Translation of Liechtenstein Law

Disclaimer

English is not an official language of the Principality of Liechtenstein. This translation is provided for information purposes only and has no legal force. The contents of this website have been compiled with utmost care and to the best of knowledge. However, the supplier of this website cannot assume any liability for the currency, completeness or accuracy of any of the provided pages and contents.

English title:	Data Protection Act (DSG) of 4 October 2018
Original German title:	Datenschutzgesetz (DSG) vom 4. Oktober 2018
Serial number (LR-Nr.):	235.1
First published:	4 October 2018
First publication no. (LGBl-Nr.):	2018-272
Last change date:	1 January 2021
Data of last amendment – publication no. (LGBl-Nr.):	2020-389
Translation date:	3 February 2021

Liechtenstein Law Gazette
Year 2018 No. 272 published on 7 December 2018

Data Protection Act (DSG)

of 4 October 2018

I hereby grant My consent to the following resolution adopted by Parliament:[1]

I. General provisions

A. Purpose, scope of application, and terminology

Article 1

Purpose

1) The purpose of this Act shall be to protect the personality and fundamental rights of natural persons with regard to the processing of their personal data.

2) It shall also serve:

a) to execute 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) (OJ L 119, 4.5.2016, 1);

b) to implement 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

1 Report and Motion of the Government No. 36/2018, Statement of the Government No. 69/2018

repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, 89).

3) The version in force of the enactments referred to in paragraph 2 results from the promulgation of the Decisions of the EEA Joint Committee and the international treaties developing the Schengen acquis in the Liechtenstein Law Gazette pursuant to Article 3(c) and (k) of the Promulgation Act.

Article 2

Scope of application

1) This Act applies to the processing of personal data by public bodies. For private bodies, this Act applies to the processing of personal data wholly or partly by automatic 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, unless the processing is carried out by a natural person in the course of a purely personal or household activity.

2) Special legal provisions on data protection take precedence over the provisions of this Act. If they do not govern or do not conclusively govern a matter to which this Act applies, the provisions of this Act shall apply in a subsidiary manner. The obligation to maintain obligations of confidentiality or professional or official secrecy remains unaffected.

3) This Act applies to public bodies. It applies to private bodies, provided:

a) the controller or processor processes personal data in Liechtenstein;

b) the processing of personal data is carried out in the course of the activities of a domestic establishment of the controller or processor; or

c) the controller or processor does not have an establishment in an EEA Member State, but falls within the scope of Regulation (EU) 2016/679.

If this law does not apply pursuant to the second sentence, only Articles 9 to 20 and 39 to 44 shall apply to the controller or processor.

4) For processing of personal data by public bodies in the context of activities not covered by Regulation (EU) 2016/679 and Directive (EU) 2016/680, Regulation (EU) 2016/679 and Chapters I and II of this Act shall apply *mutatis mutandis*, unless otherwise provided for in this Act or in another law.

5) This Act shall not apply to:

a) deliberations in Parliament and in committees of Parliament or in the Judicial Selection Commission;

b) pending civil proceedings and administrative appeals;

c) pending proceedings before the Constitutional Court;

d) the activities of the National Audit Office.

6) This Act is not applicable to the extent that EEA law, in particular Regulation (EU) 2016/679, is directly applicable.

Article 3

Definition and terminology

1) For the purposes of this Act, the following terms shall have the following meanings:

a) "public bodies":

1. the bodies of the State, the municipalities and corporate bodies, foundations, and institutions under public law;

2. private bodies, to the extent that they are acting in the performance of public responsibilities delegated to them;

b) "private bodies":

1. natural and legal persons as well as partnerships with legal capacity subject to private law, unless they fall under subparagraph (a)(2);

2. public bodies under subparagraph (a)(1) where they act in the private sector.

2) The terms used in this Act to denote persons and functions include persons of male and female gender alike.

B. Legal bases for the processing of personal data

Article 4

Processing of personal data by public bodies

Public bodies shall be permitted to process personal data if such processing is necessary to perform the task for which the controller is responsible or to exercise official authority which has been vested in the controller.

Article 5

Video surveillance of publicly accessible areas

1) Monitoring publicly accessible areas with optical-electronic devices (video surveillance) shall be permitted only as far as:

a) 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) For video surveillance of the following facilities, protecting the lives, health and freedom of persons present shall be regarded as a very important interest:

a) large publicly accessible facilities, such as sport facilities, places of gathering and entertainment, shopping centres and car parks; or

b) vehicles and large publicly accessible public transport facilities.

3) Appropriate measures shall be taken to make the surveillance and the controller's name and contact details identifiable as early as possible.

4) Storing or using data collected pursuant to paragraphs 1 and 2 shall be permitted if necessary to achieve the intended purpose and if there is nothing to indicate legitimate overriding interests of the data subjects. Paragraph 2 shall apply *mutatis mutandis*. The data may be further processed for another purpose only if necessary to prevent threats to state and public security, to defend against threats to life, limb, freedom, or property, to prosecute criminal offences, or to secure evidence; in the latter cases, the National Police may demand transmission of the data collected.

5) If data collected from video surveillance are attributed to a particular person, that person shall be informed of the processing in accordance with Articles 13 and 14 of Regulation (EU) 2016/679. Article 32 shall apply *mutatis mutandis*.

6) The data shall be deleted without delay, 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 must be notified to the Data Protection Authority before it is put into operation. Real-time image transmissions without the possibility of recording or other further processing are excluded from notification. The Government shall provide further details by ordinance.

8) Anyone who wilfully violates the reporting obligation under paragraph 7 shall be fined by the Data Protection Authority for a contravention with a fine of up to CHF 5 000. Article 40(3) to (6) shall apply *mutatis mutandis*.

C. Data protection officers of public bodies

Article 6

Designation

1) Public bodies shall designate a data protection officer. This shall also apply to public bodies as defined in Article 3(1)(b)(2) which act in the private sector.

2) A single data protection officer may be designated for several public bodies, taking account of their organisational structure and size.

3) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data

protection law and practices and the ability to fulfil the tasks referred to in Article 8.

4) The data protection officer may be a staff member of the public body, or fulfil the tasks on the basis of a service contract.

5) The public body shall publish the contact details of the data protection officer and communicate them to the Data Protection Authority.

Article 7

Position

1) The public body shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2) The public body shall support the data protection officer in performing the tasks referred to in Article 8 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain expert knowledge.

3) The public body shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. The data protection officer shall directly report to the management of the public body. The data protection officer shall not be dismissed or penalised by the public body for performing the data protection officer's tasks.

4) The dismissal of the data protection officer shall be permitted only by applying Article 24 of the State Employee Act *mutatis mutandis*.

5) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under Regulation (EU) 2016/679, this Act and other data protection provisions. The data protection officer shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless the data protection officer is released from this obligation by the data subject.

6) Where in the course of their activities data protection officers become aware of data for which the head of a public body or a person employed by such a body has the right to refuse to give evidence for employment-related reasons, this right shall also apply to the data protection officer and the data protection officer's assistants. 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, the data protection officer's files and other documents shall not be subject to seizure.

Article 8

Tasks

1) In addition to the tasks listed in Regulation (EU) 2016/679, the data protection officer shall have at least the following tasks:

a) to inform and advise the public body and the employees who carry out processing of their obligations pursuant to this Act and other data protection provisions, including legislation enacted to implement Directive (EU) 2016/680;

b) to monitor compliance with this Act and other data protection provisions, including legislation enacted to implement Directive (EU) 2016/680, and with the policies of the public body in relation to 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) to provide advice as regards the data protection impact assessment and monitor its implementation pursuant to Article 66;

d) to cooperate with the Data Protection Authority;

e) to act as the contact point for the Data Protection Authority on issues relating to processing, including the prior consultation referred to in Article 68, and to consult, where appropriate, with regard to any other matter.

2) In the case of a data protection officer ordered by a court, the tasks referred to in paragraph 1 shall not refer to the action of the court acting in its judicial capacity.

3) The data protection officer may perform other tasks and duties. The public body shall ensure that any such tasks and duties do not result in a conflict of interests.

4) The data protection officer shall in the performance of the data protection officer's 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 organisation

1) The Data Protection Authority is the national supervisory authority in accordance with Article 51 of Regulation (EU) 2016/679 and Article 41 of Directive (EU) 2016/680.

2) The Data Protection Authority shall be composed of the director of the Data Protection Authority and other employees.

3) Unless otherwise provided by Regulation (EU) 2016/679 or this Act, the State Employee Act shall apply *mutatis mutandis* to the employment relationship of the director of the Data Protection Authority and the other employees of the Data Protection Authority.

Article 10

Competence

1) The Data Protection Authority shall be competent to supervise processing operations of public bodies and private bodies.

2) The Data Protection Authority shall not be competent to supervise:

a) processing operations of the Government acting in its capacity;

b) processing operations of the courts acting in their judicial capacity.

Article 11

Independence

1) The Data Protection Authority shall act with complete independence in performing its tasks and exercising its powers. The Data Protection Authority shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

2) The Data Protection Authority shall be subject to audit by the National Audit Office in accordance with the National Audit Act.

Establishment and termination of employment relationships

Article 12

a) Director of the Data Protection Authority

1) Parliament elects the director of the Data Protection Authority for a period of six years on a proposal from the Government. Re-election is possible.

2) If the employment relationship ends upon expiry of the contract period, the Government may, in justified cases, extend the employment relationship for up to six months until a successor is appointed.

3) The employment relationship of the director of the Data Protection Authority shall end upon expiry of the contract period, subject to paragraph 4.

4) The employment relationship of the director of the Data Protection Authority may be terminated or dissolved by the Government only if:

a) the director is unable to carry out the director's responsibilities due to illness or accident; or

b) there is an important reason for termination without notice.

Article 13

b) Other employees of the Data Protection Authority

1) The other employees of the Data Protection Authority shall be appointed by the Government on a proposal from the director of the Data Protection Authority.

2) Provisions on transfer and termination of the employment relationship under Articles 16 and 18 to 27 of the State Employees Act shall apply to the other employees of the Data Protection Authority, with the proviso that transfer or termination of the employment relationship by the Government shall require a request to that effect by the director of the Data Protection Authority.

Article 14

Rights and obligations

1) The director of the Data Protection Authority shall refrain from any action incompatible with the director's duties and shall not, during the term of office, engage in any incompatible occupation, whether gainful or not. The director of the Data Protection Authority may not be a member of Parliament, the Government, a court, or an administrative authority, nor may the director exercise the function of a mayor or a member of a Liechtenstein municipal council. Upon appointment, the director shall no longer perform such offices. The director may not deliver extrajudicial opinions in exchange for payment.

2) The Director of the Data Protection Authority shall have the right to refuse to give testimony concerning persons who have confided in the director in the capacity as director of the Data Protection Authority and concerning the information confided. This shall also apply to the other employees of the Data Protection Authority, on the condition that the director of the Data Protection Authority decides on the exercise of this right. Within the scope of the director of the Data Protection Authority's right of refusal to give testimony, the director shall not be required to submit or surrender files or other documents.

3) Even after the employment relationship has ended, the director of the Data Protection Authority shall be obligated to secrecy concerning matters of which the director has become aware in the performance of responsibilities. 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 director of the Data Protection Authority shall have the due discretion to decide whether and to what extent to testify in or outside court or to make statements concerning such matters; if the director is no longer in office, the permission of the director of the Data Protection Authority in office shall be required. This shall not affect the legal obligation to report criminal offences.

4) Articles 84 and 85 of the Tax Act shall not apply to the director of the Data Protection Authority or to the other employees of the Data Protection Authority. This shall not apply where the fiscal authorities require such knowledge in order to conduct legal proceedings due to a tax offence and related tax proceedings, in the prosecution of which there is compelling public interest, or where the person required to provide information or persons acting on such a person's behalf have intentionally provided false information. If the director of the Data Protection Authority determines that data protection provisions have

been violated, the director shall be authorised to report the violation and inform the data subject accordingly.

5) The director of the Data Protection Authority may testify as a witness unless such testimony would:

a) be detrimental to the welfare of the country, in particular to the security or relations with other countries, or

b) would violate fundamental rights.

6) If the testimony referred to in paragraph 5 concerns ongoing or completed processes for which the Government is or could be responsible, the director of the Data Protection Authority may testify only with the approval of the Government. The Government may deny approval only if the welfare of the country so requires.

7) The director of the Data Protection Authority shall issue organisational regulations to be brought to the attention of the Government.

Article 15

Tasks

1) In addition to the tasks listed in Regulation (EU) 2016/679, the Data Protection Authority shall have the following tasks:

a) to monitor and enforce the application of this Act and other data protection provisions, including legislation adopted to implement Directive (EU) 2016/680;

b) to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, paying special attention to measures specifically for children;

c) to advise 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 the processing of personal data;

d) to promote the awareness of controllers and processors of their obligations under this Act and other data protection provisions, including legislation adopted to implement Directive (EU) 2016/680;

e) upon request, to provide information to any data subject concerning the exercise of their rights under this Act and other data protection provisions, including legislation adopted to implement Directive (EU) 2016/680, and if appropriate, to cooperate with the supervisory authorities in other Member States to that end;

f) to handle complaints lodged by a data subject, or by a body, organisation 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 Data Protection Authority is necessary;

g) to cooperate with, including by sharing information, and provide administrative assistance to other supervisory authorities, to ensure the consistency of application and enforcement of this Act and other data protection provisions, including legislation adopted to implement Directive (EU) 2016/680;

h) to conduct investigations on the application of this Act and other data protection provisions, including legislation adopted to implement Directive (EU) 2016/680, also on the basis of information received from another Data Protection Authority or other public authority;

i) to 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) to provide advice on the processing operations referred to in Article 68; and

l) to contribute to the activities of the European Data Protection Board.

2) Within the scope of Directive (EU) 2016/680, the Data Protection Authority shall also perform the task pursuant to Article 60.

3) To carry out the task listed in paragraph 1(c), the Data Protection Authority may, on request or at its own initiative, make recommendations to Parliament or one of its committees, the Government, and other institutions and bodies concerning all matters related to the protection of personal data. At the request of Parliament, one of its committees, 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(f) by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

5) The performance of the duties of the Data Protection Authority shall be free of charge for the data subject. Where requests are manifestly

unfounded or excessive, in particular because of their repetitive character, the Data Protection Authority may charge a reasonable fee based on effort, or refuse to act on the request. The Data Protection Authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. The Government shall provide further details concerning the fee by ordinance.

Article 16

Activity report

The Data Protection Authority shall produce an annual activity report which may contain a list of the types of violations reported and the types of measures taken, including penalties and measures taken in accordance with Article 58(2) of Regulation (EU) 2016/679. The Data Protection Authority shall submit this report for the attention of Parliament and the Government and shall make it available to the public, the European Data Protection Board, and the EFTA Surveillance Authority.

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 data protection provisions have been violated or that there are other problems with the processing of personal data, it shall inform the competent specific supervisory authority and, before exercising the powers referred to in Article 58(2)(b) to (g), (i), and (j) of Regulation (EU) 2016/679, shall give this authority the opportunity to provide its opinion to the controller within a reasonable period. The opportunity to provide an opinion may be dispensed with if an immediate decision seems necessary due to imminent danger or in the public interest, or if it would conflict with compelling public interests. The opinion should also include a description of the measures taken on the basis of the information from the Data Protection Authority.

2) If the Data Protection Authority finds that, in data processing for purposes beyond the scope of Regulation (EU) 2016/679, private bodies or public bodies have violated this Act or other data protection provisions or there are other insufficiencies with their processing or use of personal data, the Data Protection Authority shall lodge a complaint

with the controller. In the case of a public body, the Data Protection Authority shall additionally inform the Government of the complaint. The Data Protection Authority shall give the controller, and in the case of a public body also the Government, the opportunity to respond within a reasonable period to be determined by the Data Protection Authority. The Data Protection Authority may dispense with a complaint or a response, especially if the problems involved are insignificant or have been remedied in the meantime. The response should also describe the measures taken as a result of the Data Protection Authority's complaint. The Data Protection Authority may also warn a controller that intended processing operations are likely to violate provisions of this Act and other data protection provisions which apply to the data processing in question.

3) The powers of the Data Protection Authority shall also extend to:

a) personal data obtained by public or private bodies concerning the contents of and specific circumstances relating to postal communications and telecommunications, and

b) personal data that is subject to official secrecy, especially tax secrecy under Article 83 of the Tax Act.

4) The public or private bodies shall be obligated to provide the Data Protection Authority and all persons mandated by the Data Protection Authority to monitor compliance with data protection provisions with the following:

a) after notification by the Data Protection Authority or its mandated person, access to all property and premises, including to any data processing equipment and means, and to all personal data and all information necessary to perform their tasks; and

b) all information necessary to perform their tasks. In the case of private bodies, the party required to provide information may refuse if providing the information would expose itself or one of the relatives referred to in § 108(1) of the Code of Criminal Procedure to the risk of criminal prosecution. The party required to provide information must be informed of this possibility.

5) The inspection activities referred to in paragraph 4 must be performed with the greatest possible preservation of the rights of the public and private bodies and third parties.

6) The Data Protection Authority shall advise and support the data protection officers to meet their typical needs. It may demand the dismissal of a data protection officer if the officer does not have the expert knowledge needed to perform the 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 may process the data it has stored only for purposes of supervision; to this end, it may transfer data to other supervisory authorities. Processing for another purpose shall be permitted in addition to Article 6(4) of Regulation (EU) 2016/679 if:

a) it is obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if the data subject were aware of the other purpose;

b) 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

c) processing is necessary to prosecute criminal offences, to carry out or enforce punishment or measures under the Criminal Code or educational or other measures as referred to in the Juvenile Court Act or to enforce 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 shall represent Liechtenstein on the European Data Protection Board.

Article 19

Cooperation with other supervisory authorities

Before submitting a position to the supervisory authorities of other EEA Member States, the EFTA Surveillance Authority, or the European Data Protection Board, the Data Protection Authority shall involve other national supervisory authorities in accordance with Articles 85 and 91 of Regulation (EU) 2016/679, provided they are affected by the matter.

F. Legal protection

Article 20

Appeals

1) Decisions and decrees of the Data Protection Authority may be appealed by way of a complaint to the Complaints Commission for Administrative Matters within four weeks of service.

2) Decisions and decrees of the Complaints Commission for Administrative Matters may be appealed by way of complaint to the Administrative Court within four weeks; the Data Protection Authority may also exercise this right.

3) The Data Protection Authority may not deprive a public body of the suspensive effect of decisions and decrees.

II. Implementing provisions for processing 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 as referred to in Article 9(1) of Regulation (EU) 2016/679 shall be permitted:

a) by public and private bodies if:

1. processing is necessary to exercise the rights derived from the right of social security and social protection and to meet the related obligations;
2. 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 the data subject's contract with a health professional and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision; or

3. 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 referred to in paragraph 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with;

b) by public bodies if:

1. processing is urgently necessary for reasons of a prevailing public interest;
2. processing is necessary to prevent a substantial threat to public security;
3. processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; or
4. processing is necessary for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body of the State in the field of crisis management or conflict prevention or for humanitarian measures

and as far as the interests of the controller in data processing in the cases of subparagraph (b) outweigh the interests of the data subject.

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 organisational 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) restrictions on access to personal data within the controller and by processors;

f) the pseudonymisation of personal data;

g) the encryption of personal data;

h) measures to ensure the ability, confidentiality, integrity, availability and resilience of processing 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 organisational measures for ensuring the security of the processing; or

k) specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes.

Article 22

Processing for other purposes by public bodies

1) Public bodies shall be permitted to 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 obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if the data subject were aware of the other purpose;

b) it is necessary to check information provided by the data subject because there is reason to believe that this information is incorrect;

c) processing is necessary to prevent substantial harm to the common good or a threat to public security, defence or national security; to safeguard substantial concerns of the common good; or to ensure tax and customs revenues;

d) processing is necessary to prosecute criminal offences, to carry out or enforce punishment or measures under the Criminal Code, or educational or other measures as referred to in the Juvenile Court Act or to enforce 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 organisational analyses of the controller; this shall also apply to processing for training and

examination purposes by the controller, as long as it does not conflict with the legitimate interests of the data subject.

2) The processing of special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted if the conditions of paragraph 1 are met and an exception pursuant to Article 9(2) of Regulation (EU) 2016/679 or pursuant to Article 21 applies.

Article 23

Processing for other purposes by private bodies

1) Private bodies shall be permitted to 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 to prosecute 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 as referred to in Article 9(1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted if the conditions of paragraph 1 are met and an exception pursuant to Article 9(2) of Regulation (EU) 2016/679 or pursuant to 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 to whom the data are transferred to perform their duties and the conditions are met which would permit processing pursuant to Article 22. The third party to whom the data are transferred shall process the transferred data only for the purpose for which they were transferred. Processing for other purposes shall be permitted only if the conditions of Article 22 are met.

2) Public bodies shall be permitted to transfer personal data to private bodies if:

a) transfer is necessary for the transferring body to perform its duties and the conditions are met which would permit processing pursuant to Article 22;

b) the third party to whom the data are transferred credibly presents 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) processing is necessary for the establishment, exercise or defence of legal claims

and the third party has promised the public body transferring the data that it will process them only for the purpose for which they were transferred. Processing for other purposes shall be permitted if transfer pursuant to the first sentence would be permitted and the transferring body has consented to the transfer.

3) The transfer of special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679 shall be permitted if the conditions of paragraphs 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

Limitations of the right to information for journalists

1) If personal data are processed solely for publication in the editorial section of a periodically appearing medium, the controller may refuse, limit, or defer the provision of information under Article 15 of Regulation (EU) 2016/679 if:

a) the personal data reveals the sources of the information;

b) access to the drafts of publications would have to be given; or

c) the freedom of the public to form its opinion would be prejudiced.

2) Journalists may also refuse, limit, or defer the provision of information under 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

Anyone who processes data or has data processed must keep data from processing operations entrusted to them or made accessible to them based on their professional activities secret, notwithstanding other legal confidentiality obligations, unless lawful grounds exist for the disclosure of the data entrusted or made accessible to them.

Article 27

Data processing 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 as referred to in Article 9(1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research purposes or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with the second sentence of Article 21(2).

2) For scientific or historical research or statistical purposes in the public interest, the controller may process all personal data not covered by the first sentence of paragraph 1 if the processing is necessary for these purposes and if:

a) the data are publicly available;

b) the data for the controller are pseudonymised personal data and the controller cannot determine the identity of the data subject by legally permissible means; or

c) obtaining the consent of the data subject is impossible because the data subject is unreachable or would otherwise involve a disproportionate effort.

The second sentence of paragraph 1 shall apply *mutatis mutandis*. Article 4 shall remain unaffected.

3) The provisions of paragraphs 1 and 2 shall also apply to personal data which the controller has permissibly collected for other investigations or for other purposes.

4) The rights of data subjects provided in 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 fulfilment of the research or statistical purposes. Further, the right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the data are necessary for purposes of scientific research and the provision of information would involve disproportionate effort.

5) In addition to the measures listed in Article 21(2), personal data processed for scientific or historical research purposes or statistical purposes shall be rendered anonymous as soon as the research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject. Until such time, 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 publish personal data only if the data subject has provided consent or if doing so is indispensable for the presentation of research findings.

Article 28

Data processing for purposes of research into persons, families, and genealogies, as well as the keeping and publication of family chronicles and biographies

The processing of personal data is permissible even without the consent of the data subject for purposes of research into persons, families, and genealogies, as well as the keeping and publication of family chronicles and biographies if the processing is necessary for these purposes. Insofar as the processing involves special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679, such processing is permissible by derogation from Article 9(1) of Regulation (EU) 2016/679 if it is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data

subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with the second sentence of Article 21(2).

Article 29

Data processing 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 as referred to in 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 the second sentence of Article 21(2).

2) For archiving purposes in the public interest not aiming to achieve results relating to personal data, the controller may process all personal data not covered by the first sentence of paragraph 1 if the processing is necessary for these purposes and if:

a) the data are publicly available;

b) the data for the controller are pseudonymised personal data and the controller cannot determine the identity of the data subject by legally permissible means; or

c) obtaining the consent of the data subject is impossible because the data subject is unreachable or would otherwise involve a disproportionate effort.

The second sentence of paragraph 1 shall apply *mutatis mutandis*. Article 4 shall remain unaffected.

3) The provisions of paragraphs 1 and 2 shall also apply to personal data which the controller has permissibly collected for other investigations or for other purposes.

4) The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the archival material is not identified with 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 of the data subject to rectification according 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, the data subject shall have the opportunity to present their version. The responsible archive shall be obligated to add this version to the files.

6) The rights provided in Article 18(1)(a), (b) and (d) and in Articles 20 and 21 of Regulation (EU) 2016/679 shall not apply as far as 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 fulfil those purposes.

Article 30

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

1) For the rights of data subjects under Article 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 provide information to the data subject according to Article 14(1) to (4) of Regulation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose information which:
   1. is subject to a legal secrecy obligation; 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 according to Article 15 of Regulation (EU) 2016/679 shall not apply as far as access would disclose information which:
   1. is subject to a legal secrecy obligation; 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 a legal secrecy obligation; or
   2. by its nature must be kept secret, in particular because of overriding legitimate interests of a third party;

By derogation from the exception pursuant to subparagraph (c)(2), the data subject pursuant to Article 34 of Regulation (EU) 2016/679 shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

2) If in the context of a client-lawyer relationship the data of third persons are transferred to persons subject to a legal obligation of professional secrecy, the transferring body shall not be obligated to inform the data subject according to Article 13(3) of Regulation (EU) 2016/679 unless the data subject has an overriding interest in being informed.

3) The Data Protection Authority shall not have the investigative powers according to Article 58(1)(e) and (f) of Regulation (EU) 2016/679 with regard to the persons listed in § 121(1), (3) and (4) of the Criminal Code or their processors as far as exercising these powers would violate these persons' obligations to secrecy. If in the context of an investigation a Data Protection Authority becomes aware of data that are subject to an obligation of secrecy as referred to in the first sentence, 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 have been followed;

b) the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognised mathematic-statistical procedure;

c) other data in addition to address data are used to calculate the probability value; and

d) if address data are used, the data subject was notified ahead of time of the planned 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:

a) which have been established by an execution deed pursuant to Article 1 of the Execution Act;

b) which have been established pursuant to Article 66 of the Insolvency Act and have not been contested by the debtor at the examination hearing;[1]

c) which the debtor has explicitly acknowledged;

d) for which:

1. the debtor has received at least two written reminders after the due date of the claim;
2. at least four weeks have elapsed since the first reminder;
3. the debtor was previously informed, at least in the first reminder, of possible consideration by a credit reporting agency; 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 for payment in arrears and the debtor has been informed of possible consideration by a credit reporting agency.

3) The lawfulness of processing, including the calculation of probability values, other data relevant for credit reports pursuant to general data protection law shall remain unaffected.

B. Rights of the data subject

Article 32

Information to be provided where personal data are collected from the data subject

1) In addition to the exception in Article 13(4) of Regulation (EU) 2016/679, the obligation to provide information to the data subject according to Article 13(3) of Regulation (EU) 2016/679 shall not apply if providing information about the planned further use:

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 compatible with the original 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 receiving the information can be regarded as minimal, given the

1 Article 31(2)(b) amended by LGBl. 2020 No. 389.

circumstances of the individual case, in particular with regard to the context in which the data were collected;

b) would, in the case of a public body, endanger the proper performance of tasks as referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, and the controller's interests in not providing the information outweigh the interests of the data subject;

c) would endanger public security or order or would otherwise be 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 interfere with the establishment, exercise 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 endanger a confidential transfer of data 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 providing the information referred to in Article 13(1) and (2) of Regulation (EU) 2016/679 for the public in precise, transparent, understandable and easily accessible form in clear and simple language. The controller shall set down in writing the reasons for not providing information. The first and second sentences shall not apply in the cases of paragraph 1(d) and (e).

3) If notification is not provided in the cases of paragraph 1 because of a temporary obstacle, the controller shall meet the obligation to provide information, while taking into account the specific circumstances of processing, within an appropriate period after the obstacle has ceased to exist, but no later than two weeks.

Article 33

Information to be provided where personal data have not been obtained from the data subject

1) In addition to the exception in Article 14(5) of Regulation (EU) 2016/679 and in Article 30(1)(a), the obligation to provide information to the data subject according to Article 14(1), (2) and (4) of Regulation (EU) 2016/679 shall not apply if providing information:

a) in the case of a public body:

1. would endanger the proper performance of tasks as referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible; or
2. would threaten the public security or order or otherwise be detrimental to the State

and therefore the data subject's interest in receiving the information must not take precedence;

b) in the case of a private body:

1. would interfere with the establishment, exercise or defence of civil claims, or 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 disclosing the data would endanger public security or order or would otherwise be detrimental to the welfare of the State; in the case of data processing for purposes of criminal prosecution, no determination pursuant to the first half-sentence shall be 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 providing the information referred to in Article 14(1) and (2) of Regulation (EU) 2016/679 for the public in precise, transparent, understandable and easily accessible form in clear and simple language. The controller shall set down in writing the reasons for not providing information.

3) If the provision of information relates to the transfer by public bodies of personal data to the National Police for the performance of its duties relating to State security, such provision shall be permitted only with 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)(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)(a), 33(1)(b)(2), or 33(3); or

b) the data:

1. were recorded only because they may not be erased due to legal or statutory provisions on retention; or
2. only serve purposes of monitoring data protection or safeguarding data

and providing information would require a disproportionate effort, and appropriate technical and organisational measures make processing for other purposes impossible.

2) The reasons for the refusal to provide information shall be documented. The data subject shall be informed of the reasons for refusing to provide information, unless providing the reasons 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 a data subject, such information shall be provided to the Data Protection Authority at the request of the data subject, unless the Government determines in the individual case that doing so would endanger the security of the State. The notification from the Data Protection Authority to the data subject with 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 to information about personal data processed by a public body neither in automated nor in non-automated form and 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 non-automated or 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 given 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, the first and second sentences of paragraph 1 shall apply *mutatis mutandis* 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)(b) of Regulation (EU) 2016/679, paragraph 1 shall apply *mutatis mutandis* in the case of Article 17(1)(a) of Regulation (EU) 2016/679 if erasure would conflict with retention periods set by statute or contract.

Article 36

Right to object

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

Article 37

Automated individual decision-making, including profiling

1) In addition to the exceptions given in Article 22(2)(a) and (c) of Regulation (EU) 2016/679, the right according to Article 22(1) of Regulation (EU) 2016/679 not to be subject to a decision based solely on automated processing shall not apply if the decision is made in the context of:

a) providing services pursuant to an insurance contract and
   1. determining 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) performance of due diligence when establishing a business relationship, risk-appropriate monitoring of the business relations, and risk assessment in accordance with Articles 5, 9, and 9a of the Due Diligence Act;

c) lending in accordance with Article 3(3)(b) of the Banking Act; or

d) the provision of investment services or ancillary services in accordance with Article 3(4) of the Banking Act or Article 3 of the Asset Management Act.

2) With the exception of paragraph 1(a)(2) and 1(b), the controller shall take suitable measures to safeguard the data subject's legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their 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 adversely affected by the automated decision.

3) Decisions pursuant to paragraph 1(a) may be based on the processing of health data as referred to in Article 4(15) of Regulation (EU) 2016/679. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with the second sentence of Article 21(2).

C. Obligations of controllers and processors

Article 38

Data protection officers of private bodies

1) If the designation of a data protection officer is mandatory for private bodies, the dismissal of the data protection officer is permissible only under the conditions of the labour law provisions on termination without notice on important grounds pursuant to § 1173a, Article 53 of the General Civil Code (ABGB).

2) The data protection officer shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless the data protection officer is released from this obligation by the data subject.

3) Where in the course of their activities data protection officers become aware of data for which the controller or processor has the right to refuse to give evidence, this right shall also apply to the data protection officer and the data protection officer's 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, the data protection officer's files and other documents shall not be subject to seizure.

Article 39

Accreditation

1) The power to act as a certification body in accordance with the first sentence of Article 43(1) of Regulation (EU) 2016/679 shall be granted by the Liechtenstein Accreditation Body.

2) The Government may provide further details governing accreditation by ordinance.

D. Penal provisions

Article 40

Contraventions pursuant to Regulation (EU) 2016/679

1) Any person who, even negligently, infringes the provisions of Regulation (EU) 2016/679 pursuant to Article 83(4) to (6) of Regulation (EU) 2016/679 shall be punished by the Data Protection Authority with a fine in accordance with paragraph 2 for committing a contravention.

2) The fine shall be:

a) in the 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 year, whichever is higher;

b) in the 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 year, whichever is higher.

3) The Data Protection Authority shall impose fines against legal persons if the contraventions are committed in the course of business of the legal person (underlying offences) by persons who acted either on their own or as members of the board of directors, general management, management board, or supervisory board of the legal person or pursuant to other leadership positions within the legal person, on the basis of which they:

a) are authorised to represent the legal person externally;

b) exercise control in a leading position; or

c) otherwise have significant influence on the business management of the legal person.

4) For contraventions committed by employees of the legal person, even though not culpably, the legal person shall be responsible also if the contravention was made possible or significantly facilitated by the fact that the persons referred to in paragraph 3 failed to take necessary and reasonable measures to prevent such underlying offences.

5) The responsibility of the legal person for the underlying offence and the criminal liability of the persons referred to in paragraph 3 or of employees referred to in paragraph 4 for the same offence are not mutually exclusive. The Data Protection Authority may refrain from punishing a natural person if a monetary fine has already been imposed on the legal person for the same violation and there are no special circumstances preventing a waiver of the punishment.

6) The Data Protection Authority will apply the catalogue set out in Article 83(2) to (6) of Regulation (EU) 2016/679 in such a way that proportionality is ensured. In particular in the case of first-time infringements, the Data Protection Authority will make use of its corrective powers in accordance with Article 58 of Regulation (EU) 2016/679, in particular by issuing warnings.

7) No fines shall be imposed on public authorities and other public bodies.

Article 41

Unauthorised collection of personal data

Any person who collects personal data without authorisation from data processing which is not freely accessible shall at the request of the injured party be convicted by the Court of Justice of a misdemeanour and sentenced to imprisonment of up to six months or to a monetary penalty of up to 360 daily penalty units.

Article 42

Breach of data secrecy

1) Any person who wilfully and without authorisation makes available to a third party, discloses, or uses personal data that have come to the perpetrator's knowledge in the course of professional activities that require that the perpetrator has knowledge of such data shall at the request of the injured party be convicted by the Court of Justice of a misdemeanour and sentenced to imprisonment of up to six months or to a monetary penalty of up to 360 daily penalty units.

2) Any person who commits the act in order to procure a pecuniary benefit for themself or for another person, or in order to inflict a disadvantage upon another person, shall at the request of the injured party be sentenced to imprisonment of up to one year or with a monetary penalty of up to 360 daily penalty units.

3) The same punishment shall apply to any person who wilfully and without authorisation makes available to a third party, discloses, or uses personal data that have come to the perpetrator's knowledge in the course of activities for persons who are subject to a duty of professional secrecy or in the course of the perpetrator's vocational training with such persons.

4) The unauthorised making available to third parties or disclosure of confidential personal data shall remain punishable also after the perpetrator has ceased to practice their profession or has completed their vocational training.

Article 43

Prohibition of use

A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34(1) of Regulation (EU) 2016/679

may be used in criminal proceedings pursuant to Articles 41 and 42 against the person required to provide a notification or a communication or relatives as referred to in § 108(1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication.

E. Liability

Article 44

Right to compensation and liability

1) Any person who has suffered material or non-material damage as a result of an infringement of Regulation (EU) 2016/679 or the provisions of Chapter I or II shall have the right to receive compensation from the controller or processor for the damage suffered in accordance with Article 82 of Regulation (EU) 2016/679. The general provisions of civil law shall apply to the details of this claim for compensation.

2) If the controller or processor has designated a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, this representative shall also be an authorised recipient in civil law proceedings, subject to Article 12 of the Service of Documents Act.

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

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

Article 45

Scope of application

The provisions of this Chapter shall apply to the processing of personal data by public bodies competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of penalties, as far as they process data for the purpose of carrying out these tasks. The public bodies shall be regarded in that case as controllers. The prevention of criminal offences as referred to in the

first sentence shall include protection against and prevention of threats to public security. The first and second sentences shall also apply to those public bodies responsible for executing penalties, measures under criminal law, educational or other measures as referred to in the Juvenile Court Act, or fines. As far as this Chapter contains provisions for processors, it shall also apply to them.

Article 46

Definitions

For the purposes of this Chapter, the following terms shall have the following meanings:

a) "personal data": 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 person;

b) "processing": 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, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction;

c) "restriction of processing": the marking of stored personal data with the aim of limiting their processing in the future;

d) "profiling": 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": 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) "file system": 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": the competent authority which alone or jointly with others determines the purposes and means of the processing of personal data;

h) "processor": a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

i) "recipient": 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/Schengen 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": 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": 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": 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, in particular facial images or dactyloscopic data;

n) "data concerning health": personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person's health status;

o) "special categories of personal data":

   1. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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 concerning a natural person's sex life or sexual orientation;

p) "supervisory authority": an independent public authority which is established by am EEA/Schengen country pursuant to Article 41 of Directive (EU) 2016/680;

q) "international organisation": 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": any freely given, specific, informed and unambiguous indication of the data subject's wishes in a particular case by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the data subject.

Article 47

General principles for processing personal data

Personal data shall be:

a) processed lawfully and fairly;

b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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 be allowed only where strictly necessary for the performance of the controller's tasks and:

a) where expressly provided for by law;

b) to protect the vital interests of a person; or

c) where such processing relates to personal data which are manifestly made public by the data subjects themselves.

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 in particular:

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) restrictions on 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 case of transfer or processing for other purposes.

Article 49

Processing for other purposes

Processing personal data for a purpose other than the one for which they were collected shall be permitted if the other purpose is one of the purposes listed in Article 45, the controller is authorised to process data for this purpose, and processing is necessary and proportionate to this purpose. Processing personal data for another purpose not listed in Article 45 shall be permitted where a legal basis exists.

Article 50

Processing for archiving, scientific and statistical purposes

Personal data may be processed in the context of purposes listed in Article 45 in archival, scientific or statistical form if doing so is in the public interest and appropriate safeguards for the legally protected interests of data subjects are implemented. Such safeguards may consist in rendering the personal data anonymous as quickly as possible, taking measures to prevent unauthorised disclosure to third parties, or processing them organisationally and spatially separate from other tasks.

Article 51

Consent

1) If personal data may be processed in accordance with a legal provision on the basis of consent, the controller must be able to present evidence of the data subject's consent.

2) If the data subject's consent under paragraph 1 is given in the context of a written declaration 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 shall have the right to withdraw their consent under paragraph 1 at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of this before giving consent.

4) Consent under paragraph 1 shall be effective only when based on the data subject's free decision. When assessing whether consent was freely given, the circumstances in which it was given must be taken into account. The data subject shall be informed of the intended purpose of the processing. If necessary in the individual case or on request, the data subject shall also be informed of the consequences of withholding consent.

5) If special categories of personal data are to be processed, the consent under paragraph 1 must explicitly refer to these data.

Article 52

Processing on instructions from the controller

Any person acting under the authority of the controller or of the processor who has access to personal data shall not process those data except on instructions from the controller, unless required to do so by law.

Article 53

Confidentiality

Persons employed in data processing shall not process personal data without authorisation (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

1) A decision based solely on automated processing which produces an adverse legal effect concerning the data subject or significantly affects the data subject shall be permitted only where a legal basis exists.

2) Decisions referred to in paragraph 1 shall not be based on special categories of personal data unless suitable measures to safeguard the data subject's legally protected and legitimate interests are in place.

3) Profiling that results in discrimination against natural persons on the basis of 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 data subjects with regard to the processing of their personal data to access, rectification, erasure and restriction of processing;

c) the names 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 legal provisions provide for or require 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) the categories of recipients of the personal data, if any; and

e) where necessary, further information, in particular where the personal data were collected without the knowledge of the data subject.

2) In the cases of paragraph 1, the controller may postpone, limit or refrain from notification if and so long as:

a) the performance of the tasks listed in Article 45,

b) public security, or

c) the legally protected interests of third parties

would otherwise be impaired, if the interest in avoiding these threats overrides the interest of the data subject in the information.

3) If the notification relates to the transfer of personal data to the National Police for the performance of its duties relating to State security, such provision shall be permitted only with the approval of the National Police.

4) Article 57(7) shall apply *mutatis mutandis* in case of restriction pursuant to paragraph 2.

Article 57

Right of access

1) The controller shall inform data subjects on request whether data concerning them are being processed. Data subjects shall also have the right to information about:

a) the personal data being processed and the categories to which they belong;

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 period for which the data will be stored, or if that is not possible, the criteria used to determine that period;

f) the existence of the right to rectification or erasure of data or restriction of processing of data by the controller;

g) the right pursuant to Article 60 to lodge a complaint with the Data Protection Authority; and

h) the contact details of the Data Protection Authority.

2) Paragraph 1 shall not apply to personal data recorded only 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 organisational measures make processing for other purposes impossible.

3) No information shall be provided if the data subject does not provide information enabling the data to be located and if the effort required is therefore disproportionate to the data subject's interest in the information.

4) Subject to the conditions of Article 56(2), the controller may dispense with the provision of information pursuant to the first sentence of paragraph 1, or restrict, wholly or partly, the provision of information pursuant to the second sentence of paragraph 1.

5) If the information to be provided relates to the transfer of personal data to the National Police for the performance of its duties relating to State security, such provision shall be permitted only with the approval of the National Police.

6) The controller shall notify the data subject, without delay, in writing of any refusal or restriction of access. This shall not apply if providing this information would entail an impairment as referred to in Article 56(2). The notification pursuant 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 the data subject is notified pursuant to paragraph 6 of the refusal or restriction of access, the data subject may exercise their right of access also via the Data Protection Authority. The controller shall inform the data subject of this possibility and that, in accordance with Article 60, the data subject may lodge a complaint with the Data Protection Authority or demand an appealable decree. If the data subject exercises their right pursuant to the first sentence, the information shall be provided to the Data Protection Authority at the 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 permit 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 the controller could dispense with or restrict information pursuant to paragraph 4. The Data Protection Authority shall also inform the data subject of their 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 to rectification and erasure and to restriction of processing

1) The data subject shall have the right to obtain from the controller without delay the rectification of inaccurate data concerning the data subject. In particular in the case 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 ascertained, the controller shall restrict processing instead of erasing the data. In this case, the controller shall inform the data subject before lifting the restriction of processing. The data subject may also ask to have incomplete personal data completed, if doing so is appropriate when taking into account the purposes of processing.

2) The data subject shall have the right to obtain from the controller the erasure of personal data concerning the data subject without delay 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 processing where:

a) there is reason to assume 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 due to the specific mode of storage.

Data that are subject to restricted processing pursuant to the first sentence may be processed only for the purpose which prevented their erasure.

4) If the controller has rectified inaccurate data, the controller shall communicate the rectification to the body from which the controller received the personal data. In cases of rectification, erasure or restriction of processing pursuant to paragraphs 1 to 3, the controller shall inform recipients to whom the data were transferred 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 of any refusal to rectify or erase personal data or restrict its processing. This shall not apply if providing this information would entail an impairment as referred to in Article 56(2). The information pursuant 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 *mutatis mutandis*.

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 their request without delay.

3) Information provided pursuant to Article 55, any communication made pursuant to Articles 56 and 65, and requests processed 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) Where the controller has reasonable doubts concerning the identity of a data subject making the request pursuant to Articles 57 or 58, the controller may request the provision of additional information 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 any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Data Protection Authority, if the data subject believes that the processing by public bodies of personal data relating to the data subject for the purposes listed in Article 45 infringes the data subject's 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 of the progress and the outcome of the complaint and of the possibility of appeal under Article 20.

2) If a complaint about processing is lodged with the Data Protection Authority instead of the competent supervisory authority in another EEA/Schengen country, the Data Protection Authority shall transmit the complaint to the competent supervisory authority without delay. In this case, the Data Protection Authority shall inform the data subject about the transmission of the complaint and shall provide further support at the data subject's request.

D. Obligations of controllers and processors

Article 61

Processing carried out on behalf of a controller

1) Where personal data are processed by other persons or bodies on behalf of a controller, the controller shall ensure compliance with the provisions of this Act and other data protection provisions. The data subject shall assert the data subject's 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 organisational 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 authorisation by the controller. If the controller has given the processor general authorisation 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 fulfil 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 there is a legal obligation to store 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

Where 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 responsibilities under data protection law in a transparent manner in an agreement, unless these tasks and responsibilities are already set out in a law. In particular, this agreement must indicate which of them must 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 for 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 the necessary technical and organisational measures to ensure a level of security appropriate to the risk when processing personal data, in particular as regards the processing of special categories of personal data. In doing so, the controller shall take into account the relevant generally recognised guidelines and recommendations in information technology.

2) The measures referred to 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 should 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 respect of automated processing, the controller and processor, following an evaluation of the risks, shall implement measures designed to:

a) deny unauthorised persons access to processing equipment used for processing ("equipment access control");

b) prevent the unauthorised reading, copying, modification or erasure 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 personal data are protected during transfers of personal data or during transport of data media ("transport control");

i) ensure that installed systems may, in the case of interruption, be restored ("recovery");

k) ensure that all system functions perform and that the appearance of faults in the functions is reported ("reliability");

l) ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system ("integrity");

m) ensure that personal data processed on behalf of the controller can only be processed in compliance with the controller's instructions ("processing 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(b) to (f) may be achieved in particular by using state-of-the-art encryption.

Article 64

Notifying the Data Protection Authority of a personal data breach

1) In the case of a personal data breach, the controller shall notify the Data Protection Authority without delay and, if possible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the Data Protection Authority is not notified within 72 hours, the notification shall be accompanied by reasons for the delay.

2) A processor shall notify the controller of a personal data breach without delay.

3) The notification referred to in paragraph 1 shall include 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 by the controller to address the personal data breach, including measures to mitigate its possible adverse effects.

4) If it is not possible to provide the information pursuant to paragraph 3 with the notification, the controller shall provide this information as soon as it is available.

5) The controller shall document any personal data breaches. This documentation shall include all 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 a controller in another EEA/Schengen country, the information referred to in paragraph 3 shall be communicated to the controller in that country without delay.

7) The prohibition of use under Article 43 shall apply *mutatis mutandis*.

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) If a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall notify the data subject of the personal data breach without delay.

2) The notification of the data subject pursuant to paragraph 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Article 64(3)(b) to (d).

3) Notification under paragraph 1 shall not be required if any of the following conditions are met:

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 them, such as encryption;

b) the controller has taken subsequent measures which ensure that the substantial risk referred to in paragraph 1 is no longer likely to exist; or

c) it would involve a disproportionate effort; in this case, a public communication shall be made or a similar measure taken to inform the data subjects in an equally effective manner.

4) If the controller has not informed the data subjects of a personal data breach, the Data Protection Authority may formally determine that, in its opinion, the conditions referred to in paragraph 3 have not been met. In doing so, the Data Protection Authority shall consider the likelihood of the personal data breach resulting in a high risk as referred to in paragraph 1.

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) The prohibition of use under Article 43 shall apply *mutatis mutandis*.

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, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the data subjects.

2) A joint assessment may address a set of similar processing operations that present similarly high risks.

3) The controller shall involve the Data Protection Authority in carrying out the impact assessment.

4) The impact assessment shall take the rights of the data subjects affected by the processing into account 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 purposes;

c) an assessment of the risks to the rights and freedoms of the 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 carrying out the latter's tasks.

Article 68

Prior 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 pursuant to Article 66 indicates that the processing would result in a high risk to the rights and freedoms of data subjects 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 draw up a list of the processing operations which are subject to prior consultation pursuant to the first sentence.

2) In the case of paragraph 1, the Data Protection Authority shall be presented with:

a) the data protection impact assessment carried out 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 legal interests of the data subjects; and

e) the name and contact details of the data protection officer.

On request, the Data Protection Authority shall be given any other information it requires 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, it 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 especially 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 especially urgent, the controller may initiate processing after the consultation has started but before the period referred to in the first sentence of paragraph 3 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 keep a record of all categories of processing activities under its responsibility. This record shall contain all of the following information:

a) the name and contact details of the controller and, where applicable, of the joint controller; and the name and contact details of the data protection officer;

b) the purposes of the processing;

c) the categories of recipients to whom the personal data have been or are to 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 bodies in a third country or to an international organisation;

g) information about the legal basis for the processing;

h) the envisaged time limits for the 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 organisation, including the identification of that third country or international organisation; and

c) a general description of the technical and organisational security measures according to Article 63.

3) The records referred to in paragraphs 1 and 2 shall be in writing or in electronic form.

4) Controllers and processors shall make these records available to the Data Protection Authority on 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

minimisation, 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 rights and freedoms 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 only the necessary personal data. Personal data shall be rendered anonymised or pseudonymised as early as possible, as far as possible in accordance with the purpose of processing.

2) The controller shall implement appropriate technical and organisational 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

When processing personal data, the controller shall, as far as possible, make a clear distinction between different categories of data subjects. This applies in particular to the following categories:

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 indicate 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 points (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 countries or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the Third Part 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 its tasks.

3) Article 58(3) and (4) shall apply *mutatis mutandis*. 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 legally defined time limits for storing or erasing data, 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 processors shall provide for logs to be kept for at least the following processing operations in automated processing 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 may be used only 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 the year in which they were generated.

5) The controller and the processor shall make the logs available to the Data Protection Authority on request.

Article 76

Confidential reporting of violations

The controller shall ensure that it is able to receive confidential reports of violations of data protection law which have occurred in its area of responsibility.

E. Transfers of data to third countries and to international organisations

Article 77

General requirements

1) If all other conditions applicable to data transfers are met, the transfer of personal data to bodies in third countries or to international organisations shall be permitted if:

a) the body or international organisation is responsible for the purposes referred to in Article 45; and

b) the European Commission has adopted an adequacy decision pursuant to Article 36(3) of Directive (EU) 2016/680 that is applicable in Liechtenstein.

2) No transfer of personal data shall be permitted, despite an adequacy decision as referred to in paragraph 1(b) and the public interest in the data transfer to be taken into account, if in the individual case it cannot be ensured that the data will be handled appropriately in terms of data protection law and in accordance with fundamental rights in the area of responsibility of the recipient, or if a transfer would conflict with other overriding legitimate interests of a data subject. 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 country are to be transferred pursuant to paragraph 1, the competent body of the other EEA/Schengen country must provide prior authorisation of the transfer. Transfers without the prior authorisation 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 an EEA/Schengen country and the prior authorisation cannot be obtained in time. In the case of the second

sentence, the other EEA/Schengen country's body responsible for giving prior authorisation shall be informed of the transfer without delay.

4) The controller transferring data pursuant to paragraph 1 shall take appropriate measures to ensure that the recipient will transfer the data onward to other third countries or other international organisations only with the prior authorisation of the controller. When deciding whether to authorise the transfer, the controller shall take into account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data were originally transferred and the level of personal data protection in the third country or international organisation to which the data are to be transferred onward. The transfer shall be authorised only if a direct transfer to the other third country or international organisation would be lawful. The responsibility for issuing authorisation may also be otherwise provided for.

Article 78

Data transfers with appropriate safeguards

1) If, in derogation from Article 77(1)(b), no decision pursuant to Article 36(3) of Directive (EU) 2016/680 exists, transfers which meet the remaining requirements of Article 77 shall be permitted also 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 document transfers pursuant to paragraph 1(b). The documentation shall include the date and time of the transfer, the identity of the recipient, the reason for the transfer and the personal data transferred. It shall be provided to the Data Protection Authority on request.

3) The controller shall file a report to the Data Protection Authority at least once a year covering transfers conducted on the basis of an assessment pursuant to paragraph 1(b). In this report, the controller may categorise the recipients and the purpose of the transfers appropriately.

Article 79

Data transfers without appropriate safeguards

1) If in derogation from Article 77(1)(b), no decision pursuant to Article 36(3) of Directive (EU) 2016/680 or appropriate safeguards as referred to in Article 78(1) exist, transfers which meet the remaining requirements of Article 77 shall be permitted also if they are necessary:

a) to protect the vital interests of a natural person;

b) to safeguard legitimate interests of the data subject;

c) to prevent an immediate and serious threat to the public security of a country;

d) in individual cases for the purposes referred to in Article 45; or

e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes referred to in Article 45.

2) The controller shall not transfer data pursuant to paragraph 1 if the fundamental rights of the data subject override the public interest in the transfer.

3) Article 78(2) shall apply *mutatis mutandis* to transfers pursuant to paragraph 1.

Article 80

Other data 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 in Article 77(1)(a) if the transfer is strictly necessary for the performance of their tasks and:

a) in the specific case no fundamental rights of the data subject override the public interest in the transfer;

b) transfer to the bodies referred to in Article 77(1)(a) would be ineffective or inappropriate, in particular because the transfer cannot be carried out in time; and

c) the controller informs the recipient of the purposes of processing and instructs the recipient that the transferred data may be processed only to the extent necessary for these purposes.

2) In the case of paragraph 1, the controller shall inform the bodies referred to in Article 77(1)(a) of the transfer without delay, unless this is ineffective or inappropriate.

3) Article 78(2) and (3) shall apply *mutatis mutandis* to transfers pursuant to paragraph 1.

4) In the case of transfers pursuant to paragraph 1, the transmitting 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 in the field of judicial cooperation in criminal matters and police cooperation shall remain unaffected.

F. Cooperation among supervisory authorities

Article 81

Mutual administrative assistance

1) The Data Protection Authority shall provide the supervisory authorities in other EEA/Schengen countries with information and administrative assistance as far as necessary to implement and apply Directive (EU) 2016/680 in a consistent manner. Administrative assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

2) The Data Protection Authority shall take all appropriate measures required to reply to a request for administrative assistance without delay and no later than one month after receiving the request.

3) The Data Protection Authority may refuse to comply with the request only if:

a) it is not competent for the subject matter of the request or for the measures it is asked to execute; 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 country of the results or, as the case may be, of the progress of the measures taken in response to the request. In the case of paragraph 3, the Data Protection Authority shall provide reasons for refusing to comply with the request.

5) The Data Protection Authority shall, as a rule, supply the information requested by the other EEA/Schengen country's supervisory authority by electronic means and using a standardised format.

6) The Data Protection Authority shall not charge a fee for action taken pursuant to a request for administrative assistance unless it has agreed with the other EEA/Schengen country's supervisory authority in the individual case on the reimbursement of expenses incurred.

7) A request for administrative assistance by the Data Protection Authority shall contain all the necessary information, including in particular the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

G. Liability and penalties

Article 82

Damages and compensation

1) If a controller has caused a data subject to suffer damage by processing personal data in violation of this Act or other law applicable to this processing, the controller or its legal entity shall be obligated to provide compensation to the data subject. This obligation to provide 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, in the case of automated processing of personal data, it is not possible to determine which of several controllers caused the damage, each controller or its legal entity shall be liable.

4) §§ 1301 to 1304 of the General Civil Code (ABGB) shall apply *mutatis mutandis* to contributory negligence on the part of the data subject.

5) Claims for damages shall be subject to a limitation period of three years after the end of the day on which the damage became known to the injured party.

Article 83

Penal provision

Articles 41 and 42 shall apply *mutatis mutandis* to the processing of personal data by public bodies in the context of activities pursuant to the first, third, or fourth sentence of Article 45.

IV. Special provisions for processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

Article 84

Processing of personal data in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

1) The transfer of personal data to a third country, to supranational or intergovernmental bodies or to international organisations in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall be permitted in addition to the cases permitted under Regulation (EU) 2016/679 also if the processing is necessary to perform tasks for urgent reasons of defence or to fulfil treaty obligations of the State in the field of crisis management or conflict prevention or for humanitarian measures. The recipient shall be instructed that the transferred data may be used only for the purpose for which they were transferred.

2) Article 17(4) shall not apply to processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 by the National Police if the Government determines in the individual case that meeting the obligations referred to in that provision would endanger the security of the State.

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:

a) in the cases referred to in Article 32(1)(a) to (c); or

b) if meeting this obligation would disclose information which by a law or by its nature must be kept secret, in particular because of legitimate

interests of a third party which outweigh the interests of the data subject in obtaining the information.

4) If the data subject is not to be informed in the cases of paragraph 3, no right of access shall apply. Articles 32(2) and 33(2) shall not apply.

V. Transitional and final provisions

Article 85

Implementing ordinances

The Government shall issue the ordinances required to implement this Act, especially on:

a) the conditions under which a public body may have personal data processed by a third party or process personal data for third parties;

b) the notification of video surveillance under Article 5;

c) The adequacy decisions by the European Commission applicable in Liechtenstein under Article 45 of Regulation (EU) 2016/679 and the standard data protection clauses adopted by the European Commission under Article 46 of Regulation (EU) 2016/679;

d) the fees for official acts of the Data Protection Authority.

Article 86

Repeal of law hitherto in force

The Data Protection Act (DSG) of 14 March 2002, LGBl. 2002 No. 55, as amended, is hereby repealed.

Article 87

Data Protection Commissioner and other employees

The Data Protection Commissioner elected under the law hitherto in force shall, after entry into force of this Act, assume directorship of the Data Protection Authority (Article 12) and shall perform this function in accordance with the new law until 31 December 2025. The existing employment relationships of the other employees of the Data Protection Authority shall continue.

Article 88

Data Protection Commission

1) The term of the existing Data Protection Commission shall end upon entry into force of this Act.

2) Complaints proceedings or proceedings relating to recommendations of the Data Protection Authority pending before the Data Protection Commission at the time of entry into force of this Act shall be dealt with by the Complaints Commission for Administrative Matters under the law hitherto in force.

Article 89

Video surveillance

1) Approval for video surveillance granted under the law hitherto in force shall continue to be valid until the expiry of such approval.

2) If it is intended to continue video surveillance after expiry of the approval, a notification must be made in accordance with Article 5(7).

Article 90

Accreditations and certifications

Accreditations and certifications granted under the law hitherto in force shall continue to be valid until their expiry. The law hitherto in force shall apply to accreditation and certification proceedings pending at the time of entry into force of this Act.

Article 91

Entry into force

Provided that the referendum period expires without a referendum being called, this Act shall enter into force on 1 January 2019, otherwise on the day of its promulgation.

Representing the Reigning Prince:
signed *Alois*
Hereditary Prince

signed *Adrian Hasler*
Prime Minister