The information from the Data Protection Authority to the data subject on the results of the data protection assessment shall not permit any conclusions to be drawn concerning the information held by the controller unless the latter agrees to the provision of more extensive information.
- 4) The data subject shall have the right of access to personal data processed by a public body neither automatically nor stored in a filing system only if the data subject provides information enabling the data to be located and if the effort required is not disproportionate to the data subject's interest in the information.

Article 35

Right to erasure

1) If in the case of automated or non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of processing or storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data in accordance with Article 17 (1) of Regulation (EU) 2016/679 in addition to the exceptions in Article 17 (3) of Regulation (EU) 2016/679. In this case, restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679 shall apply

in place of erasure. The first and second sentences shall not apply if the personal data were processed unlawfully.

- 2) In addition to Article 18 (1) (b) and (c) of Regulation (EU) 2016/679, paragraph 1, first and second sentences shall apply accordingly in the case of Article 17 (1) (a) and (d) of Regulation (EU) 2016/679 as long and as far as the controller has reason to believe that erasure would adversely affect legitimate interests of the data subject. The controller shall inform the data subject of the restriction of processing if doing so is not impossible or would not involve a disproportionate effort.
- 3) In addition to Article 17 (3) lett. b of Regulation (EU) 2016/679, paragraph 1 shall apply in the case as set out in Article 17 (1) lett. a of Regulation (EU) 2016/679 if contractual or legal retention periods prevent the erasure.

Article 36

Right to object

The right to object pursuant to Article 21 (1) of Regulation (EU) 2016/679 shall not apply with regard to a public body if there is an urgent public interest in the processing of data which outweighs the interests of the data subject or if a legal provision requires the processing.

Article 37

Automated individual decision-making, including profiling

- 1) In addition to the exceptions in Article 22 (2), lett. a and c of Regulation (EU) 2016/679, the right not to be subject to a decision based solely on automated processing pursuant to Article 22 (1) of Regulation (EU) 2016/679 shall not apply if the decision:
- a) is taken in the context of providing services pursuant to an insurance contract and
- 1. aims at the determination of the insurance premium;
- 2. the request of the data subject was fulfilled; or
- 3. the decision is based on the application of binding rules of remuneration for therapeutic treatment;
- b) is taken in order to fulfill the due diligence obligations with regard to establishing a business relationship, the adequate monitoring of risks as well as for the risk evaluation pursuant to Article 5, 9 and 9a of the Due Diligence Act;
- c) is taken with regard to credit transactions pursuant to Article 3 (3) lett. b of the Banking Act; or
- d) is taken with regard to providing an investment service or ancillary services according to Article 3 (4) of the Banking Act or Article 3 of the Asset Management Act.

- 2) With the exception as set out in (1) lett. a no. 2 and lett. b, the controller shall take appropriate measures to safeguard the legitimate interests of the data subject, at least the rights to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision; the controller shall inform the data subject of these rights no later than the notification indicating that the data subject's request will not be granted in full or the data subject could be negatively affected by the automated decision-making.
- 3) Decisions pursuant to (1) lett. a may be based on the processing of health data according to Article 4 no. 15 of Regulation (EU) 2016/679. The controller shall take appropriate and specific measures to safeguard the interests of the data subject according to Article 21 (2) second sentence.

C. Obligations of controllers and processors

Article 38

Data protection officers of non-public bodies

- 1) If the designation of a data protection officer by private bodies is mandatory, the dismissal of the data protection officer is only permissible if the conditions on the termination without notice for cause pursuant to § 1173a Article 53 ABGB are met.
- 2) The data protection officer shall be bound by professional secrecy regarding the identity of the data subject as well as any circumstances that allow to draw conclusions to the data subject as long as the data subject does not consent to the disclosure of information.
- 3) Where in the course of their activities data protection officers become aware of data for which the controller or the processor has the right to refuse to give evidence, this right shall also apply to the data protection officer and his or her assistants. The person to whom the right to refuse to give evidence applies, shall decide whether to exercise this right unless it is impossible to effect such a decision in the foreseeable future. Where the right of the data protection officer to refuse to give evidence applies, his or her files and other documents shall not be subject to seizure.

Article 39

Accreditation

- 1) The power to act as a certification body pursuant to Article 43 (1) first sentence of Regulation (EU) 2016/679 shall be granted by the Accreditation Body of Liechtenstein.
- 2) The Government regulates further details in the according ordinance.

D. Penal provisions

Article 40

Violations according to Regulation (EU) 2016/679

- 1) The Data Protection Authority shall impose fines pursuant to paragraph 2 for violations of Regulation (EU) 2016/679 also if the violation is determined to be negligent according to Article 83 (4) to (6) of Regulation (EU) 2016/679.
- 2) The fines are as follows:
- a) In cases pursuant to Article 83 (4) of Regulation (EU) 2016/679: up to 11 Million Swiss Francs or in the case of a legal person up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher;
- b) In cases pursuant to Article 83 (5) and (6) of Regulation (EU) 2016/679: up to 22 Million Swiss Francs or in the case of a legal person up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- 3) The Data Protection Authority shall impose fines against legal persons if the violation occurred in the course of the business activity of the legal person by a person that was solely responsible or as a member of the board, the management, the chairman or the supervisory board of the legal person or based on any other management staff forming part of the legal person provided that they:
- a) are entitled to represent the legal person;
- b) have powers of control as a member of the management staff; or
- c) have other considerable influence on the management of the legal person.
- 4) For violations which were committed by an employee of the legal person even if not culpable the legal person is responsible and liable if the violation was made possible or greatly facilitated by not taking appropriate measures to prevent the violation by the persons mentioned in paragraph 3.
- 5) The responsibility of the legal person for the violation and the criminal liability of the person mentioned in paragraph 3 or of employees mentioned in paragraph 4 of the same violation do not exclude each other. The Data Protection Authority may refrain from imposing a fine on the natural person if the legal person was already fined for the same violation and there are no special circumstances which would prevent such refrain.
- 6) The Data Protection Authority shall apply Article 83 (2) to (6) of Regulation (EU) 2016/679 on the condition that the proportionality principle is respected. Particularly, in the case of first time violations the Data Protection Authority shall make use of their corrective powers according to Article 58 of Regulation (EU) 2016/679 and issue warnings.
- 7) Authorities and other public bodies shall not be subject to any administrative fines.

Article 41

Unlawful gathering of personal data

The data subject may request the district court ("Landgericht") to prosecute anyone for unlawful gathering of personal data which was not freely available. This offense is punishable by up to six months imprisonment or a fine up to 360 daily rates.

Article 42

Violation of data secrecy

- 1) Deliberately giving access to, publishing or processing secret personal data by a person who had access to such data through his profession may be brought to the district court ("Landgericht") upon request by the data subject and may be sentenced by up to six months imprisonment or a fine up to 360 daily rates.
- 2) If the offence was committed for a pecuniary advantage or in order to inflict a considerable disadvantage to a person may be sentenced upon request by the data subject by up to one year imprisonment or a fine up to 360 daily rates.
- 3) Penalties or sentences shall also be imposed on anyone who deliberately gives access to, publishes or processes secret personal data which he or she had access to in the course of his activity for the person bound by professional confidentiality or during the training or education with that person.
- 4) Giving access to, publishing or processing secret personal data is also punishable after termination of the employment or an educational relationship.

Article 43

Prohibition of use

A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a notification pursuant to Article 34 (1) of Regulation (EU) 2016/679 may only be used in a criminal proceeding according to Article 41 and 42 against the person subject to mandatory reporting or the notifying person or any other person as set out in § 108 (1) of the Code of Criminal Procedure if the person subject to mandatory reporting or the notifying person have given their consent.

E. Liability

Article 44

Liability and right to compensation

1) Any person who was subject to material or immaterial damages through a violation of Regulation (EU) 2016/679 or of the provisions of Chapter I or II is eligible for compensation from the controller or the

processor pursuant to Article 82 of Regulation (EU) 2016/679. The general provisions of the Civil Code shall apply for this right to compensation.

2) If the controller or processor has appointed a representative pursuant to Article 27 (1) of Regulation (EU) 2016/679, the representative may also be entitled and authorised to accept documents sent in the course of a civil procedure. Article 12 of the Delivery Act shall remain unaffected.

III. Implementing provisions for processing for purposes in accordance with Article 1 (1) of Directive (EU) 2016/680

A. Scope, definitions and general principles for processing personal data

Article 45

Scope

The provisions of this Part shall apply for the processing of personal data by public bodies which are competent for the prevention, investigation, detection or prosecution of criminal offences, as far as they process data for the purpose of carrying out these tasks. The public body shall be regarded in that case as the controller. The prevention of criminal offences pursuant to the 1st sentence shall include protection against and prevention of threats to public security. Additionally, the 1st and 2nd sentences shall apply to all public bodies which are responsible for executing penalties, measures as referred to in the criminal code, educational measures or any other measures or correctional actions in accordance with juvenile law as well as fines. Provisions in this chapter shall likewise apply to processors.

Article 46

Definitions

For the purposes of this Act:

- a) "personal data" means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- b) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- c) "restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

- d) "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- e) "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- f) "filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- g) "controller" means the competent authority, which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- h) "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- i) "recipient" means a natural or legal person, public authority, agency or other body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with EEA law or other laws shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- k) "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- l) "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- m) "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- n) "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- o) "special categories of personal data":
- 1. data revealing racial or ethnic origin, political opinions, religious or ideological convictions or any trade union membership;
- 2. genetic data;

- 3. biometric data for the purpose of uniquely identifying a natural person;
- 4. data concerning health; and
- 5. data regarding a natural person's sex life or sexual orientation;
- p) "supervisory authority" means an independent public authority which is established by an EEA Member State pursuant to Article 41 of Directive (EU) 2016/680;
- q) "international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
- r) "consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Article 47

General principles for processing personal data

Personal data shall:

- a) be processed lawfully and in good faith;
- b) be collected for specific, explicit and legitimate purposes and not be processed contrary to these purposes;
- c) be adequate, relevant and not excessive in relation to the purposes for which they are processed;
- d) be accurate and if necessary kept up to date; therefore, all appropriate measures shall be taken that personal data which are false or contain errors are erased or rectified without delay;
- e) be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed; and
- f) be processed in a manner that ensures appropriate security of the personal data; including technical and organizational measures to prevent unauthorised or unlawful processing, accidental loss, accidental destruction or accidental damage.

B. Legal basis for processing personal data

Article 48

Processing of special categories of personal data

- 1) The processing of special categories of personal data shall only be permitted if it is strictly necessary for the performance of the tasks and:
- a) is authorised by law;
- b) aims at the protection of the vital interests of a natural person; or
- c) relates to personal data which are manifestly made public by the data subject.
- 2) If special categories of personal data are processed, appropriate safeguards for the legally protected interests of the data subject shall be implemented. Appropriate safeguards may be:
- a) specific requirements for data security or data protection monitoring;
- b) special time limits within which data must be reviewed for relevance and erasure;
- c) measures to increase awareness of staff involved in processing operations;
- d) limitation of access to personal data within the controller;
- e) separate processing of such data;
- f) the pseudonymisation of personal data;
- g) the encryption of personal data; or
- h) specific codes of conduct to ensure lawful processing in the case of transfer or processing for other purposes.

Article 49

Processing for other purposes

Processing of personal data for another purpose than the one defined when collecting the data shall only be permitted if the other purpose is listed in Article 45, the controller is authorised to process the data for that purpose and the processing for the new purpose is required and proportionate to this purpose. The processing of personal data for a purpose not listed in Article 45 shall only be permitted if it is allowed by law.

Article 50

Processing of personal data for archiving, scientific and statistical purposes

Personal data may only be processed for purposes listed in Article 45 for archiving, scientific or statistical purposes if it is in the public interest and appropriate safeguards are taken to guarantee the legally protected interests of the data subjects. Such safeguards may include the prompt anonymisation of personal data, measures to prevent unauthorised disclosure to third parties, or in processing them organizationally and spatially separate from other tasks.

Article 51

Consent

- 1) If the processing of personal data takes place on the basis of consent, the controller shall be able to provide evidence of the data subject's consent.
- 2) If the data subject's consent is given in writing pursuant to paragraph 1, which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
- 3) The data subject has the right to withdraw his or her consent pursuant to paragraph 1 at any time. The withdrawal of consent shall not affect the lawfulness of any prior processing until the time of withdrawal. The data subject shall be informed of this before giving consent.
- 4) The consent pursuant to paragraph 1 shall only be effective when based on the data subject's free decision. When determining if the consent was freely given, the circumstances of giving consent must be considered. The affected person shall be informed of the intended purpose of processing. In particular cases or on request, data subject shall also be informed of the consequences of withholding consent.
- 5) If special categories of personal data are being processed, the consent pursuant to paragraph 1 shall explicitly mention this fact.

Article 52

Processing on instruction from the controller

Any person acting under the authority of the controller or the processor who has access to personal data shall only process this data on instructions from the controller, unless he or she is legally required to process the data.

Article 53

Confidentiality

Persons entrusted with the processing of personal data shall not process data without authorization (confidentiality). They shall be obligated when taking up their duties to maintain confidentiality. The obligation of confidentiality shall continue after their employment ends.

Article 54

Automated individual decision-making

- 1) A decision which is based solely on automatic processing and may have an adverse legal effect for the data subject or significantly affects him or her, shall only be permitted when authorised by law.
- 2) Decisions pursuant to paragraph 1 shall not be based on special categories of personal data unless appropriate measures to safeguard the data subject's legally protected and legitimate interests are in place.
- 3) Profiling which results in the data subject being discriminated based on special categories of personal data shall be prohibited.

C. Rights of the data subject

Article 55

General information on data processing

The controller shall provide general and publicly accessible information on:

- a) the purposes of the processing;
- b) the rights of the data subject with regard to the processing of his or her personal data to access, rectification, erasure and restriction of processing;
- c) the name and contact details of the controller and the data protection officer;
- d) the right to lodge a complaint with the Data Protection Authority; and
- e) the contact details of the Data Protection Authority.

Article 56

Notification of data subjects

1) If special legislation provides for or requires notifying data subjects of the processing of their personal

data, especially in the case of undercover operations, such notification shall include at least the following information:

- a) the information listed in Article 55;
- b) the legal basis for the processing;
- c) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- d) where applicable, the categories of recipients of personal data; and
- e) if necessary, further information, particularly if the personal data were collected without the knowledge of the data subject.
- 2) In cases of paragraph 1, the controller may delay, limit or refrain from the notification if it would affect:
- a) the performance of the tasks set out in Article 45,
- b) public security or
- c) the legally protected interests of third parties

if the interest in avoiding these threats overrides the interest of the data subject in the information.

- 3) If the notification concerns the transfer of personal data to the National Police for the performance of their tasks regarding state security it requires approval of the police.
- 4) In cases of limitation as mentioned in paragraph 2, Article 57 (7) shall apply accordingly.

Article 57

Right of access

- 1) The controller shall inform the data subject upon request if he or she processes data concerning the data subject. Data subjects shall have the right to receive information about:
- a) the personal data processed as well as the categories of data;
- b) the available information on the origin of the data;
- c) the purposes of and legal basis for the processing;
- d) the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organisations;
- e) the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

- f) the existence of the right to request from the controller rectification or erasure or restriction of processing of personal data;
- g) the right to lodge a complaint with the Data Protection Authority pursuant to Article 60; and
- h) the contact details of the Oata Protection Authority.
- 2) Paragraph 1 shall not apply to personal data which are only being processed because they may not be erased due to legal or statutory provisions on retention, or only for purposes of monitoring data protection or safeguarding data, if providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossible.
- 3) The controller may refrain from providing information if the data subject does not provide sufficient information enabling the data to be located and therefore the efforts are disproportionate to the data subject's interest in the information.
- 4) Subject to the conditions of Article 56 (2) the controller may refrain from providing information pursuant to paragraph 1 first sentence or may partially or wholly limit it according to paragraph 1, second sentence.
- 5) If the information concerns the transfer of personal data to the National Police for the fulfillment of their tasks regarding state security, it requires approval of the federal police.
- 6) The controller shall inform the data subject in writing and without delay about the refusal or limitation of the provision of information. This does not apply if the issuance of information would already cause an impairment pursuant to Article 56 (2). The notification according to the first sentence shall include the reasons for the refusal or the restriction unless providing the reasons would undermine the intended purpose of the refusal or restriction of access.
- 7) If a data subject is notified about the refusal or limitation of provision of information pursuant to paragraph 6, the data subject may exercise their right of access via the Data Protection Authority. The controller shall inform the data subject about the possibility of consulting the Data Protection Authority and the available legal remedies pursuant to Article 60. If a data subject exercises its rights according to the first sentence, the information shall be provided to the Data Protection Authority upon request of the data subject, unless the government determines in the individual case that doing so would threaten the security of the state. The Data Protection Authority shall at least inform the data subject that all necessary checks have been conducted or that the Data Protection Authority has conducted a review. This notification may include information as to whether violations of data protection law were found. The notification from the Data Protection Authority to the data subject shall not allow any conclusions to be drawn concerning the information held by the controller unless the latter agrees to the provision of more extensive information. The controller may refuse to such provision only as far as and for as long as he or she could dispense with or restrict information pursuant to paragraph 4. The Data Protection Authority shall also inform the data subject of his or her right to seek a judicial remedy.
- (8) The controller shall document the factual or legal reasons on which the decision is based.

Article 58

Right of rectification and deletion and to restriction of data processing

- 1) The data subject shall have the right to obtain from the controller the rectification of any inaccurate data concerning him or her. Especially, in cases of statements or assessments, the question of accuracy is not relevant for the content of the statement or assessment. If the accuracy or inaccuracy of the data cannot be verified, the controller shall restrict the processing instead of erasing the data. In that case the controller shall inform the data subject before lifting the restriction of processing. The data subject may also have incomplete personal data completed, if doing so is appropriate when taking into account the purposes of processing.
- 2) The data subject has the right to request the erasure of personal data concerning him or her where processing such data is unlawful, knowledge of the data is no longer necessary for the performance of tasks, or the data must be erased to comply with a legal obligation.
- 3) Instead of erasure, the controller may restrict the processing if:
- a) there is reason to believe that erasure would adversely affect legitimate interests of the data subject;
- b) the data must be retained for the purposes of evidence in proceedings serving the purposes of Article 45; or
- c) erasure would be impossible or would involve a disproportionate effort because of the specific type of storage.

Data which is restricted pursuant to the first sentence may only be processed for purposes which prevented their erasure.

- 4) If the controller has rectified inaccurate data, he or she shall inform the body, from which he or she received the personal data, about the rectification. In cases of rectification, erasure or restriction of processing pursuant to paras.1 to 3, the controller shall inform the recipients who received inaccurate data about these measures. The recipient shall rectify or erase the data or restrict their processing.
- 5) The controller shall inform the data subject in writing about any refusal to rectify or erase personal data or restrict its processing. This shall not apply if the provision of this information would result in an impairment pursuant to Article 56 (2). The information according to the first sentence shall include the reasons for the refusal unless providing the reasons would undermine the intended purpose of the refusal.
- 6) Article 57 (7) and (8) shall apply accordingly.

Article 59

Modalities for exercising the rights of the data subject

1) The controller shall communicate with data subjects in a concise, intelligible and easily accessible form, using clear and plain language.

- 2) When responding to requests, without prejudice to Article 57 (6) and Article 58 (5) the controller shall inform the data subject in writing about the follow-up to his or her request without delay.
- 3) The provision of information pursuant to Article 55, the notification according to Articles 56 and 65 as well as the processing of requests pursuant to Articles 57 and 58 shall be free of charge. Where a request pursuant to Articles 57 and 58 is manifestly unfounded or excessive, the controller may charge a reasonable fee, or may refuse to act on the request. In this case, the controller must be able to demonstrate the manifestly unfounded or excessive character of the request.
- 4) If the controller has reasonable doubts as to the identity of the data subject who submitted the request pursuant to Articles 57 or 58, the controller may request further information that is necessary to confirm the identity of the data subject.

Article 60

Right to lodge a complaint with the Data Protection Authority

- 1) Without prejudice to other administrative or judicial remedy, every data subject may lodge a complaint with the Data Protection Authority if the data subject believes that the processing of personal data for the purposes as set out in Article 45 by a public body infringes his or her rights. This shall not apply to the processing of personal data by courts, if they have processed these data in the context of their judicial activities. The Data Protection Authority shall inform the data subject on the progress and the outcome of the complaint and of the possibility of a judicial remedy pursuant to Article 20.
- 2) If a data subject lodges a complaint with the Data Protection Authority instead of the competent supervisory authority in another EEA or Schengen member state, the Data Protection Authority shall transmit the complaint to the competent supervisory authority without delay. In this case, the data subject shall be informed about the forwarding of his or her complaint and, upon request of the data subject, the Data Protection Authority shall provide further support.

D. Obligations of controllers and processors

Article 61

Processing carried out on behalf of a controller

- 1) If personal data is being processed on behalf of a controller by another person or body on behalf of the controller, the latter shall ensure compliance with the rules and regulations of this Act as well as of other data protection provisions. The data subject shall assert his or her rights to access, rectification, erasure, restriction of processing and the right to receive compensation against the controller.
- 2) A controller may use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the law and ensure the protection of the rights of the data subjects.

- 3) Processors shall not engage other processors without prior written authorization by the controller. If the controller has given the processor general authorization to engage other processors, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors. In this case, the controller may object to such changes.
- 4) Where a processor engages another processor, the former shall impose on the latter the same data protection obligations as set out in the contract between the controller and the processor as referred to in paragraph 5 if these obligations are not already binding for the latter processor because of other legislation. Where that other processor fails to fulfill these obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.
- 5) Processing by a processor shall be governed by a contract or other legal instrument that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal instrument shall stipulate, in particular, that the processor
 - a. acts only on documented instructions from the controller; if the processor believes that an instruction is unlawful, the processor shall inform the controller without delay;
 - b. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - c. assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;
 - d. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless law requires storage of the personal data;
 - e. makes available to the controller all information necessary, in particular the logs kept in accordance with Article 75, to demonstrate compliance with these obligations;
 - f. allows for and contributes to audits conducted by the controller or another auditor mandated by the controller;
 - g. complies with the conditions referred to in paragraphs 3 and 4 for engaging another processor;
 - h. takes all measures required pursuant to Article 63; and
 - i. assists the controller in ensuring compliance with the obligations pursuant to Articles 63 to 66 and 68 taking into account the nature of processing and the information available to the processor.
- 6) The contract referred to in paragraph 5 shall be in writing or in an electronic form.
- 7) A processor that determines, in violation of this provision, the purposes and means of processing, shall be considered a controller in respect of that processing.

Article 62

Joint controllers

If two or more controllers jointly determine the purposes and means of processing, they shall be considered joint controllers. Joint controllers shall determine their respective tasks and duties regarding data protection in a mutual agreement and in a transparent way, unless these tasks and responsibilities are

already determined by law. In particular, this agreement must indicate which of them shall meet which information obligations, and how and with respect to whom data subjects may exercise their rights. Such an agreement shall not prevent data subjects from asserting their rights against each of the joint controllers.

Article 63

Requirements regarding the security of data processing

- 1) The controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data. The controller shall take into account the relevant generally recognised technical guidelines and recommendations in information technology.
- 2) The measures mentioned in paragraph 1 may include pseudonymisation and encryption of personal data, if such means are possible in view of the purposes of processing. The measures pursuant to paragraph 1 shall ensure
- a) the ongoing confidentiality, integrity, availability and resilience of processing systems and services in connection with processing; and
- b) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- 3) In cases of an automatic processing of data, following a risk assessment, the controller and the processor shall take appropriate measures designed to:
- a) deny unauthorised persons access to processing equipment used for processing ('access control');
- b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');
- c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');
- d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');
- e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');
- f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');
- g) ensure that it is subsequently possible to verify and establish which personal data have been input into

automated processing systems and when and by whom the personal data were input ('input control');

- h) ensure that the confidentiality and integrity of the data are protected when transmitting personal data and when transporting data media ('transport control');
- i) ensure that installed systems may, in the case of interruption, be restored ('recovery');
- k) ensure that the functions of the system perform without fault, that the appearance of faults in the functions is immediately reported (reliability);
- 1) ensure that stored personal data cannot be corrupted by system malfunctions (integrity);
- m) ensure that personal data which are being processed by a processor can only be processed according to the instructions by the controller (assignment control);
- n) ensure that personal data are protected against loss and destruction ('availability control');
- o) ensure that personal data collected for different purposes can be processed separately ('separability').
- 4) A purpose pursuant to paragraph 3 lett. b to f may especially be fulfilled using state of the art encryption techniques.

Article 64

Notifying the Data Protection Authority of a personal data breach

- 1) The controller shall, in the case of a personal data breach, notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Data Protection Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
- 2) A processor shall notify the controller without undue delay after becoming aware of a personal data breach.
- 3) The notification according to paragraph 1 shall contain at least the following information:
- a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned:
- b) the name and contact details of the data protection officer or other contact point where more information can be obtained;
- c) a description of the likely consequences of the personal data breach; and
- d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

- 4) If the information according to paragraph 3 cannot be provided at the same time with the notification, the controller shall submit said information as soon as it is available.
- 5) The controller shall document any personal data breaches. This documentation must include the facts relating to the personal data breach, its effects and the remedial action taken.
- 6) If the personal data breach involves personal data that have been transmitted by or to the controller of another EEA Member State, the information referred to in paragraph 3 shall be communicated to the controller of that Member State without undue delay.
- 7) Article 43 shall apply accordingly.
- 8) Additional obligations of the controller regarding notifications of personal data breaches shall remain unaffected.

Article 65

Notifying data subjects affected by a personal data breach

- 1) The controller shall, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, notify the data subjects of the personal data breach without undue delay.
- 2) The notification referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in Article 64 (3), (b), (c) and (d).
- 3) The notification according to paragraph 1 shall not be required if:
- a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize;
- (c) it would involve a disproportionate effort; in this case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.
- 4) If the controller has not communicated the personal data breach to the data subjects, the Data Protection Authority, having considered the likelihood of the personal data breach resulting in a high risk pursuant to paragraph 1, may decide that the conditions referred to in paragraph 3 have not been met.
- 5) The notification of data subjects pursuant to paragraph 1 may be delayed, restricted or omitted under the conditions referred to in Article 56 (2) unless the interests of the data subjects outweigh those of the controller owing to the high risk resulting from the personal data breach as referred to in paragraph 1.
- 6) Article 43 shall apply accordingly.

Article 66

Conducting a data protection impact assessment

- 1) Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of data subjects, the controller shall carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.
- 2) A joint assessment may address a set of similar processing operations that present similar high risks.
- 3) The controller shall involve the Data Protection Authority in carrying out the impact assessment.
- 4) The data protection impact assessment shall take into account the rights of the data subjects affected by the processing and shall contain at least the following:
- a) a systematic description of the envisaged processing operations and the purposes of the processing;
- b) an assessment of the necessity and proportionality of the processing operations in relation to their purpose;
- c) an assessment of the risks to the rights and freedoms of data subjects; and
- d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the law.
- 5) Where necessary, the controller shall carry out a review to assess whether processing is performed in accordance with the data protection impact assessment.

Article 67

Cooperation with the Data Protection Authority

The controller shall cooperate with the Data Protection Authority in the performance of his or her tasks.

Article 68

Consultation of the Data Protection Authority

- 1) The controller shall consult the Data Protection Authority prior to processing which will form part of a new filing system if:
- a) a data protection impact assessment as provided for in Article 66 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or
- b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

The Data Protection Authority may establish a list of the processing operations which are subject to prior consultation pursuant to sentence 1.

- 2) In cases of paragraph 1, the following shall be submitted to the Data Protection Authority:
- a) the data protection impact assessment pursuant to Article 66;
- b) where applicable, information on the respective responsibilities of the controller, joint controllers and processors involved in the processing;
- c) information on the purposes and means of the envisaged processing;
- d) information on the measures and safeguards intended to protect the legally protected interests of the data subjects; and
- e) name and contact details of the data protection officer.

Upon request, the Data Protection Authority shall be given any other information they require to assess the lawfulness of the processing and, in particular, the existing risks to the protection of the data subjects' personal data and the related safeguards.

- 3) If the Data Protection Authority believes that the planned processing would violate the law, in particular because the controller has not sufficiently identified the risk or has not taken sufficient measures to mitigate the risk, the Data Protection Authority may provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, as to which additional measures should be taken. The Data Protection Authority may extend this period by a month, if the planned processing is particularly complex. In this case, the Data Protection Authority shall inform the controller and, where applicable, the processor of the extension within one month of receipt of the request for consultation.
- 4) If the envisaged processing has substantial significance for the controller's performance of tasks and is therefore particularly urgent, the controller may initiate processing after the consultation has started but before the period referred to in paragraph 3, first sentence, has expired. In this case, the recommendations of the Data Protection Authority shall be taken into account after the fact, and the way the processing is carried out shall be adjusted where applicable.

Article 69

Records of processing activities

- 1) The controller shall maintain a record of all categories of processing activities under its responsibility. This record shall contain the following information:
- a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;
- b) the purposes of the processing;

- c) the categories of recipients to whom the personal data were or will be disclosed;
- d) a description of the categories of data subjects and of the categories of personal data;
- e) where applicable, the use of profiling;
- f) where applicable, the categories of transfers of personal data to a third country or an international organisation;
- g) details regarding the legal basis for the processing;
- h) the envisaged time limits for erasure or for a review of the need to store the various categories of personal data; and
- i) a general description of the technical and organisational security measures referred to in Article 63.
- 2) The processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
- a) the name and contact details of the processor, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;
- b) where applicable, transfers of personal data to bodies in a third country or to an international organization, including the identification of that third country or international organization; and
- c) a general description of the technical and organizational security measures according to Article 63.
- 3) The register according to paragraph 1 and paragraph 2 shall be in writing or electronically.
- 4) Controllers and processors shall make these records available to the Data Protection Authority upon request.

Article 70

Data protection by design and by default

1) The controller, both at the time the means of processing are determined and at the time of the processing itself, shall take appropriate measures to implement data protection principles, such as data minimization, in an effective manner, to ensure compliance with legal requirements and to protect the rights of data subjects. In doing so, the controller shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the legally protected interests of the data subject posed by the processing. In particular, personal data shall be processed, and processing systems shall be selected and designed in accordance with the aim of processing as few personal data as possible. Personal data shall be rendered anonymous or pseudonymised as early as possible, as far as this is possible in accordance with the purpose of processing.

2) The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. In particular, the measures must ensure that by default the data are not made accessible by automated means to an indefinite number of persons.

Article 71

Distinction between different categories of data subjects

The controller shall, where applicable and as far as possible, make a clear distinction between personal data of different categories of data subjects, such as:

- a) persons with regard to whom there are serious grounds for believing that they have committed a criminal offence;
- b) persons with regard to whom there are serious grounds for believing that they are about to commit a criminal offence;
- c) persons convicted of a criminal offence;
- d) victims of a criminal offence or persons with regard to whom certain facts give reasons for believing that they could be the victim of a criminal offence; and
- e) other persons, such as witnesses, persons who can provide information, or contacts or associates of the persons referred to in lett. a to d.

Article 72

Distinction between facts and personal assessments

In processing, the controller shall distinguish, as far as possible, personal data based on facts from personal data based on personal assessments. To this end, the controller shall identify evaluations based on personal assessments as such, as far as possible and reasonable in the context of the processing in question. It must also be possible to determine which body keeps the records on which an evaluation based on a personal assessment is based.

Article 73

Procedures for data transfers

1) The controller shall take appropriate measures to ensure that personal data which are inaccurate or no longer up to date are not transmitted or otherwise made available. To that end, the controller shall, as far as possible with reasonable effort, verify the quality of the data before they are transmitted or made available. The controller shall also, as far as possible and reasonable, in all transmissions of personal data include the necessary information to enable the recipient to assess the degree of accuracy, completeness and reliability of the data, and the extent to which they are up to date.

- 2) If the processing of personal data is subject to special conditions, in transmissions of data the transmitting body shall inform the recipient of these conditions and the requirement to respect them. The obligation of providing information may be met by marking the data accordingly.
- 3) The transmitting body shall not apply conditions to recipients in other EEA/Schengen Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the Treaty on the Functioning of the European Union other than those applicable to similar domestic transmissions.

Article 74

Rectification and erasure of personal data and restriction of processing

- 1) The controller shall rectify inaccurate personal data.
- 2) The controller shall erase personal data without delay if their processing is unlawful, they must be erased to comply with a legal obligation, or knowledge of the data is no longer necessary for the controller to perform his or her tasks.
- 3) Article 58 (3) and (4) apply accordingly. The recipient shall also be informed if inaccurate personal data have been transmitted, or if personal data have been transmitted unlawfully.
- 4) Without prejudice to any time limits for storing or erasing data defined in law, the controller shall provide for appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data and shall take procedural measures to ensure that these time limits are observed.

Article 75

Logging

| 1) Controllers and processor | s shall provide for | or logs to be l | kept for at leas | t the following pr | ocessing |
|------------------------------|---------------------|-----------------|------------------|--------------------|----------|
| operations in automated pro- | cessing systems: | | | | |

- a) collection;
- b) alteration;
- c) consultation;
- d) disclosure including transfers;
- e) combination, and
- f) erasure.
- 2) The logs of consultation and disclosure must make it possible to ascertain the justification, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed personal data, and the identity of the recipients of the data.

- 3) The logs shall be used solely by the data protection officer, the Data Protection Authority or the data subject to verify the lawfulness of the processing; and for self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.
- 4) The log data shall be erased at the end of the year following their generation.
- 5) The controller as well as the processor shall provide the records to the Data Protection Authority upon request.

Article 76

Confidential reports of violations

The controller shall make it possible to receive confidential reports of violations against data protection regulations which have occurred in his or her area of responsibility.

E. Transfer of data to third countries and international organizations

Article 77

General requirements

- 1) In addition to meeting the general requirements of data transfers, the transfer of personal data to bodies in third countries or international organisations shall be permitted if:
- a) the body or international organization is responsible for a purpose as set out in Article 45; and
- b) the European Commission has adopted an adequacy decision pursuant to Article 36 (3) of Directive (EU) 2016/680 which is applicable in the Principality of Liechtenstein.
- 2) Despite an adequacy decision pursuant to paragraph 1 lett. b and the according public interest for the transfer of data, that transfer of personal data shall be avoided if, on a case-by-case basis, the recipient cannot guarantee appropriate protection of the data according to basic fundamental rights or the legitimate interest of the data subject overrides the interest of the transfer. The controller shall base its assessment on whether the recipient in the individual case guarantees appropriate protection of the transferred data.
- 3) If personal data which have been transmitted or made available from another EEA/Schengen Member State are to be transferred pursuant to paragraph 1, the competent body of the other EEA/Schengen Member State shall provide prior authorization of the transfer. Transfers without the prior authorization shall be permitted only if the transfer is necessary to prevent an immediate and serious threat to the public security of a country or to essential interests of a EEA/Schengen Member State and the prior authorization cannot be obtained in time. In the case of the second sentence, the other EEA/Schengen Member State's body responsible for giving prior authorization shall be informed of the transfer without delay.
- 4) The controller who transfers data according to paragraph 1 shall take appropriate measures to ensure that the recipient forwards data to other third states or other international organizations only if the controller has given prior authorization. When deciding on the approval of such transfers, the controller

shall consider all relevant facts such as the seriousness of the criminal offence, the purpose of the initial transfer and the level of protection in the country or within the international organization to which the data are to be transferred onward. An authorization shall only be granted if a direct transfer to the third country or international organization would be permissible. The responsibility for granting an authorization may also be otherwise provided for.

Article 78

Transfers with appropriate safeguards

- 1) If contrary to Article 77 (1) lett. b) no decision is available pursuant to Article 36 (3) of Directive (EU) 2016/680, a transfer which meets the remaining requirements of Article 77 shall also be permitted if:
- a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or
- b) the controller has assessed all the circumstances surrounding the transfer and concludes that appropriate safeguards exist for the protection of personal data.
- 2) The controller shall record any transfer according to paragraph 1 lett. b. The documentation shall include the date and time of the transfer, the identity of the recipient, the reason for the transfer and the transferred personal data. This information shall be made available to the Data Protection Authority upon request.
- 3) At least once a year, the controller shall inform the Data Protection Authority regarding transfers which were made based on an assessment pursuant to paragraph 1 lett. b. In this information the controller may categorize the recipients and purposes of transfers accordingly.

Article 79

Transfers without appropriate safeguards

- 1) If contrary to Art. 77 (1) lett. b no decisions is available pursuant to Article 36 (3) of Directive (EU) 2016/680 and also no appropriate guarantees according to Article 78 (1) are available, a transfer meeting the requirements according to Article 77 shall be permitted if the transfer is required:
- a) for the protection of vital interests of a natural person;
- b) for the protection of legitimate interests of the data subject;
- c) for the prevention of an immediate and serious threat to the public security of a country;
- d) in particular cases, for the purposes mentioned in Article 45; or
- e) on a case-by-case basis, for the establishment, exercise or protection of legal claims in conjunction with the purposes as mentioned in Article 45.

- 2) The controller shall avoid the transfer according to paragraph 1 if the fundamental rights of a data subject override the public interest of the transfer.
- 3) For transfers pursuant to paragraph 1, Article 78 (2) shall apply accordingly.

Article 80

Other transfers to recipients in third countries

- 1) In special individual cases and if all other requirements for data transfers to third countries are met, controllers may transfer personal data directly to recipients in third countries not referred to Article 77 (1) lett. a if the transfer is strictly necessary for the performance of their tasks and:
- a) in a particular case, no fundamental rights of the data subject override the public interest in a transfer;
- b) the transfer to an authority or body mentioned in Article 77 (1) lett. a would be unsuitable or ineffective, especially if it could not be completed in time; and
- c) the controller notifies the recipient regarding the purposes of the processing and indicates that the transferred data are only to be transferred for the purposes that are required for the fulfillment of his or her tasks.
- 2) In cases according to paragraph 1, the controller shall notify the bodies or authorities mentioned in Article 77 (1) lett. a regarding the transfer unless this is ineffective or inappropriate.
- 3) For transfers according to paragraph 1, Article 78 (2) and (3) shall apply accordingly.
- 4) For transfers according to paragraph 1, the controller shall obligate the recipient to process the transferred personal data without the controller's consent only for the purpose for which they were transferred.
- 5) Agreements regarding judicial cooperation in criminal matters and the police cooperation shall remain unaffected.

F. Cooperation of supervisory authorities

Article 81

Mutual assistance

1) The Data Protection Authority shall transmit information to supervisory authorities in other EEA/Schengen member states and provide mutual assistance, as far as necessary for the consistent implementation and application of Directive (EU) 2016/680. The mutual assistance shall cover in particular requests of information and supervisory measures such as requests to carry out consultations, inspections and investigations.

- 2) The Data Protection Authority shall take all appropriate measures to comply with requests for mutual assistance requests without delay and no later than one month after receiving the request.
- 3) The Data Protection Authority may only deny requests for mutual assistance if:
- a) the Data Protection Authority is not competent for the subject matter or for the measures they are asked to take; or
- b) compliance with the request would violate the law.
- 4) The Data Protection Authority shall inform the requesting supervisory authority of the other EEA/Schengen member state of the results or, if applicable, the progress of further measures which have been taken to comply with the request for mutual assistance. In cases of paragraph 3, the Data Protection Authority shall state the reasons for the denial of the request.
- 5) The Data Protection Authority shall transfer information requested by the supervisory authority of another EEA/Schengen member state in general electronically or using another standardised format.
- 6) The Data Protection Authority shall handle requests for mutual assistance free of charge if no other agreement regarding the reimbursement of fees with the supervisory authority of the other EEA/Schengen member state was reached in advance.
- 7) Any request for mutual assistance by the Data Protection Authority shall contain all the necessary information such as the purpose and the reasons for the request. The information transferred shall only be used for the purpose for which it was requested.

G. Liability and penalties

Article 82

Compensation

- 1) If a controller has caused damages to a data subject by processing personal data in violation of this Act or other legal provisions regarding the processing of personal data, the controller or its legal entity shall be obligated to provide compensation to the data subject. The obligation to pay compensation shall not apply if, in the case of non-automated processing, the damage was not the result of fault by the controller.
- 2) The data subject may request appropriate financial compensation for non-material damage.
- 3) If it is not possible to determine who of multiple controllers has caused the damage in the course of an automatic processing, all the controllers or, if applicable, their legal entity shall be liable.
- 4) If a data subject has contributed to the occurrence of damages through culpable conduct, the provisions of §§ 1301 to 1304 of the Civil Code shall apply accordingly.
- 5) Claims for compensation come under the statute of limitations and are therefore time-barred no later than after three years after the day on which the damaged party became aware of the damage.

Article 83

Penal provisions

Articles 41 and 42 shall apply accordingly to the processing of personal data by public authorities in the course of their tasks pursuant to Article 45, sentences 1, 3 or 4.

IV. Special provisions for the processing in the course of tasks which are not subject to Regulation (EU) 2016/679 and Directive (EU) 2016/680

Article 84

Special provisions for the processing in the course of tasks which are not subject to Regulation (EU) 2016/679 and Directive (EU) 2016/680

- 1) The transfer of personal data to a third country or supra- or international organizations in the course of tasks which are not subject to Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall be permitted in addition to the cases permitted under Regulation (EU) 2016/679 if the transfer is necessary for the fulfillment of tasks for the protection or the fulfillment of obligations of the state in crisis management or conflict prevention or for humanitarian measures. The recipient shall be notified that the transferred data shall only be used for the purposes for which they were transferred.
- 2) Article 17 (4) shall not apply to the processing by the National Police if the processing relates to tasks that are not subject to Regulation (EU) 2016/679 and Directive (EU) 2016/680, if the government determines on a case-by-case basis that the fulfillment of the obligations mentioned in that provision would endanger the security of the country.
- 3) Processing by public bodies in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall not be subject to the obligation to provide information in accordance with Article 13 (1) and (2) of Regulation (EU) 2016/679 if:
- a) it concerns cases according to Article 32 (1) lett. a to c; or
- b) by fulfilling the request, information would be disclosed which is protected by law or is to be kept secret due to the overriding legitimate interests of a third person and therefore the interest of the data subject in receiving the requested information must stand back.
- 4) If the data subject is not to be informed in the cases of paragraph 3, no right of access shall apply. Article 32 (2) and Article 33 (2) shall not apply.

V. Transitional and final provisions

Article 85

Implementing provisions

The government shall enact the required ordinances for the implementation of this Act, in particular regarding:

- a) the requirements under which a public body shall be allowed to have personal data processed by third parties or process personal data on behalf of third parties;
- b) the notification of video surveillance according to Article 5;
- c) the adequacy decisions issued by the EU Commission pursuant to Article 45 of Regulation (EU) 2016/679 and the standard data protection clauses adopted by the EU Commission pursuant to Article 46 of Regulation (EU) 2016/679 which shall apply to the Principality of Liechtenstein;
- d) the fees for official acts of the Data Protection Authority.

Article 86

Repeal of current legislation

The Data Protection Act ("DSG") dated March 14, 2002, LGBI. 2002 No. 55, in its current version, is repealed.

Article 87

Data Protection Officer and other personnel

The Data Protection Officer who was elected under the previous law shall assume the position of head of the Data Protection Authority after this Act comes into force (Article 12) and shall carry out his or her functions pursuant to the provisions of the new law until December 31, 2025. The consisting employment relationships of other personnel of the Data Protection Authority shall remain in force.

Article 88

Data Protection Commission

- 1) With the entry into force of this Act, the mandate and term of office of the current Data Protection Commission ends.
- 2) The complaints procedures or procedures in conjunction with recommendations of the Data Protection Authority that are pending with the Data Protection Commission at the time this Act enters into force shall be handled under the previous law.

Article 89

Video surveillance

- 1) All approvals of video surveillance systems that were granted according to the previous law shall remain in force until the expiration of the approval.
- 2) If it is intended to maintain the video surveillance after the expiration of the approval, a notification according to Article 5 (7) shall be made.

Article 90

Accreditations and certifications

All granted accreditations and certifications shall remain in force until the date of their expiry. For all pending accreditation and certification procedures at the time this Act enters into force, the previous law is applicable.

Article 91

Entry into force

This Act shall enter into force on January 1, 2019, with reservation to the idle expiration of the referendum deadline, otherwise on the day after its announcement.

In representation of the Prince Regnant

sig. Alois

Hereditary Prince

sig. Adrian Hasler

Prime Minister of the Principality of Liechtenstein

1. Report and proposal as well as statement of the government No. 36/2018 and 69/2018