Iceland - Health and Pharma Overview

TABLE OF CONTENTS

November 2019

1. INTRODUCTION

Icelandic health and pharmaceuticals legislation and data protection legislation are closely intertwined due to the sensitive nature of personal data often processed in the health and pharmaceuticals sectors. In many cases, health and pharmaceuticals sectoral law refers to data protection legislation as discussed in the sections below

lslation as discussed in the sections below.

Furthermore, the Icelandic data protection authority ('Persónuvernd') has issued rules regarding various subjects relating to privacy and security of personal data in the health and pharmaceuticals sectors (see section 1.2 below).

Persónuvernd also plays a role when certain licences or approvals are sought in the health and pharmaceuticals sectors. For example, Persónuvernd will submit an opinion when a licence to operate a biobank or health databank is sought.

Similarly, whenever an application is made for a scientific study in the health sector to the National Bioethics Committee and institutional review boards, these organisations will submit a summary of the application to Persónuvernd, which in turn reviews it, and may provide comments as well as determine that the study contravenes data protection legislation, in which case approval shall not be granted for the study.

1.1. Legislation

Although Iceland is not an EU Member State, it is a member of the European Free Trade Association ('EFTA'), and therefore participates fully in the internal market of the EU through the EEA Agreement. In order to achieve homogeneity of the EEA, EEA-relevant EU acts are incorporated into the EEA Agreement by the EEA Joint Committee. Accordingly, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') was incorporated into the EEA Agreement on 6 July 2018 by the Decision of the EEA Joint Committee ('JCD') No. 154/2018, and implemented into Icelandic law by Act No. 90/2018 on Privacy and Processing of Personal Data (only available in Icelandic here) ('the Data Protection Act'), which came into force on 15 July 2018. The GDPR was implemented with the so-called 'referral method', in accordance with Articles 2 and 5(3) of the Data Protection Act.

In addition to the GDPR and the Data Protection Act, the key acts governing the health and pharmaceuticals sectors in Iceland, and which are relevant to privacy and data protection, are the following:

- the Biobanks and Health Databanks Act No. 110/2000 ('the Biobanks Act')
- the Medicinal Products Act No. 93/1994 ('the Medicinal Products Act')
- the Act No. 16/2001 on Medical Devices
- the Patients' Rights Act No. 74/1997
- the Health Records Act No. 55/2009
- the Act No. 112/2008 on Health Insurance, implementing the Directive 2011/24/EU on the Application of Patients' Rights in Cross-Border Health Care

- the Act No. 44/2014 on Scientific Research in the Health Sector ('the Health Sector Research Act')
- the Medical Director of Health and Public Health Act No. 41/2007 ('the Public Health Act')

Furthermore, Persónuvernd has published the following rules:

- Rules No. 660/2019 on the Safety of Processing Personal Data in Health Databanks (only available in Icelandic here) ('the Processing Rules for Health Databanks')
- Rules No. 920/2019 on the Safety of Processing and Retention of Human Biological Samples in Biobanks (only available in Icelandic here)
- Rules No. 1100/2008 on the Processing of Personal Data for Genetic Investigations (only available in Icelandic here)

Finally, the following regulations published by Icelandic ministries that are applicable in the health and pharmaceuticals sectors are the following:

- Regulation No. 134/2001 on the Keeping and Utilisation of Biological Samples in Biobanks (only available in Icelandic here)
- Regulation No. 443/2004 on Clinical Trials on Medicinal Products in Humans (only available in Icelandic here) ('the Clinical Trials Regulation')
- Regulation No. 1188/2008 on the Quality and Safety when Treating Human Cells and Tissue (only available in Icelandic here)
- Regulation No. 441/2006 on the Collection, Treatment, Storage and Distribution of Blood (only available in Icelandic here)

1.2. Supervisory authorities

In Iceland, the supervisory authorities for privacy and data protection in the health and pharmaceuticals sectors are as follows:

- Persónuvernd, which is the supervisory authority responsible for monitoring the application of the GDPR, in accordance with Chapter VI of the GDPR
- the Icelandic Medicines Agency ('IMA'), the main functions of which are to issue marketing authorisations for medicines in Iceland in collaboration with regulatory authorities in the EEA, to ensure control and surveillance of the pharmaceutical industry in Iceland, and to contribute to making professional and unbiased information available to health professionals and consumers

- the Directorate of Health, the primary role of which is to promote high-quality and safe health care for the people of Iceland, to facilitate health promotion and to undertake effective disease prevention measures

1.3. Guidelines

The Directorate of Health has issued guidelines on the topic of safety of data processing when providing telemedicine services (only available in Icelandic here), as well as procedural guidelines when applying for data samples from health registers and other centralised registers from the Directorate of Health (only available in Icelandic here).

Persónuvernd has issued guidelines for those parties who maintain registers regarding handing over data for the purpose of scientific research (only available in Icelandic here).

1.4. Definitions

Sensitive Personal Data: Data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, biometric data, and data concerning a natural person's sex life or sexual orientation (Article 3(3) the Data Protection Act).

Health Data (1): Personal data related to the physical or mental health of a natural person, including healthcare services the person has received, and information regarding the use of medicinal products, alcohol and drugs (Article 3(3)(b) of the Data Protection Act).

Health Data (2): Information in health records, information and data from biobanks and health databanks, and other information on medical history and health (Article 3(14) of the Biobanks Act).

Genetic Data: Personal data relating to the inherited or acquired generic characteristics of a natural person, which give unique information about the physiology or health of that natural person, and which result in particular from an analysis of a biological sample from the person in question (Article 3(3)(d) of the Data Protection Act).

Biobank: A collection of biological samples which are permanently preserved (Article 3(5) of the Biobanks Act).

Biological Sample: Organic material from a human being, alive or deceased, which may provide biological information about him/her (Article 3(1) of the Biobanks Act).

Health Databank: A databank which has been licensed by the Minister to store health data which are acquired for scientific research, or which arise from such research (Article 3(16) of the Biobanks Act).

Scientific Research in the Health Sector: Research on human subjects, biological samples and health data in which scientific methods are applied in order to enhance knowledge of health and diseases (Article 3(1) of the Health Sector Research Act).

Consent: Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her (Article 3(8) of the Data Protection Act).

The Biobanks and Health Databanks Act defines two types of consent: 'informed, free consent' and 'assumed consent.' This distinction is further discussed in section 2.1.1. below.

Informed, Free Consent: Consent granted in writing, of the person's own free will, after the donor of a biological sample has been informed of the purpose of taking the sample, its usefulness, risks attendant upon the process, and that the biological sample will be permanently preserved in a biobank (Article 3(10) of the Biobanks Act).

Assumed Consent: Consent that consists in the donor of a biological sample not expressing any unwillingness for a biological sample taken from him/her for a clinical test to be permanently preserved in a biobank, provided that information in writing on this possibility has been available to him/her (Article 3(11) of the Biobanks Act).

Clinical Trial: Systematic testing of a medicinal product intended to discover or confirm its effect and/or to discover any adverse reactions to the medicinal product and/or to investigate the absorption, distribution, metabolism and excretion of the medicinal product for the purposes of evaluating its safety and effectiveness (Article 9 of the Medicinal Products Act) .

Clinical Investigation: Research on humans for the purpose of obtaining information and/or verifying that medical devices, in normal use, conform to basic requirements on characteristics and performance as provided for in relevant EU directives that have been adopted into the EEA Agreement (Article 3(4) of the Medicinal Devices Act).

2. CLINICAL RESEARCH AND CLINICAL TRIALS

The Health Sector Research Act applies to scientific studies in the health sector, carried out, in whole or in part, in Iceland. The National Bioethics Committee evaluates specific scientific research projects in the health sector to ensure that they are consistent with scientific and ethical principles. A scientific research project in the health sector may not be commenced unless it has been approved by the National Bioethics Committee or an institutional review board. The National Bioethics Committee or institutional review board shall evaluate the research protocol of a scientific research project from the perspectives of science, ethics and human rights. The National Bioethics Committee and institutional review boards may attach certain conditions to their approval of a research project. No alterations to the nature or scope of a scientific study, nor any other major alteration, may be made unless previously approved by the National Bioethics Committee or an institutional review board which approved the original research protocol.

The Clinical Trials Regulation contains requirements regarding clinical trials. Before a clinical trial is conducted, the National Bioethics Committee must evaluate it from a scientific and ethical standpoint. Furthermore, all clinical trials must be notified to Persónuvernd, and applications for clinical trials shall be sent to the IMA and the applicable review board. Any changes to the research plan that may affect the safety of participants or that may affect a trial's result must also be notified, as well as the completion of a clinical trial.

In addition to the above, clinical investigations regarding medical devices subject to the Act on Medicinal Devices are worth mentioning. Clinical investigations include assessments of undesired side-effects of medical devices. Such investigations are subject to approval by the IMA, which ensures that the conduct of the investigation is compatible with rules of good practice and rules on patients' rights, including provisions on research and on the evaluation of the National Bioethics Committee.

2.1. Data collection and retention

The processing of health data must be compliant with the provisions of the Data Protection Act. According to Article 3(3) of the Data Protection Act, health data, genetic and biometric data are considered sensitive data. Such data shall generally not be processed, according to Article 11 of the Data Protection Act. Nonetheless, Article 11 allows for some exceptions where the processing of sensitive data is authorised, for example:

- if the data subject has given explicit consent for the processing of personal data for one or more specified purposes;
- if the processing is necessary for reasons of public interest in the area of public health;

or

- if the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment, provided that the processing is permitted by law and is performed by a professional of such services who is bound by a duty of confidentiality.

Generally, prior notification of the processing of such personal data to Persónuvernd is not necessary according to the Data Protection Act. However, according to health and pharmaceuticals sectoral law, a licence for such processing is often required. For example, this is the case for biobanks, joint health information systems and scientific research in the health sector. This is also the case if the Medical Director of Health takes disease databanks, which were established before the enactment of data protection legislation, into safekeeping.

According to Article 4 of the Biobanks Act, the establishment and operation of a biobank and a health databank (i.e. the collection, keeping, handling, utilisation and storage of biological samples and health data, which are acquired for scientific research) is only permissible to those who have been granted a licence by the Minister of Health, who seeks the opinion of the Medical Director of Health, the National Bioethics Committee and Persónuvernd.

According to Article 20 of the Health Records Act, the consent of the Minister of Health is needed for two or more healthcare facilities, or premises of self-employed healthcare practitioners, to enter and store health records of patients treated by them in a joint health information system. The Minister shall only grant consent if a joint health system is demonstrated to be conducive to enhancing the security of patients in their treatment.

According to Article 27 of the Health Sector Research Act, the National Bioethics Committee or an institutional review board may authorise access to health information materials for approved scientific studies. Article 13 of the Act states that the National Bioethics Committee and institutional review boards must submit a summary of each application for a scientific study to Persónuvernd. The summary should provide information on the processing of personal data to be carried out for the study in question. Persónuvernd may require security measures to be applied to the handling of personal data. Should Persónuvernd find that the handling of personal data in the study contravenes the Data Protection Act, approval will not be granted.

According to Article 7 of the Clinical Trials Regulation, a notice of all clinical trials of medicinal products must be sent to Persónuvernd before they commence.

Finally, Article 8 of the Public Health Act is worth mentioning. The Article states that the Medical Director of Health must organise and maintain national registers on health, diseases, accidents, prescriptions, births, and the work and performance of the health service. The data in the registers should not be personally identifiable, except in registers of births, cardiovascular disease, neurological diseases, cancer patients, accidents, admissions to healthcare facilities, healthcare centres' contact, diabetes, and causes of death, where information on patients' names, identity numbers, and other personally identifying features may be recorded without the consent of the patient. Furthermore, the Medical Director of Health has the authority to take disease databanks, which were established before the enactment of data protection legislation into safekeeping. The processing of data from such databanks is subject to authorisation from Persónuvernd and the National Bioethics Committee.

2.1.1. Consent

According to Article 11 of the Data Protection Act, the processing of health data is permitted if the data subject has explicitly consented to the processing for one or more specified purposes. Pursuant to Article 10(1) of the Data Protection Act, the data controller shall be able to prove that the consent was given under valid conditions. Article 10(3) of the Data Protection Act permits the data subject to withdraw his/her consent at any time. However, the withdrawal does not affect the legitimacy of the processing prior to the withdrawal.

Further to the above, sectoral laws provide requirements concerning consent in relation to health and pharmaceuticals issues. The Biobanks Act allows for two types of consent, free, informed consent and assumed consent. When a biological sample is collected for preservation in a biobank of research samples, the free, informed consent of the person giving the biological sample shall be sought. However, Article 7(3) of the Biobanks Act states that the consent of a patient may be assumed for the storage of the biological sample when it is collected for the purpose of a clinical test or treatment, provided that the patient receives general information by a health care professional or health care institution.

A donor of a biological sample for preservation in a biobank of research samples can at any time withdraw his/her free, informed consent and the biological sample must subsequently be destroyed. Material that has been produced from a biological sample by performance of a research or the results of researches already carried out shall, however, not be destroyed. The donor of a biological sample may also revoke his/her assumed consent for a biological sample to be stored in a biobank of clinical samples, in which case it shall thereafter only be used in the interest of the donor of the biological sample or by his/her specific permission.

Children

The legislation contains certain deviations concerning minors' consent. Pursuant to Article 10(5) of the Data Protection Act, when a child is directly offered services online and the processing of children's personal data is based on its consent, the processing is only lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Further requirements are applicable for the consent of children for clinical trials in the Clinical Trials Regulation. Pursuant to the Clinical Trials Regulation, a parent or legal guardian must provide his/her consent if the child is under the age of legal competence, which is 18 years in Iceland. This also applies to adults who, due to mental incapacity, illness or other reasons specified by the regulation, are incapable of granting their own consent. Moreover, a trial concerning children or individuals who lack capacity to give consent may only be carried out if:

- the results of the trial could be of positive significance for the health of the individual concerned;
- a comparable clinical trial cannot be carried out on individuals with full capacity to give their informed consent; and
- the individual concerned is not opposed to participating.

Clinical trials

Pursuant to the Clinical Trials Regulation, prior written consent is required before a clinical trial is conducted. In addition, the data subject must be informed orally and in writing about the clinical trial and receive information, including about the sponsors of the trial, information about who will handle personal information, the purpose of the trial, and how it will be conducted, including expected benefits, duration and possible risks.

The data subject may at any time revoke his/her consent. Once consent is revoked, the participation of the individual concerned shall conclude immediately and unconditionally. The data subject may not in any way suffer retribution for a decision to cease participation.

2.1.2. Data obtained from third parties

Article 14 of the GDPR states that the data controller shall provide series of information to data subjects whose data are collected indirectly, for example:

- the identity of the controller;
- the purpose of the processing operation and its legal basis;
- the categories of personal data concerned;
- the recipients or categories of recipients of the data;
- the source of the data;
- the rights of individuals concerning these data (i.e. the right to object, access, erasure, restriction of processing, portability, rectification, the right to withdraw consent where the processing is based on the data subject's consent, and the right to lodge a complaint with a supervisory authority); and
- the existence of transfers outside the EU.

As mentioned above, pursuant to Article 8 of the Public Health Act, the Medical Director of Health organises and maintains national registers on health, diseases, accidents, prescriptions, births, and the work and performance of the health service. Access to these registers for researchers is granted when the conditions of Article 27 are met, namely that the National Bioethics Committee or an institutional review board has approved access.

Pursuant to Article 26 of the Medicinal Products Act, the Icelandic Health Insurance operates a database on the dispensing of medicinal products to patients, for the purpose of monitoring the cost of medicinal products and to process data on national consumption of medicinal products. Other parties may obtain information from the database for the purposes of instruction and research.

Access to medicinal files of a subject in a clinical trial is permitted, for the purpose of ensuring the quality of the clinical trial and when necessary for quality control, when the National Bioethics Committee or an institutional review board has approved access. When access is granted, it must be noted in the patient's journal, according to Article 22 of Clinical Trials Regulation.

3. PHARMACOVIGILANCE

The IMA explains pharmacovigilance as an important system which aims to improve the safety of medicinal products. Pharmacovigilance values and improves the safety of the medicinal product, after the marketing of the medicine. The IMA considers pharmacovigilance the most powerful tool it has at its disposal and often the only way to detect very uncommon adverse reactions. The results of pharmacovigilance are better information and instructions that reduce the risk and improve the benefit of the use of medicines.

.

Pursuant to the Medicinal Products Act, both the IMA and marketing authorisation holders are permitted and obligated to perform pharmacovigilance. Marketing authorisations holders are obligated to manage a pharmacovigilance system with the aim of monitoring the safety of medicinal products, assessing the possibility of minimising and preventing risk and taking appropriate measures when necessary.

Holders of marketing authorisations for medicinal products for human use may not publish information on product safety from the pharmacovigilance system without notifying the IMA, the European Medicines Agency and the European Commission, either beforehand or at the time of the publication. On the other hand, the IMA may demand that holders of marketing authorisations for medicinal products for human use publish product information concerning patient safety, including information on adverse effects which are suspected of being connected with products, or that they disseminate such information to a specific group of healthcare professionals.

4. BIOBANKING

According to the Biobanks Act, the establishment and operation of a biobank is only permissible to those who have been granted a licence by the Minister of Health. Before granting the licence, the Minister obtains an opinion from the Medical Director of Health, The National Bioethics Committee and Persónuvernd.

A licence for the establishment and operation of a biobank is contingent upon the following conditions:

- the biobank is located in Iceland;
- the objectives of the operation of the biobank and information on the operational basis of the biobank are clearly defined;
- a governing board has been nominated and one individual, with necessary expertise, is nominated to be responsible for the biobank;
- scientific samples and clinical samples, when both are stored in the same biobank, are clearly separated and labelled in such a way as to ensure that their keeping;
- storage, handling, and utilisation of scientific and clinical samples is in accordance with the Biobanks Act; and
- the evaluation of security and security measures, in gathering and handling of human biological samples, is consistent with the rules laid down by Persónuvernd, which have

been published and further enumerate the security conditions (only available in Icelandic here).

5. DATA MANAGEMENT

According to the Data Protection Act, the data controller is responsible for the processing of personal data, undertaken by or for him, and that the processing is consistent with applicable data protection rules and legislation. The data controller also bears the burden of proof in this regard. This includes that data processing needs legal ground, must be consistent with the main principles of the Data Protection Act (such as fair, transparent and lawful processing, purpose limitation and data minimisation), the data subjects must be sufficiently informed, and the security of the personal data must be guaranteed. Generally, no prior formalities are needed for the processing operations, but as previously mentioned in section 2.1 above, there are certain exceptions in the health and pharmaceuticals sectors.

Pursuant to Article 26 of the Data Protection Act, the data controller, the data processor and, if applicable, its representative, must hold a record of processing activities under their responsibility. Since health data is considered sensitive information according to Article 3 of the Data Protection Act , the data controller may need to carry out a Data Protection Impact Assessment before data is processed according to Article 29(1) of the Data Protection Act and Article 3 of Persónuvernd's Notice No. 828/2019 (only available in Icelandic here).

The data controller is obliged to take relevant technical and organisational measures to ensure sufficient security of personal data, with regards to the state of the art technology, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, according to Article 27 of the Data Protection Act. Security requirements increase with the degree of data sensitivity. In addition, Persónuvernd has issued safety rules that specifically apply for the processing of personal data in biobanks and health databanks (see section 1.2 above).

Sectoral law in health and pharmaceuticals often mandates the anonymisation of certain health data, such as the Biobanks Act, the Medicinal Products Act and the Public Health Act.

Furthermore, many health care professionals and health care institutions are required to appoint a data protection officer ('DPO'), pursuant to Article 37 of the GDPR, based either on them being a public body or their core activities involving the processing of sensitive personal data on a large

scale.

The Health Records Act contains instructions regarding access to individuals' health records. Pursuant to Article 12 of the Health Records Act, access to health records is prohibited except in circumstances provided for by the Act or other legislation. Health care professionals who are involved in a patient's treatment and require access to health records in connection with the treatment shall have access to health records. Such access may, however, be subject to restrictions. For example, access to especially sensitive health data shall be restricted to those health care professionals who necessarily require access to such data for the patient's treatment.

In addition, health care professionals may be granted access to such data on the basis of the patient's consent. A patient or his/her representative has the right to access his/her own health records in whole or in part, and to receive copies upon request, unless it is deemed not to be in the patient's interest. Access to health records of a deceased person may be granted to close relatives of the individual, such as their spouse, parent or descendant. The relative's interests in requesting such access, as well as the wishes of the deceased, if at hand, should be considered when a request for access to a deceased person's health records is assessed. Healthcare authorities which receive a complaint or appeal from a patient or his/her representative with respect to treatment for consideration, are entitled to access the patient's health records in the same manner as the patient.

6. OUTSOURCING

In the context of clinical trials, the Clinical Trials Regulation distinguishes between a principal investigator, investigator and sponsors. The principle investigator is the investigator responsible for the performance of a clinical trial at a trial site. If a trial has no sponsor the principal investigator shall also perform the tasks of the sponsor. The investigator is defined as a medical doctor or dentist who is authorised to perform a clinical trial. If only one investigator is performing a clinical trial, he/she shall be defined as the lead investigator. The principal investigator is responsible for the clinical trial in question and for any reports and notifications that must be made in connection with a trial. However, when a clinical trial is performed in collaboration with a sponsor, the sponsor shall participate in any work relating to such reports and notifications. The principal investigator is responsible for choosing, handling and monitoring the participants. The principal investigator and sponsor who sign the application for the clinical trial are responsible for ensuring that it is performed in accordance with applicable rules.

Sponsors and principal investigators may both be the data controllers of a clinical trial. They may also be regarded as joint data controllers in accordance with Article 26 of the GDPR. This will depend on their roles and responsibilities in connection with the trial in question and upon whether or not they jointly determine the purposes and means of processing. If they are joint controllers, they shall, pursuant to Article 26(1) of the GDPR, determine their respective responsibilities for compliance with the obligations under the GDPR in a transparent manner by means of an arrangement between them.

7. DATA TRANSFERS

A data controller may only transfer personal data outside Icelandic jurisdiction if the state provides a sufficient level of protection of personal data. According to Persónuvernd's Notice No. 228/2010 (only available in Icelandic here), EU and EFTA member states, Switzerland, Canada, Argentina, Guernsey, the Isle of Man, Jersey, Faroe Islands, Andorra, Israel, Uruguay and New Zealand provide a sufficient level of protection. A special agreement is in force with the United States, according to which personal data may be transferred from Iceland to parties in the United States that have been registered on the Privacy Shield list of the US Department of Commerce.

If the data controller wishes to transfer personal data to countries not mentioned above, exceptions in Article 49 of the GDPR are applicable to such transfers. Generally, the data controller would have to obtain the data subject's consent prior to the transfer, except in specific cases, for example when the transfer is necessary to ensure the protection of the data subject's life or the protection of public interest, or to meet obligation related to legal claims. Furthermore, according to Article 47 of the GDPR, an adequate level of compliance can be ensured by binding corporate rules, i.e. a code of practice for intragroup transfers.

In relation to health and pharmaceuticals sectoral law, it is worth pointing out, and was also briefly mentioned in section 4 above, that according to the Biobanks Act, one of the conditions for the establishment and operation of a biobank or health databank is that it must be located in Iceland.

8. BREACH NOTIFICATION

The Data Protection Act defines a personal data breach as 'a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal

data transmitted, stored or otherwise processed.'

As mentioned above, the data controller is obliged to take relevant technical and organisational measures to ensure sufficient security of personal data, according to Article 27 of the Data Protection Act.

When the data controller has a reasonable degree of certainty that a personal data breach has occurred, the Persónuvernd must be notified as soon as possible and preferably no later than 72 hours after becoming aware of the breach. If Persónuvernd is not notified of the breach within 72 hours, reasons for the delay shall follow the notification.

When the data controller receives information on or discovers a potential personal data breach, the data controller has a short period of time to evaluate if a breach has really occurred. According to guidelines issued by Persónuvernd on personal data breaches, the data controller is not considered to have become aware of a personal data breach in that investigative time period.

In case of a personal data breach, first reactions should also include an evaluation of risk for the data subjects concerned to establish whether they should be made aware of the breach, as the Data Protection Act requires that data subjects shall be notified of a personal data breach when it is likely to result in a high risk to the rights and freedoms of natural persons.

9. DATA SUBJECT RIGHTS

Pursuant to Section III of the Data Protection Act, and with reference to Chapter III of the GDPR, data subjects enjoy several rights in relation to their personal data. The data controller must provide information regarding the collection and processing of the data. Data subjects may also gain access to personal data concerning them and may receive copies of it. Furthermore, data subjects have the right to rectification of inaccurate personal data concerning them and to have incomplete data completed. Data subjects have the right to request from the data controller that their personal data be erased, that processing be restricted, and to data portability.

The abovementioned rights may be subject to restrictions, depending on the circumstances. For example, data subjects may only request erasure of their data in certain instances, such as when the processing of the personal data is no longer necessary or when the personal data have been unlawfully processed. Furthermore, in certain circumstances, data subjects cannot request erasure of their data, for example when processing is necessary for scientific research purposes in so far as

erasure would be likely to render impossible or seriously impair the achievement of the objectives of the processing. Restrictions to these rights may also be contained in sectoral law, such as the Health Records Act, as discussed in section 5 above.

As discussed in section 2.1.1., when the processing is based on the data subject's consent, the data subject may at any time revoke his/her consent. The data subject may not in any way suffer retribution for a decision to revoke his/her consent.

10. PENALTIES

The Data Protection Act differs in some ways from the GDPR with regard to penalties. According to the Data Protection Act, Persónuvernd may impose daily fines before issuing administrative fines until the infringement is remedied. Daily fines may be up to ISK 200,000 (approx. €1,477) for each day of infringement.

According to the Data Protection Act, Persónuvernd may also impose administrative fines. The amount varies between ISK 100.000 (approx. €736) and ISK 2.4 billion (approx. €17.7 million), or up to 4% of the global annual turnover of the entity in question, depending on the severity of the infringement. Administrative fines may be imposed on natural persons and legal entities as well as public bodies and institutions.

A natural person who has grossly infringed the Data Protection Act may be sentenced to imprisonment for up to three years. The same goes for representatives or employees of legal entities who have been imposed an administrative fine. DPOs, as well as board members, employees and contractors of Persónuvernd, who have breached their confidentiality obligations in accordance with the relevant provisions of the Data Protection Act, can also be fined or sentenced to imprisonment for up to three years, depending on the severity of the breach of confidentiality.

Health and pharmaceuticals sectoral law also contains penalty provisions. For example, according to the Medicinal Products Act, the IMA may issue reprimands, impose daily fines or halt or limit the infringing activities or use in question. In cases of repeated or major violations, punishment may consist of imprisonment for up to two years.

The Biobanks Act states that violation of its terms or of government directives based on it may lead to fines or imprisonment for up to three years. Similar penalty provisions may be found in the Health Sector Research Act.

11. OTHER AREAS OF INTEREST

Telemedicine

Telemedicine is not defined in Icelandic law and is not prominent in Icelandic health care. According to a parliamentary discussion on the topic in February 2019, the Ministry of Health is considering an increased focus on telemedicine in coming years. With the ever-growing use of technology in the healthcare sector, telemedicine will likely become a bigger part of Icelandic healthcare. The increased use of telemedicine will specifically affect medical services in rural areas of Iceland.

Medical devices

Section 2 above referred to medical devices, which are subject to the Act on Medical Devices and government directives derived from the Act. The Act applies to the manufacturing, sale, marketing, market surveillance, maintenance and use of medical devices and the surveillance of authorities of such devices.

Digital Health Records

According to the Health Records Act, health records shall be entered in electronic form as far as possible. Furthermore, an online platform was recently established where the general public can log in and view their own health records online at any time (i.e. without having to request such access). Information that can be viewed on the platform includes health information, doctor and hospital visits and prescriptions for medicinal products.

ABOUT THE AUTHORS

Erla S. Árnadóttir

LEX

Erla S. Árnadóttir is a supreme court attorney and partner at LEX. She is among the country's leading experts in the fields of intellectual property law and information technology law. During the past years, Erla has provided extensive services in the field of data protection law and has been working with many of the largest companies in the country, as well as some municipalities and official institutions in relation to the implementation of the General Data Protection Regulation in

Iceland.

Erla graduated with a cand. jur. degree from the University of Iceland in 1983. She studied corporate law and copyright law at a postgraduate level at the University of Oslo Faculty of Law in 1983–1984, and was a grantee at the Max Planck Institut für Patent-, Urheber- und Wettbewerbsrecht in Munich in 1988–1989. Erla was an alternative member of the board of the Icelandic Data Protection Authority during the years 1990 – 2004.

erlas@lex.is

Lena Markusdóttir

LEX

Lena Markusdóttir has worked as a lawyer at LEX since March 2017 and is specialised in the field of privacy and data protection. She assists LEX' clients, which include private entities, public bodies and municipalities, with complying with applicable data protection laws and regulations as well as serving as a Data Protection Officer and advising on various related matters. Lena graduated from Reykjavik University School of Law with an ML degree in 2014 and completed her bachelor's degree from the same faculty in 2012.

lena@lex.is

María Kristjánsdóttir

LEX

María Kristjánsdóttir is an attorney at law at LEX whose main focus is in the fields of intellectual property law, competition law and data protection law. Maria has several years' experience in data protection, specifically with respect to the GDPR. She has extensive experience in providing legal and strategic advice to clients in their GDPR implementation and related issues. These include private corporations, official bodies and municipalities. María currently serves as a Data Protection Officer for several of LEX' clients. María graduated with an ML degree from Reykjavík University in 2007 and completed an LL.M degree from Fordham University in 2008. That same year, she joined LEX and was admitted to the Icelandic Bar Association. Finally, María is active in the International Trademark Association (INTA) and is currently a member of the Data Protection Committee.

maria@lex.is

RELATED CONTENT

LEGAL RESEARCH

Healthcare Services Bill (Bill No. /2018).

LEGAL RESEARCH

Regulatory Guideline for Telehealth Products FAQ

LEGAL RESEARCH

Regulatory Guideline for Telehealth Products (2019)

LEGAL RESEARCH

Food, Medicine and Health Care Administration and Control Council of Ministers Regulation No.299/2013

LEGAL RESEARCH

Health Products (Medical Devices) Regulations 2010