Arnošt Lustig Foundation: Data Protection Guidelines

1. General principles

1.1. Introduction

This Directive regulates the technical and organisational measures to ensure the protection of personal data in accordance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regards to the processing of personal data and on the free movement of such data, and abolishing Directive 95/46/EC (General Data Protection Regulation), the so-called "General Data Protection Regulation". GDPR (hereinafter referred to as "GDPR") and related regulations in order to ensure good practice in the adoption and implementation of measures to protect personal data of the person: Arnošt Lustig Foundation, Identification Number: 09549609, Drtinova 557/10, Smíchov, 150 00 Prague 5 (hereinafter referred to as "the Foundation").

1.2. Scope of application

a) All members of the Foundation's statutory bodies, employees, staff and other persons who come into contact with personal data at the Foundation or in the course of their work for the Foundation are bound by this Directive.

b) This Directive shall also apply accordingly to third parties who come into contact with personal data in the course of their work for the Foundation.

c) If the Foundation carries out its activities in another country, it is also obliged to comply with the rules on the protection of personal data applicable in that country.

1.3. Definition of terms

For the purposes of this Directive:

a) **archiving** – the storage of information in paper or electronic form;

b) **security of processing the personal data** – technical and organisational measures to ensure a level of security appropriate to the risk involved;

c) **biometric data** – means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

d) **sensitive data** – personal data consisting of information as to the racial or ethnic origin of the data subject; his political opinions; his religious beliefs or other beliefs of a similar nature; whether he is a member of a trade

union; his physical or mental health or condition; his sexual life; the commission or alleged commission by him of any offence; or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings;

e) **genetic data** – means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

f) **destruction of personal data** – the physical destruction of its medium, its physical erasure or its permanent exclusion from further processing;

g) **personal data** – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

h) **recipient** – means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

i) **pseudonymisation of personal data** – means the processing of personal data in such a manner that the

personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

j) **collection of personal data** – a systematic procedure or set of procedures designed to obtain personal data for the purpose of storing them on a storage medium for immediate or subsequent processing;

k) **consent of the data subject** – means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

l) **controller** – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

m) **data subject** – the natural person to whom the personal data relate;

n) **personal data retention** – keeping the data in a form which permits further processing;

o) **processing personal data** – means any operation or set

of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

p) **processor** – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

q) **disclosed personal data** – personal data made available, in particular by mass media, other public communication or as part of a public list.

2. Obligations in the management and processing of personal data

2.1. The director of the foundation

The Director of the Foundation himself or through authorised persons:

a) ensures the conditions for proper protection of personal data in the sense of the GDPR and other legal regulations, including the relevant European Union legislation;

b) ensures the ongoing education of the persons concerned in the field of personal data protection, primarily through self-study, if necessary through training or consultation;

c) is responsible for the staffing of the data protection staff;

d) provide sources of information on good practice in the protection of personal data, including contacts to

persons professionally able to consult on the subject, or to the Data Protection Officer, if appointed;

e) ensuring the control of data protection activities;

f) ensuring the implementation of data protection measures, including knowledge of the obligations of persons coming into contact with personal data;

g) where necessary, carry out an assessment of the impact of the activity on the protection of personal data,

h) where necessary, carry out prior consultation with the Data Protection Authority (hereinafter referred to as the DPA);

i) keep records of the processing of personal data;

j) report personal data breaches within 72 hours of becoming aware of the breach as a data controller to the DPOA and, if necessary, to the data subjects whose personal data have been compromised;

k) allow the portability of personal data to another controller in an appropriate format;

l) where necessary, appoint a data protection officer;

m) comply with the instructions of the supervisory authorities in the field of data protection.

2.2. Other persons coming into contact with personal data

Persons coming into contact with personal data are obliged to:

a) process personal data in accordance with the GDPR and relevant laws, other legal standards, as well as other EU regulations and international treaties that apply to this issue in their work;

b) maintain the confidentiality of personal data and the measures taken to protect it, even after the end of their employment or contractual relationship with the Foundation;

c) prevent the unauthorised reading, alteration, deletion or disclosure of personal data, not to make copies of software or documents containing personal data for purposes other than for work purposes, and not to allow others to do so, for example by not copying large amounts of personal data from computer data carriers or storage devices to other media without two or more persons simultaneously authorising and technically enabling (e.g. by entering passwords) such copying;

d) use only secure hardware and software when using computing technology, and do so in a secure manner, and report any abnormal manifestations of computing technology to the relevant experts without delay;

e) adhere to the principles of safe use of computing technology, in particular by using appropriate passwords and taking care to protect them from disclosure; do not visit risky websites, etc., and report immediately any reasonable suspicion of a threat to the security of personal data.

3. Technical measures to ensure the protection of personal data

3.1. Data storage

Writings and other tangible data carriers containing personal data may only be stored in locked rooms and, where possible, in lockable cabinets.

3.2. Electronic data files

Electronic data files containing personal data may only be stored in computer memory:

a) if access to such files is protected by a domain name that allows traceability of who has accessed the personal data and to whom the personal data may have been transmitted, and a password that must be at least 6 characters long, at least one of which must be a number or character (an appropriate password);

b) access to the use of the computer in whose memory the files are located is protected by an appropriate password (software or hardware) or an appropriate lock;

c) so that all data must be backed up regularly and the back-up media must be changed at reasonable intervals and unauthorised access to the data media must be prevented;

d) so that the competent persons have access only to personal data corresponding to the authorisation of those persons, on the basis of specific user authorisations established exclusively for those persons.

Detailed instructions for the protection of data files (including the hardware they use) and for the allocation, storage and creation of domains, passwords and other security features are contained in the protected clause of this Directive, to which only authorised persons named in the protected clause have access.

3.3. Paper data storage device

a) Personal data that are not in electronic form must be protected in locked rooms or locked cabinets, where

the keys are held only by authorised persons who must not make them accessible to any unauthorised persons. Where sensitive data is handled, sensitive personal data must be secured with particular care and the range of persons who may have access to it must be minimised).

b) All documents and disposable data carriers and other disposable materials containing personal data must be destroyed or otherwise disposed of once the reasons for retaining the personal data on them have ended. When a large number of documents and other tangible data carriers containing personal data are disposed of, a disposal report shall be drawn up indicating the date, place and manner of disposal; the same shall apply to the disposal of documents, data carriers or other materials containing sensitive personal data. The destruction of personal data on reusable media shall be carried out in such a way that they cannot be recovered (the media need not be destroyed).

4. Activity impact assessment on the protection of personal data

4.1. Where it is likely that a type of processing of personal data by the Foundation, in particular using new (computer) technologies, will result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing, the Foundation shall prepare a personal data protection impact assessment. The data protection impact assessment shall include a systematic description of the intended processing, a risk assessment, a proportionality test, etc. The data protection

impact assessment must also clearly define the security measures and safeguards adopted to protect personal data.

4.2. In particular, the Director is required to examine whether the Foundation carries out a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based which produce legal effects in relation to natural persons or have a similarly significant impact on natural persons. In particular, it is obliged to examine whether employees, customers or other persons are not classified into certain groups according to computer technology, in particular in the case of the use of artificial intelligence, and whether, as a result of such classification into groups, their rights or obligations are then determined without a final human decision (e.g. decisions on a change of job classification, on the amount of pay or benefits, on the termination of employment, etc.).

5. Obligation to keep records of personal data processing activities

5.1. The Director is obliged to ensure that records are kept of all processing of personal data, on the basis of which it is possible to prove at any time who was the controller (name, surname and contact details) or who acted as data protection officer, the purposes of the processing of personal data, a description of the categories of data subjects and categories of personal data, categories of recipients, including recipients in third countries or international organisations, information on any transfer of personal data

to a third country or international organisation, including identification of that third country or international organisation, evidence of appropriate safeguards for the protection of personal data, planned time limits for erasure of categories of personal data (according to the shredding rules), general description of technical and organisational security measures.

5.2. Record-keeping on the processing of personal data may be carried out in both electronic and paper form.

5.3. If the Foundation has personal data processed by another person, the Foundation shall ensure that the personal data are processed on the basis of a duly concluded contract on the processing of personal data.

6. Obligation to report personal data breaches

6.1. The Director is obliged to ensure that all personal data breaches are reported to the Data Protection Authority within 72 hours of becoming aware of such a breach. In doing so, they must ensure that a proper distinction is made as to whether the personal data breach is actually a personal data breach or whether the risk to the protection of personal data in such a case is insignificant.

7. Right to data portability

7.1. The Director must ensure that records are kept of all processing of personal data so that it can be demonstrated at any time who was the data controller (name, surname and contact details) or who acted as data protection officer, the purposes of the processing of personal data, a description of the categories of data subjects and categories of personal

data, categories of recipients, including recipients in third countries or international organisations, information on any transfer of personal data to a third country or international organisation, including identification of that third country or international organisation, evidence of appropriate safeguards for the protection of personal data, planned time limits for erasure of categories of personal data (according to the shredding rules), general description of technical and organisational security measures.

7.2. The Director is also required to ensure that the rights and freedoms of other persons or intellectual property rights are not adversely affected when personal data of a particular person are transferred to another controller.

7.3. The portability of personal data must be explicitly brought to the attention of the data subject and this right must be clearly indicated, separately from any other information, at the time of the first communication with the data subject, i.e. the persons whose personal data are to be processed.

8. Erasure of personal data and the right to be forgotten

8.1. The Principal shall ensure that all personal data are erased without undue delay if:

a) the personal data are no longer necessary for the purpose for which they were collected or processed.

b) the data subject withdraws consent where the processing is based on consent and there is no other legal basis for the processing.

c) the personal data have been unlawfully processed.

d) where parental consent is not given for the processing of children's personal data in connection with the offer of information society services.

8.2. The Director must also ensure that reasonable steps, including technical measures, are taken to erase all personal data, including backups and automatic restores of IT systems.

9. Transfer of personal data abroad

9.1. If it is necessary to transfer personal data abroad, the Foundation is obliged to ensure that such personal data is transferred only to suitable and reliable business partners, that the legal environment in the country of the business partner is properly examined before transferring personal data abroad, including verification of the existence of international data protection treaties with the country of the business partner.

9.2. When transferring personal data abroad, there must always be an appropriate contract with the business partner for such transfer, which will also address data protection, including penalties for breach).

10. Electronic communication

10.1. Where the Foundation has any presentation of its activities on the Internet, it is the Foundation's responsibility to ensure that any visitors to the Foundation's website are properly informed of their rights and obligations. In particular, information on the conditions for processing personal data, the use of cookies, etc. must be provided.

10.2. If any consents to the processing of personal data are requested on the website, such consent must always be obtained in a free, informed, non-deceitful and transparent

manner, i.e. so that anyone who consents to the processing of their personal data is not penalised in any way for not giving such consent. If there are checkboxes on the website for giving consent, these must be set so that the individual items are checked by the person, not that they override a check that has already been made.

10.3. All requests for consent to the processing of personal data must state that this consent is revocable. All instructions regarding consent to the processing of personal data must be written in clear, plain language.

11. Final provisions

11.1. Individual measures under this Directive may be further elaborated in specific directives, guidelines or other relevant Foundation documents. Matters not covered by this Directive shall be governed by generally binding legislation, both Czech and European Union, including recommendations.

11.2. This Directive shall enter into force on 16. 6. 2021.

11.3. Any changes or additions to this directive shall be approved by the Foundation's Board of Directors or an authorized member of the Board of Directors.