Act on Data Protection and the Processing of Personal Data

No 90 of 27 June 2018

Entered into force on 15 July 2018. *EEA Agreement:* Annex XI to Regulation 2016/679.

If mention is made in this Act of a Minister or Ministry without further specification, this shall be understood to mean the **Minister of Justice** or the **Ministry of Justice,** under whose auspices this Act is administered. Information on the division of responsibilities between ministries, laid down in a Presidential Decree, can be found here.

Chapter I Objective, Definitions and Coverage.

Article 1

Objectives.

The objective of this Act is to promote that personal data be treated in accordance with fundamental principles and rules on the protection of personal data and respect for private life, and to ensure the reliability and quality of such data and their free flow within the EEA single market.

A special Authority, The Data Protection Authority, monitors the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council, this Act and rules laid down pursuant to it, *cf*. the provisions of Chapter VII of this Act. A European supervisory authority pursuant to Chapter VII of the Regulation is the European Data Protection Board.

Article 2

Incorporation into law.

The provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as it is incorporated into the Agreement on the European Economic Area, shall apply in Iceland with the adaptations resulting from the Decision of the EEA Joint Committee amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement. [1)] The Regulation is included as an attachment to this Act.

[1)] *Decision of the EEA Joint Committee No 154/2018.*

Article 3

Definitions.

For the purposes of this Act:

1. *The Regulation:* 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.

2. *Personal data:* 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.

3. *Sensitive personal data:*

a. Personal data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership.

b. Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, and data on any drug, alcohol or substance consumption.

c. Data on a natural person's sex life or sexual orientation.

d. 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.

e. 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, on the condition that the data is used for the purpose of uniquely identifying a natural person.

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

5. *Filing system:* A structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

6. *Controller:* The natural or legal person, public authority or other body which determines, alone or jointly with others, the purposes and means of the processing of personal data.

7. *Processor:* A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

8. *Consent:* A 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.

9. *Electronic surveillance:* Surveillance that is continuous or repeated on a regular basis and incorporates the monitoring of individuals with remote-controlled or automatic equipment and is carried out in public places or areas normally traversed by a limited number of people. The concept entails:

a. Surveillance which does, shall or may lead to the processing of personal data and

b. video surveillance carried out by television cameras, webcams or other comparable equipment without any collection of recorded material or other actions corresponding to the processing of personal data.

10. *Profiling:* 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.

11. *Personal data breach:* Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Article 4

Material scope.

This Act and the Regulation apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

This Act and the Regulation shall not apply to how a natural person uses his or her own personal data that concern his or her family's private affairs or is solely intended for private purposes.

This Act shall apply to the processing of personal data of deceased natural persons, where appropriate, for a five-year period from their deaths or longer, when this concerns personal data which is fair and reasonable to keep confidential.

This Act and this Regulation shall not apply to processing of personal data by the judiciary in the performance of its judicial tasks.

This Act and this Regulation shall not apply to processing of personal data in relation to the function of the Althingi and its bodies and investigative bodies.

This Act and this Regulation shall not apply to processing of personal data by the State in relation to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The provisions of this Act and this Regulation shall apply regardless of whether an issue falls within the scope of the EEA Agreement, with the exception of Chapter VII of the Regulation.

Article 5

Relation to other legislation.

Special provisions of other acts on the processing of personal data, adopted within the framework of the Regulation, prevail over the provisions of this Act.

This Act shall not limit the right of access to data stipulated in the Information Act and the Administrative Procedures Act.

The provisions of the Regulation prevail over the provisions of this Act.

Article 6

Relation to the freedom of expression.

To the extent that it is necessary to reconcile the right to privacy on the one hand with the freedom of expression on the other, derogations can be made from provisions in this Act and the Regulation for journalistic purposes and artistic or literary expression.

When personal data is processed solely for journalistic purposes or artistic or literary expression, only the provisions of Article 5(1)(a) and (d), Articles 24, 26, 28, 29, 32, 40-43 and 82 of the Regulation, and Articles 48 and 51 of this Act shall apply.

Article 7

Geographical scope.

This Act and the Regulation shall apply to processing of personal data in relation to the function of controllers or processors established in Iceland, regardless of whether the processing itself is carried out in the European Economic Area or not.

This Act and the Regulation shall apply to processing of personal data of data subjects in Iceland carried out within the function of controllers or processors not established in the European Economic Area or when the processing is related to:

1. the offering of goods or services to such data subjects in the European Economic Area, irrespective of whether a payment is required of the data subject; or

2. the monitoring of their behaviour as far as their behaviour takes place within that area.

In the case specified in paragraph 2, the controller or the processor shall designate its representative within the European Economic Area or in a Member State of the Convention establishing the European Free Trade Association, with the exceptions provided for in Article 27 of the Regulation. In that case, the provisions of this Act concerning controllers or processors shall apply to the representative, as further stipulated in Article 27 of the Regulation.

Chapter II General Rules on Processing.

Article 8

Principles relating to processing of personal data.

In the processing of personal data, all following shall be adhered to, as may be further stipulated in Article 5 of the Regulation, i.e. that the data are:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject;

2. collected for specified, explicit, legitimate and objective purposes and not further processed in a manner that is incompatible with those purposes; further processing for historical, statistical or scientific purposes shall not be considered to be incompatible with the initial purposes, provided that appropriate security is taken into consideration;

3. adequate, relevant and limited to what is necessary in relation to the purpose of the processing;

4. accurate and, where necessary, kept up to date; personal data that are inaccurate or incomplete, given the purpose of their processing, shall be erased or rectified without delay;

5. kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that appropriate security is taken into consideration;

6. processed in a manner that ensures appropriate security of the personal data.

The controller shall be responsible for, and be able to demonstrate compliance with, the provisions of paragraph 1.

Article 9

General rules on lawfulness of processing personal data.

The processing of personal data shall be lawful only if, and to the extent that, at least one of the following applies, as further stipulated in Article 6 of the Regulation:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

3. processing is necessary for compliance with a legal obligation to which the controller is subject;

4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third person, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 10

Conditions for consent.

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data, as further stipulated in Articles 7 and 8 of the Regulation.

If the data subject's consent 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.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

When a child is offered information society services directly and the processing of personal data is based on the child's consent, the processing shall be lawful only if the child is at least 13 years old. If the child is below the age of 13, the processing shall be lawful only to the extent the consent is given by the holder of parental responsibility. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

Article 11

Specific conditions for processing sensitive personal data.

The processing of sensitive personal data pursuant to Article 3(3) of this Act shall be lawful only if one of the conditions of Article 9 of this Act is fulfilled, and, furthermore, that one of the following conditions, as further stipulated in Article 9 of the Regulation, is fulfilled:

1. the data subject has given explicit consent to the processing for one or more specific purposes;

2. the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, and is carried out on the basis of law which provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

3. the processing is necessary to protect the vital interests of the data subject or of another natural person not physically or legally capable of giving his or her consent;

4. the processing is carried out in the course of the legitimate activities of a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subject, and with appropriate safeguards;

5. the processing relates only to personal data which are manifestly made public by the data subject;

6. the processing is necessary for the establishment, exercise or defence of legal claims;

7. the processing is necessary for reasons of substantial public interest and is carried out on the basis of law which provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

8. the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis and the provision of health or social care or treatment, on the basis of a special legal authorisation, provided it is carried out by a professional of such services subject to the obligation of professional secrecy;

9. the 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, and is carried out on the basis of law which provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

10. the processing is necessary for statistical purposes, scientific or historical research purposes, provided that the right to data protection is ensured with specific measures, where appropriate, in accordance with this Act, and is carried out on the basis of law which provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

11. the processing is necessary for archiving purposes of public interest and is carried out on the basis of law which provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, in particular professional secrecy.

The Data Protection Authority will settle disputes on whether personal data should be considered sensitive data or not.

Article 12

Processing of data on criminal offences.

Public authorities are not authorised to process data on criminal offences unless it is necessary for the purposes of their statutory tasks.

Data pursuant to paragraph 1 must not be shared unless:

1. the data subject has given explicit consent for sharing the data;

2. the data sharing is necessary for legitimate public or private interests that evidently override the interests of data confidentiality, including the interests of the data subject;

3. the data sharing is necessary for statutory tasks carried out by the authority concerned or for the purpose of making an administrative decision; or

4. the data sharing is necessary for a task carried out in the public interest that has been legitimately entrusted to a private body.

Private bodies are not authorised to process data on criminal offences unless the data subject has given his or her explicit consent or the processing is necessary for legitimate interests that evidently override the fundamental rights and freedoms of the data subject.

Data according to paragraph 3 shall not be shared unless the data subject has given explicit consent. However, data may be shared without consent if it is necessary for legitimate public or private interests that override the interest of keeping the data confidential, including the interest of the data subject.

Processing according to this Article shall always be by virtue of one of the authorisations of Article 9 of this Act, *cf.* Article 6(1) of the Regulation.

Articles 13

Use of a personal identification number.

The use of a personal identification number is authorised if its purpose is objective and necessary to ensure secure personal identification. The Data Protection Authority may prohibit or order the use of a personal identification number.

Article 14

Electronic surveillance.

Electronic surveillance shall always be with the precondition that it is carried out for objective reasons. Electronic surveillance in an area generally used by a limited number of people is also subject to the condition that it is necessary on account of the nature of the activities carried out there.

Processing of personal data carried out in relation to electronic surveillance shall comply with the provisions of this Act.

Material produced during electronic surveillance, such as audio and video, including sensitive personal data and data on criminal offences, may be collected provided that the following conditions are met:

1. the surveillance is necessary and is carried out for reasons concerning security and the safeguarding of property;

2. the material collected through surveillance will not be transmitted to others or processed further except with the consent of the person concerned or on the basis of authorisations laid down in rules, *cf.* paragraph 5; it is, however, permitted to transmit material to the police with information

concerning accidents or criminal offences in which case all other copies of the material must be deleted;

3. the material collected through surveillance will be deleted when there are no longer objective grounds to keep it.

When electronic surveillance is carried out in a workplace or in public this shall be clearly indicated by a warning sign or other visible means, together with the identity of the controller.

The Data Protection Authority shall lay down rules and provide instructions on electronic surveillance and the processing of material collected through surveillance, such as audio and video, including on its security, the right of the data subject to watch or listen to recordings, retention time and deletion, storage method, material transmission and its uses.

Article 15

Processing of data on financial issues and creditworthiness.

An authorisation by the Data Protection Authority is required for the operation of financial information agencies and for the processing of information on the financial affairs and creditworthiness of natural and legal persons, including default records and credit quality assessments, for the purpose of transmitting it to others. In the case of a legal person, only the following provisions of this Act shall apply: Article 17 on the right of the data subject to information, Article 20 on the right to rectification or erasure of data, Article 25 on the processing of data by processors, Article 31 on processing requiring authorisation, Article 32 on requirements regarding the granting of authorisations, Article 33 on terms, Article 41(1), points 5 and 6, on access by the Data Protection Authority to information, etc., Article 42, point 6, on the cessation of processing, etc., Article 45 on daily fines, Article 48 on penalties, and Article 51 on compensation.

The Minister shall set out further conditions for processing pursuant to paragraph 1 in a regulation.

Article 16

Transfer of personal data to another country or international organisations.

Decisions of the Commission on the transfer of data to a third country or an international organisation pursuant to Article 45 of the Regulation shall apply in Iceland in accordance with a decision of the EEA Joint Committee. The Minister shall confirm such decisions and publish a notification thereof in the Official Gazette.

Chapter III Rights of the Data Subject and Restrictions of such Rights.

Article 17

Principles of information transparency, right of the data subject to information and access, and exceptions to the right of the data subject.

The controller shall take appropriate measures to ensure transparency of information and notifications to the data subject pursuant to Article 12 of the Regulation, so as to enable him or her to exercise his or her right to information and the right of access.

The data subject has the right to information on processing, regardless of whether personal data were collected from him or her or not, as well as the right of access to his or her own personal data pursuant to Articles 13 to 15 of the Regulation, with the exceptions specified in paragraph 3.

Article 13(1) to (3), Article 14(1) to (4), and Article 15 of the Regulation on the rights of the data subject shall not apply if urgent interests of natural persons connected to the information, including the data subject, override these rights.

A right provided pursuant to Articles 13 to 15 of the Regulation may be restricted by way of a legislative measure if such restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

1. national security;
2. national defence;
3. public security;
4. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
5. other important objectives of general public interest, in particular important economic or financial interests, including monetary, budgetary and taxation matters, public health and social security;
6. the protection of a data subject, important public interests or the fundamental rights of others;
7. the enforcement of civil law claims;
8. legislative provisions on professional secrecy.

The provision of paragraph 4 may be applied to personal data in working documents used in the preparation of decisions by the controller, that have not been transferred to others, to the extent necessary to ensure the preparation of the procedure.

Information in cases that are being processed by the authorities may be exempted from the right of access pursuant to Article 15(1) of the Regulation to the same extent as exceptions to the right of information pursuant to the Information Act and the Administrative Procedures Act.

The provisions of Article 34 of the Regulation on the obligation to communicate any personal data breach to the data subject shall not apply if the provisions of paragraph 4, points 1 and 4, apply.

Article 18

Safeguard procedures and exemptions regarding processing for research, statistical or archiving purposes carried out in the public interest.

Processing for scientific or historical research purposes, statistical purposes or archiving purposes in the public interest shall be subject to appropriate safeguards, including technical and organisational measures, to protect the rights and freedoms of data subjects in accordance with Article 89 of the Regulation, in particular in order to ensure respect for the principle of data minimisation.

The provisions of Articles 15, 16, 18 and 21 of the Regulation on the rights of the data subject shall not apply where the personal data are only processed for scientific or historical research purposes or statistical purposes, in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes.

The provisions of Articles 15, 16, 18, 19 and 21 of the Regulation on the rights of the data subject shall not apply where the personal data are only processed for archiving purposes, in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes. Nevertheless, the data subject has the right to provide a statement to be kept with any documentation containing his or her personal data.

Data falling within this Act may be transferred to a public archive in accordance with the provisions of the Public Archives Act.

Article 19

Exception to the obligation to provide information on the processing of personal data by the authorities.

The obligation to provide information pursuant to Articles 13(3) and 14(4) of the Regulation shall not apply when a public authority transfers personal data to another public authority in the course of its statutory role in implementing the law and data is transferred only to the extent necessary to comply with the legal obligation of a public authority.

Article 20

Right to rectification, erasure, data portability, etc.

The data subject has the right to have inaccurate personal data concerning him or her rectified, as well as the right to obtain from the controller the erasure of personal data concerning him or her without undue delay (right to be forgotten) and the right to restriction of processing by the controller, as further stipulated in Articles 16 to 19 of the Regulation.

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, as further stipulated in Article 20 of the Regulation.

Article 21

Right of the data subject to object and the restricted registry of Registers Iceland.

The data subject has the right to object the processing of personal data concerning him or her, based on Article 6(1)(e) or (f), including profiling. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or if it is necessary for the establishment, exercise or defence of legal claims, as further stipulated in Article 21 of the Regulation. If the objection is just, the controller is prohibited to process the said data any further.

Registers Iceland shall keep a register of those who object to having their names used for marketing purposes. The Minister will lay down, following consultation with the Data Protection Authority, further rules on the establishment and use of such register and which information shall be included therein. Controllers directly involved in market penetration and controllers who use a register with names, addresses, electronic addresses, phone numbers and such, or transfer these to a third party in relation to such activities, shall, before using such registry for this purpose, compare the register to that of Registers Iceland in order to prevent the sending of direct mail or contact by phone natural persons who have already made their objection clear. The Data Protection Authority may authorise exemption from this obligation in specific cases.

Any use of a restricted registry pursuant to paragraph 2 is prohibited for other purposes than those described therein.

The name of the controller must be displayed clearly on any direct mail with information on who those opposing such mail or phone calls should contact. The recipient of direct mail has the right to know who provides the information used for such phone calls or mail. This does not apply to marketing by a controller of its own products and services on the basis of its own client lists, provided the material sent states its origins. If direct mail is sent electronically it must be stated unequivocally

upon its receipt what type of post it is. In other respects, the sending of such direct mail shall be in keeping with the Electronic Communications Act.

A controller may transmit its member, staff, student or client lists in relation to marketing activities. However, this only applies if:

1. the information transmitted does not include sensitive personal data;

2. each data subject has been given the opportunity to object, prior to transmission, that his or her data be displayed in the transmitted register;

3. this does not contravene applicable rules of procedures or instruments of incorporation of the controller concerned;

4. the controller investigates whether any of the data subjects has presented his or her objections to Registers Iceland, *cf.* paragraph 2, and, if that is the case, deletes the data of the person concerned before it transmits the register.

The provision of paragraph 5 shall not apply when transmission of a member, staff or client list for the distribution of direct mail is based on consent by the data subject, *cf.* Article 9(1) of this Act.

The provisions of paragraphs 2 to 5 shall apply, as the case may be, also to market surveys, consumer surveys and opinion polls.

Article 22

Rights related to individual decision-making based on automated processing.

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, as further stipulated in Article 22 of the Regulation, with the exceptions mentioned therein.

Chapter IV General Rules on the Obligations of Controllers and Processors and the Security of Personal Data.

Article 23

Responsibility of the controller.

A controller shall implement appropriate technical and organisational measures that take into account the nature, scope, context and purposes of processing as well as the risks for rights and freedoms of data subjects to ensure and demonstrate that processing of personal data of data subjects fulfils the requirements of the Regulation, as further stipulated in Articles 24 and 25 of the Regulation. When two or more act as joint controllers, they shall fulfil their duties in accordance with Article 26 of the Regulation.

Article 24

Data protection by design and by default.

A controller shall, both at the time of the determination of the means for processing and at the time of processing itself, implement appropriate technical and organisational measures designed to enforce data protection principles, and integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation and protect the rights of data subjects, as further stipulated in Article 25(1) of the Regulation.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed, as further stipulated in Article 25(2) of the Regulation.

Article 25

General rules on controllers.

Where processing of personal data is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of data subjects.

The processor shall not engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract or other legal act under law, 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, categories of data subjects and the obligations and rights of the controller, as further stipulated in Article 28 of the Regulation.

Article 26

Records of processing activities.

Each controller and processor and, where applicable, their representatives shall maintain a record of its processing activities. The provisions of Article 30 of the Regulation shall apply to information included in a record of processing activities, the form of the record, accessibility, etc.

The obligations referred to in paragraph 1 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal data as referred to in Article 11(1) of this Act, or personal data relating to criminal convictions and offences referred to in Article 12 of this Act.

Article 27

Security of personal data and notifications of breaches.

The controller and the processor shall implement appropriate technical and organisational measures to ensure adequate level of security of personal data 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, as further stipulated in Article 32 of the Regulation.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Data Protection Authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Furthermore, the processor shall notify the controller without undue delay after becoming aware of a personal data breach. The provisions of Article 33 of the Regulation shall apply to the content of such notification to the Data Protection Authority.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The provisions of Article 34 of the Regulation shall apply with regard to the content of such notification and exemptions from notification obligations.

Article 28

Cooperation with the Data Protection Authority.

The controller and the processor and, where applicable, their representatives shall cooperate, on request by the Authority, with the Data Protection Authority in the performance of its tasks.

Chapter V Data Protection Impact Assessment, Authorisation Requirement, etc.

Article 29

Data protection impact assessment.

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 natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, as further stipulated in Article 35 of the Regulation. A single assessment may address a set of similar processing operations that present similar high risks.

The Data Protection Authority shall make public a list[1)] of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

The Data Protection Authority may also make public a list of the kind of processing operations for which no data protection impact assessment is required.

[1)] *Notice 337/2019.*

Article 30

Prior consultation.

The controller shall consult the Data Protection Authority prior to processing, as further stipulated in Article 36 of the Regulation, where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Where the Data Protection Authority is of the opinion that the intended processing referred to in paragraph 1 would infringe the Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the Authority shall, within a period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in Articles 41 to 43 of this Act. That period may be extended by six weeks, taking into account the complexity of the intended processing. The Data Protection Authority shall inform the controller and, where applicable, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay. Those periods may be suspended until the Data Protection Authority has obtained information it has requested for the purposes of the consultation.

Article 31

Processing requiring authorisation.

In the case of processing of personal data for the performance of a task carried out in the public interest that may carry a specific risk of contravening the rights and freedoms of data subjects, the Data Protection Authority may decide that the processing shall only start once the Authority has checked the processing and approved it by issuing a special authorisation. The Data Protection Authority may decide that such authorisation requirement be suspended once general rules and security standards have been put in place that must be followed in such processing.

The Data Protection Authority shall lay down rules on processing requirements pursuant to paragraph 1.

Article 32

Requirements regarding the granting of authorisations, etc.

An authorisation may be granted to a controller pursuant to Article 31 of this Act only if it is likely that it will be able to fulfil its obligations pursuant to the Regulation and to this Act or instructions of the Data Protection Authority.

When granting authorisations pursuant to Article 31 of this Act, related to the processing of sensitive personal data, the Data Protection Authority shall consider whether the processing may cause such inconvenience for the data subject that will not be sufficiently remedied with the conditions stipulated pursuant to Article 33 of this Act. If such inconvenience might occur, the Data Protection Authority shall consider whether the interest related to the processing outweighs the interest of the data subject.

Article 33

Terms of the Data Protection Authority regarding the processing of personal data.

When a controller is granted an authorisation pursuant to Article 31 of the Act, the Data Protection Authority shall make this contingent upon the conditions it deems necessary in any given case to mitigate or prevent any possible inconvenience to the data subject related to the processing.

In assessing which conditions regarding processing should be put in place, the Data Protection Authority shall investigate *inter alia*:

1. whether it has been guaranteed that the data subject can exercise his or her rights pursuant to this Act, including withdraw his or her consent and, where applicable, have his or her personal data erased, as well as receive instruction on his or her rights and how to exercise these rights;

2. whether the personal data are sufficiently secure, reliable and updated in accordance with the purposes of the processing;

3. whether the personal data will be treated with the caution required by rules on professional secrecy and the purpose of processing;

4. whether a plan is in place as to how to inform and guide the data subject within reasonable limits considering the scope of the processing and other security measures applied;

5. whether security measures that are reasonable given the purpose of the processing have been adopted;

6. whether an impact assessment for data protection will be carried out prior to processing.

Article 34

Approval of scientific research in the health sector.

The Act on Scientific Research in the Health Sector governs approvals of scientific research in the health sector.

Chapter VI Data Protection Officers and Certification Bodies.

Article 35

Data protection officers.

The controller and the processor shall designate a data protection officer in every case where:

1. the processing is carried out by a public authority;

2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

3. the core activities of the controller or the processor consist of processing on a large scale of sensitive personal data or data relating to criminal convictions and offences.

A group of undertakings may appoint a single data protection officer provided that the data protection officer is easily accessible from each establishment. More than one authority may also appoint a single data protection officer taking account of their organisational structure and size.

The provisions of Articles 37 to 39 of the Regulation otherwise stipulate the competency of the data protection officer, his or her position and tasks.

Article 36

Data protection officer bound by an obligation of professional secrecy.

A data protection officer may not disclose any information brought to his or her knowledge in the course of his or her work and covered by the obligation of professional secrecy.

The obligation of professional secrecy shall, however, no longer apply if the data subject has given his or her consent for lifting the secrecy, and if it is necessary in regard to the function of the data protection officer.

Article 37

Certification and certification bodies.

The accreditation division of the Icelandic Intellectual Property Office may, following an opinion of the Data Protection Authority, accredit certification bodies issuing certification pursuant to Article 42 of the Regulation.

In other respect, the provisions of Article 42 and 43 of the Regulation, apply to the conditions for the accreditation of certification bodies, arrangements and content of the accreditation.

Chapter VII Supervision and Penalties.

Article 38

Organisation of the Data Protection Authority and administration.

The Data Protection Authority is an independent body with by a special Board of Directors. It does not accept instructions from the authorities or other bodies. Decisions of the Data Protection Authority pursuant to this Act will not be appealed to another authority although the parties to a case may bring their dispute before the courts following normal procedures.

The Minister appoints five people to the Board of the Data Protection Authority and an equal number in reserve for a term of five years at a time. Members of the Board may not be appointed for more the three consecutive terms. The Minister appoints the chairperson and his or her deputy chairperson without nomination and these shall all be legal professionals and fulfil the conditions of qualification of district court judges. The Minister in charge of internet security and telecommunications and the Minister of Health shall appoint one member of the Board each. In addition, the Icelandic Computer Society appoints one member of the Board who shall have professional knowledge in the field of computers and technology. Members of the Board and their deputies shall possess knowledge of matters related to data protection and be qualified in that area. The Minister determines the remuneration of members of the Board.

The Board has the task of shaping the policy in consultation with the Data Protection Commissioner and overseeing the activity and operation of the Data Protection Authority. Moreover, the Board shall make any major material or policy-making decisions in matters that are being processed by the Data Protection Authority, including regarding the imposition of daily fines and administrative fines. The Board of the Data Protection Authority shall stipulate further rules [1)] on the division of tasks between the Board and the Secretariat of the Authority and their implementation.

A member of the Board may be removed from the Board only on account of serious accusations or if he or she no longer meets the conditions required for his or her work.

If members of the Board do not agree, the matter in question shall be decided by a majority vote. If the votes are tied, the Chair shall have a deciding vote.

The Minister appoints the Data Protection Commissioner of the Data Protection Authority for a term of five years at a time following a proposal by the Board. The Data Protection Commissioner shall have a university degree and possess knowledge and experience in issues concerning data protection.

The Data Protection Commissioner shall attend Board meetings and has freedom of speech and the right to submit proposals.

The Data Protection Commissioner shall be responsible for and oversee the daily management of the activities, financial matters and operation of the Authority and employs its personnel.

[1)] *Regulation 876/2018.*

Article 39

Tasks of the Data Protection Authority.

The Data Protection Authority is a supervisory body pursuant to Chapter VI of the Regulation and shall oversee the implementation of the Regulation, this Act, special legal provisions concerning the processing of personal data and other rules on the subject.

Each data subject or his or her representative has the right to lodge a complaint with the Data Protection Authority if he or she believes that the processing of his or her personal data in Iceland, or pursuant to the special rules in Article 7 of this Act, infringes the Regulation or the provisions of this Act. Furthermore, a body, organisation or association pursuant to Article 80 of the Regulation may lodge a complaint with the Data Protection Authority if they have reason to believe that the rights of a data subject have been infringed. The Data Protection Authority determines whether an infringement has taken place.

The Data Protection Authority may address individual cases and make a decision on its own initiative or following a request by the person that believes that his or her personal data has not been processed in accordance with this Act and rules adopted pursuant to it or individual orders.

Other tasks of the Data Protection Authority include *inter alia*:

1. to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing personal data, as well as the awareness of controllers and processors of their obligations;

2. to advise the Althingi, the government and other bodies in the field of law-making and administration in relation to the protection of natural persons with regard to the processing of personal data;

3. upon request, to provide information to any data subject concerning the exercise of his or her rights under this Act and the Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

4. to cooperate with, including sharing information and provide mutual assistance to, supervisory authorities in other countries with a view to ensuring the consistency of application and enforcement of this Act and the Regulation;

5. to monitor developments in fields related to the protection of personal data, in particular the development of information and communication technologies and commercial practices;

6. to adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2) of the Regulation;

7. to establish and maintain a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to Article 35(4) of the Regulation;

8. to give advice on the processing operations referred to in Article 36(2) of the Regulation;

9. to encourage the drawing up of codes of conduct pursuant to Article 40(1) of the Regulation and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5) of the Regulation;

10. to approve the criteria of certification pursuant to Article 42(5) of the Regulation and, where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7) of the Regulation;

11. to draft and publish the criteria for accreditation of bodies for monitoring the implementation of codes of conduct pursuant to Article 41 of the Regulation and of certification bodies pursuant to Article 43 of the Regulation and carry out the accreditation of those bodies;

12. to adopt provisions, including in contracts, as referred to in Article 46(3) of the Regulation;

13. to approve binding corporate rules pursuant to Article 47 of the Regulation;

14. to contribute to the activities of the European Data Protection Board;

15. to keep records of infringements of the Regulation and of measures taken in accordance with Article 58(2) of the Regulation;

16. to publish an annual report on its operations;

17. to fulfil any other tasks related to the protection of personal data.

Article 40

Fees.

The Minister can establish a tariff stipulating a fee to be paid by the controller to the Data Protection Authority for the costs resulting from control of whether the controller fulfils the conditions of this Act and rules established pursuant to it or individual instructions. The tariff may also stipulate that the controller pay the costs of auditing activities aimed at preparing for the issuance of a processing permit and other services.

Article 41

Supervisory powers of the Data Protection Authority.

The Data Protection Authority shall have supervisory powers pursuant to Article 58(1) of the Regulation, including:

1. to order the controller and the processor and, as the case may be, their representatives to provide any information it needs to implement this Act and the Regulation;

2. to carry out an audit of the processing of personal data;

3. to carry out a review on certifications issued pursuant to Article 42(7) of the Regulation;

4. to notify the controller or the processor of an alleged infringement of the Regulation;

5. to obtain access from the controller and the processor to all data, including personal data, necessary for the implementation of this Act;

6. to access premises where the processing of personal data is carried out or data is stored, including any data-processing equipment; the Data Protection Authority may carry out any test or supervisory action it deems necessary and require necessary assistance from staff on such premises to implement a test or supervisory action.

The Data Protection Authority may request the assistance of the police if an attempt is made to obstruct it in its supervisory role.

Where it is revealed that the processing of personal data infringes the provisions of the Regulation, this Act or rules established pursuant to it, the Data Protection Authority can assign to the Chief of Police the task of temporarily halting the operations of the party and seal its place of operation without delay.

The right of the Data Protection Authority to require information or access to a place of operation and technical equipment shall not be limited with reference to the rules on professional secrecy.

Article 42

Orders of the Data Protection Authority regarding remedial measures.

The Data Protection Authority may lay down remedial measures, as further stipulated in Article 58(2) of the Regulation, for example:

1. issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the Regulation;

2. issue reprimands to a controller or a processor where processing operations have infringed provisions of the Regulation;

3. order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to the Regulation;

4. order the controller or processor to bring processing operations into compliance with the provisions of the Regulation, where appropriate, in a specified manner and within a specified period;

5. order the controller to communicate a personal data breach to the data subject;

6. restrict or prohibit the processing temporarily or permanently;

7. order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 of the Regulation and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 of the Regulation;

8. withdraw a certification or order the certification body to withdraw a certification issued pursuant to Article 42 and 43 of the Regulation;

9. order the temporary suspension of data flows to a recipient in a third country or to an international organisation.

Article 43

The granting of authorisations and provision of advice by the Data Protection Authority.

The Data Protection Authority has the following powers in regard to the granting of authorisations and provision of advice:

1. to advise the controller in accordance with the prior consultation procedure referred to in Article 36 of the Regulation;

2. to issue, on its own initiative or on request, opinions to the Althingi or the government or other bodies on any issue related to the protection of personal data;

3. to authorise processing where a prior authorisation is required by law;

4. to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) of the Regulation;

5. to give opinion on the accreditation of a certification body pursuant to Article 43 of the Regulation and adopt criteria in accordance with Article 42(5) of the Regulation;

6. to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2) of the Regulation;

7. to authorise contractual clauses referred to in point (a) of Article 46(3) of the Regulation;

8. to authorise administrative arrangements referred to in point (b) of Article 46(3) of the Regulation;

9. to approve binding corporate rules pursuant to Article 47 of the Regulation.

Article 44

Obligations of secrecy.

Members of the Board and staff of the Data Protection Authority, as well as others working on projects under the auspices of the Authority, are not authorised to disclose any information brought to their knowledge in the course of their work and covered by the obligation of professional secrecy.

Provisions on professional secrecy shall not prevent the Data Protection Authority from providing foreign data protection authorities with information when necessary so that the Authority or the foreign data protection authority can decide or carry out operations to ensure data protection.

In establishing terms pursuant to Article 33 of this Act, the Data Protection Authority may decide that the controller and the processor, as well as members of their staff, shall sign a declaration of professional secrecy regarding personal data brought to their knowledge in the course of processing such data. A controller or its representative shall attest to the signature of the employee and the date of such declaration and submit it to the Data Protection Authority within the prescribed time limit.

The obligation of professional secrecy pursuant to paragraphs 1 and 3 shall remain in force even after the employment ceases.

Article 45

Daily fines.

When the orders of the Data Protection Authority pursuant to Article 42(6), (7) and (9) of this Act have not been followed, the Authority may impose, before it imposes an administrative fine pursuant to Article 46 of this Act, daily fines on the party to which the orders apply until such time that the situation has been remedied in the Authority's opinion. The fines may amount to up to ISK 200,000 per each day passed or started without following the instructions.

If the decision of the Data Protection Authority on daily fines is appealed to the courts, daily fines shall not be imposed until the final judgment has been rendered. Daily fines shall be paid to the State Treasury and may be enforced without prior judgment.

Article 46

Administrative fines.

The Data Protection Authority may impose administrative fines on each controller or processor pursuant to paragraph 4 who infringes any of the provisions of the Regulation and this Act listed in paragraphs 2 and 3.

The administrative fines may amount to ISK 100,000 up to ISK 1.2 billion or, in case of a corporation, up to 2% of its annual overall turnover globally in the previous financial year, whichever is higher, when an infringement of the following provisions has taken place:

1. on the obligations of a controller and a processor pursuant to Articles 8, 25 to 39, 42 and 43 of the Regulation;

2. on the obligations of a certification body pursuant to Articles 42 and 43 of the Regulation;

3. on the obligations of the monitoring body pursuant to Article 41(4) of the Regulation.

The administrative fines may amount to ISK 100,000 up to ISK 2.4 billion or, in case of a corporation, up to 4% of its annual overall turnover globally in the previous financial year, whichever is higher, when an infringement of the following provisions has taken place:

1. on the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9 of the Regulation;

2. on the data subjects' rights pursuant to Articles 12 to 22 of the Regulation;

3. on the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49 of the Regulation;

4. if the obligation has not been fulfilled to give the Data Protection Authority access to all data and premises pursuant to Article 41 (1), points 5 and 6, of this Act;

5. if the orders of the Data Protection Authority have not been followed to restrict or prohibit the processing of personal data, rectify or erase them or prevent the flow of data pursuant to Article 42(6), (7) and (9) of this Act.

Fines may be imposed on natural persons and legal persons, including authorities and institutions falling within the scope of application of the Administrative Procedures Act.

Administrative fines will be imposed regardless of whether the violation is intentional or is the result of negligence.

Decisions on administrative fines shall be taken by Board of the Data Protection Authority and are enforceable. Collected fines are deposited to the State Treasury minus any collection costs. If administrative fines are not paid within a month of the decision of the Data Protection Authority, post-maturity interest shall be paid on the amount of the fine. The determination and calculation of post-maturity interest is subject to the Act on Interest and Price-Level Indexation.

The authorisation of the Data Protection Authority to impose administrative fines pursuant to this Act expires once five years have passed since the conduct in question was abandoned. The limitation period is interrupted when the Data Protection Authority notifies the entity of the onset of an investigation of an alleged violation. The interruption of a limitation period has legal effects vis-à-vis everyone involved in the violation.

Article 47

Issues affecting a decision to impose an administrative fine.

When deciding whether to impose an administrative fine and deciding the amount of the administrative fine in each individual case due regard shall be given to the following:

1. the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

2. the intentional or negligent character of the infringement;

3. any action taken by the controller or processor to mitigate the damage suffered by data subjects;

4. the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 of the Regulation;

5. any relevant previous infringements by the controller or processor;

6. the degree of cooperation with the Data Protection Authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

7. the categories of personal data affected by the infringement;

8. the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified it of the infringement;

9. adherence to the orders of the Data Protection Authority regarding remedial measures pursuant to Article 42 of this Act if orders on such measures have previously been directed at the controller or processor concerned on the same subject;

10. adherence to approved codes of conduct pursuant to Article 40 of the Regulation or approved certification mechanisms pursuant to Article 42 of the Regulation;

11. any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of the Regulation and this Act, the total amount of the fine shall not exceed the amount specified for the gravest infringement.

Article 48

Penalties.

A serious offence by a natural person is punishable by imprisonment of up to three years. An offence is considered serious when it is intentional and for profit in a particularly reprehensible manner and the personal data of a large number of data subjects covered by secrecy pursuant to law or on grounds of their very nature are disclosed to a third party or published.

If a representative of a legal person, its employee or another person acting on its behalf has committed an offence pursuant to paragraph 1 in connection with the operations of the legal person, the person concerned may be subject to penalties, as well as administrative fines being imposed on the legal person pursuant to Article 46 of this Act.

A breach by a natural person of professional secrecy pursuant to Articles 36 and 44 of this Act is punishable by fines or imprisonment of up to one year. If he or she has committed the offence in order to procure an unjustifiable advantage, this may be punishable by imprisonment of up to three years.

The provisions of Chapter VII A of the General Penal Code apply to the seizure of the proceeds from an offence and items used to commit such offence.

Article 49

Report to the police.

The Data Protection Authority shall assess whether the alleged offence of a natural person pursuant to Article 48 of this Act shall be reported to the police or whether the Authority will conduct an investigation which would be concluded with an administrative ruling. A report by the Data Protection Authority shall include a copy of the data upon which a suspected offence is based. The provisions of Chapters IV–VII of the Administrative Procedures Act do not apply to the decision of the Data Protection Authority to report a matter to the police.

The Data Protection Authority may provide the police and the prosecutor with information and data obtained by the Authority that are connected to an offence pursuant to Article 48 of this Act. The Data Protection Authority may participate in police operations concerning their investigation of these offences.

The police and the prosecutor may provide the Data Protection Authority with information and data obtained by them that are connected to offences pursuant to Article 48 of this Act. The police may also participate in operations of the Data Protection Authority concerning the investigation of offences specified in Article 46 of this Act.

If the prosecutor determines that there are no grounds for bringing legal proceedings on account of a possible criminal act that is also subject to administrative penalties, it may return the case to the Data Protection Authority for processing and ruling.

Article 50

Right against self-incrimination.

In a case involving a natural person, which may be concluded with the imposition of an administrative fine or a report to the police pursuant to Article 49 of this Act, the person has the right, if there is reasonable suspicion that this person has violated this Act, to refuse to answer any questions or surrender any documents or articles, unless the possibility that this could affect the outcome of a case brought against him or her can be excluded. The Data Protection Authority shall advise the suspect in regard to this right.

Article 51

Compensation.

If a controller or a processor has processed personal data in contravention to the provisions of the Regulation, this Act or rules adopted on its basis, or orders of the Data Protection Authority, it shall compensate the data subject for the financial damages he or she has suffered for this reason. However, a controller or processor will not be required to compensate for any detriment which it proves that can neither be traced to a mistake nor negligence on its behalf.

A processor shall, however, only be liable for the damage caused by processing where it has not complied with obligations of the Regulation and this Act specifically directed to processors or where it has acted outside or contrary to lawful orders of the controller.

Chapter VIII Entry into Force, etc.

Article 52

Regulations on the basis of the Act.

The processing of personal data and security measures in a particular sector or certain professions may be prescribed in a regulation.

Article 53

Entry into force.

This Act shall enter into force on 15 July 2018. …

Article 54

Amendments to other acts. …

Transitional provisions.

I.

The Minister appoints members of the Board of the Data Protection Authority in accordance with Article 38 of this Act when the term of the existing Board comes to an end.

II.

Regulations, as well as rules, orders and permits issued by the Data Protection Authority or the Minister on the basis of Act No. 77/2000, shall remain in force provided they are not inconsistent with this Act and the Regulation.

III.

Notwithstanding Article 4(6) of this Act, Article 1(2), Article 3, Article 4(1) to (5) and (7), Article 5, Article 7(1), Articles 8 to 13, Article 14(1) and (2), Article 14(3), points 1 and 3, Article 22, Article 23, Article 25, Articles 25 to 33, Chapter VI, Articles 38 to 45, Article 48 and Articles 51 to 53 of this Act on the processing of personal data concerning public security, national defence, state security and state activities in the area of criminal law shall apply until Directive (EU) 2016/680 of the European Parliament and of the Council has been implemented into Icelandic law. The provisions of Article 20(1) of this Act on the right of the data subject to have inaccurate, misleading or incomplete personal data relating to him or her rectified, also apply to the aforementioned processing and for the same period.

Attachment.

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).