DATA PROTECTION LAWS OF THE WORLD

Iceland

DLA PIPER

ICELAND

Last modified 11 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The GDPR was incorporated in the EEA Agreement by a Joint Committee Decision dated July 6, 2018. The Act No. 90 /2018 on Data Protection and the Processing of Personal Data (the ‘**DPA**’) implements the GDPR in Iceland. The law contains derogations and exemptions from the position under the GDPR in certain permitted areas.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The DPA defines a public authority or body in accordance with Article 1 of the Administrative Procedures Act no. 37 /1993. The term public authority refers to all parties, institutions, committees, etc. which are governed by state and local government.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Data Protection Authority (Icelandic: ‘*Persónuvernd*’) is the supervisory authority in Iceland for the purposes of Article 51 of the GDPR.

Contact details:
Persónuvernd – The Icelandic Data Protection Authority
Rauðarárstígur 10, 105 Reykjavík, Iceland.
Tel. +354 510-9600
postur@personuvernd.is
www.personuvernd.is

The Board of Directors and employees of the Data Protection Authority have an obligation of confidentiality in accordance with Chapter X of the Icelandic Administrative Procedures Act no. 37/1993. The same applies to others who work on behalf of the Authority.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

According to Article 31 of the DPA, controllers need to consult with and obtain prior authorization from the supervisory authority in relation to processing by a controller for the performance of a task carried out in the public interest.The GDPR generally implies certain withdrawal from the previous policy that processing of personal data may be based on licenses, but this Article in the DPA is an exception. The Data Protection Authority’s Rules no. 811/2019 on processing subject to authorization provides for a list of processing activities which are subject to the Authority’s written authorization, such as the transfer of sensitive personal data, which is stored with authorities, to third parties for research purposes.

Article 30 of the DPA implements the requirement to consult the supervisory authority in certain cases following a data protection impact assessment. Furthermore advertisement no. 828/2019 lists the processing activities that require a data protection impact assessment.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Iceland did not extend the requirement to appoint a Data Protection Officer, cv. Article 37(4) of the GDPR.

The DPA defines a public authority or body in accordance with Article 1 of the Administrative Procedures Act no. 37 /1993. The term public authority refers to all parties, institutions, committees, etc. which are governed by state and local government. According to the bill to the DPA, it is regarded desirable that companies entrusted with certain projects for the public interest designate a Data Protection Officer with regard to those projects. Such projects are for example in the field of public transport, road construction and energy utility.

The 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. Further, the Data Protection Officer has an obligation of confidentiality in accordance with Chapter X of the Icelandic Administrative Procedures Act no. 37/1993.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where 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 health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle

of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Criminal convictions and offences data (Article 10)

According to Article 12 of the DPA, processing of personal data relating to criminal convictions and offences is subject to certain conditions and the processing must be based on one of the legal basis in Article 9 of the DPA, cf. Article 6(1) of the GDPR.

According to Article 12(1) of the DPA, authorities may not process data relating to criminal convictions and offences unless it is necessary for the purpose of their statutory tasks.

According to Article 12(2) of the DPA, the data cannot be disclosed unless:

- the data subject has explicitly given its consent for the disclosure;
- disclosure is necessary for the legitimate interests of the public or private sector which obviously outweigh the interests of the confidentiality of the data, including the interests of the data subject; or
- the disclosure is necessary for the legitimate tasks of the relevant authority or for the authority’s decision or disclosure is necessary for public-sector projects that have been legally assigned to private parties.

Private entities cannot process information on criminal convictions and offences unless the data subject has given its explicit consent or the processing is necessary for legitimate interests which obviously outweigh the interest of the data subject.

Use of personal identification numbers

According to Article 13 of the DPA, 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.

Children's consent to information society services (Article 8)

Article 8(1) of the GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless member state law applies a lower age. The DPA reduces the age of consent for these purposes to 13 years for Iceland, cf. Article 10(5).

Data subject’s rights

The data subject has the right to be informed about the processing of his personal data, however, Article 17 of the DPA implements certain restrictions from these rights.

According to Article 17(3) of the DPA, Articles 13(1)-(3), 14(1)-(4) and 15 of the GDPR regarding the data subjects’ rights do not apply if the interests of individuals linked to the personal data, including the interests of the data subject itself, outweigh the interests of the data subject.

The rights granted to the data subject in Articles 13 – 15 of the GDPR can be restricted with a legislative measure if such a limitation of fundamental rights and freedoms constitutes necessary and proportionate measure in a democratic society to safeguard:

- national security;
- national defense;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security;
- other important objectives of general public interest, in particular those of economic or financial interest including monetary, budgetary and taxation matters, public health and social security;
- the protection of the data subject, the vital interests of the public or the fundamental rights of others;
- the enforcement of civil law claims; and
- legal obligation of professional secrecy.

The right to restrict the data subjects right also applies to personal data in working documents used in preparation for the controllers’ decisions if it has not been distributed to others, to the extent necessary to ensure the preparation of the proceedings.

Information regarding cases that are being processed by authorities may be exempted from access according to Article 15 (1) of the GDPR to the same extent as applies according to the Information Act no. 140/2012 and the Administrative Procedures Act no. 37/1993.

Rules No. 50/2023 on Electronic Surveillance

Rules No. 50/2023 on Electronic Surveillance apply to electronic monitoring in public places, as well as in workplaces, schools and other areas where a limited group of people usually moves around, i.e. in the common area of apartment buildings or on a common lot. The rules apply regardless of what type of equipment is used, such as surveillance cameras, web cameras, tachographs, positioning equipment or telemonitoring equipment. The rules set out requirements for the collection, distribution and storage of data collected by means of electronic surveillance. All processing of personal data must meet the requirements of GDPR on the basis of the provisions of the rules.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Article 16 of the DPA implements the provisions of GDPR on the transfer of personal data to third countries and international organisations into Icelandic national legislation. The same restrictions therefore apply as under the GDPR.

Furthermore advertisement no. 1155/2022 prescribes for the transfer of personal data to countries which have received an adequacy status from the European Commission.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Chapter IV of the DPA implements the provisions of the GDPR on security measures into Icelandic national legislation.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

A personal data breach is defined in the DPA as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Regarding the security of the processing and notification of a personal data breach, Articles 32, 33 and 34 of the GDPR are implemented into Icelandic national legislation via Article 27 of the DPA, without any alterations.

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.

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 Icelandic Data Protection Authority has issued guidelines for notifications of personal data breaches which are based on the instructions of the Article 29 Working Party and all such breaches, which are subject to the notification requirement, shall be notified to the Data Protection Authority via a centralized reporting portal.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Non-compliance with the instructions of the Data Protection Authority regarding a) temporary or definitive limitation including a ban on processing, b) rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed, or c) suspension of data flows to a recipient in a third country or to an international organization, can lead to daily fines until necessary improvements have been made. Fines can amount up to ISK 200,000 (approximately 1,320 euros) for each day that passes without the Data Protection Authority’s instructions being observed.

Breaches of the DPA and the GDPR can lead to administrative fines that are imposed by the Data Protection Authority. The administrative fines may amount to ISK 100,000 (approx. EUR 660) up to 1,2 billion ISK (approx. EUR 7,900,000), 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 provisions detailed in Article 83(4) of the GDPR has taken place.

The administrative fines may amount to ISK 100,000 to ISK 2,4 billion (approx. EUR 15,850,000) 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 provisions detailed in Articles 83(5)-83(6) of the GDPR, cf. Article 46 of the DPA, has taken place.

Major breaches can also lead to imprisonment up to 3 years and breach of confidentiality of a data protection officer can lead to fines or imprisonment up to 1 year and in severe cases, up to 3 years, cf. Article 48 of the DPA.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon,

the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Based on the Electronic Communications Act No. 70/2022 the use of electronic communications systems, including for email and other direct marketing, is only allowed if a subscriber has given prior informed consent.

If the email address has been obtained in the context of the sale of a good or service, the controller may use it for direct marketing of the controller’s own goods or services to customers who have not objected to receiving email marketing from the controller, provided the customers are given the opportunity, free of charge, to object to such use of their email address when it is collected and each time a message is sent.

Further, all marketing emails must include the name and address of the party responsible for the marketing.

ONLINE PRIVACY

Electronic Communication Data

The Electronic Communications Act No. 70/2022 provides that any processing of electronic communication data is prohibited, including storage, listening, recording or interception, unless it takes place with the informed consent of the user or as authorized by law.

Use of any kind of systems and equipment, including software that collects and/or stores information about the user's activities or interactions in his end equipment, provides access to information stored in his end equipment or monitors his activities is prohibited except with the informed consent of the user or as authorized by law. Despite this, the use of such equipment is permitted to gain access to information and / or to technical storage for legitimate purposes and with the knowledge of the user.

Cookies are considered to fall under the definition of equipment. If the use of cookies leads to the use of IP addresses or other personal data, the processing of such data must comply with the Data Protection Act. The processing is therefore not permissible without a legal basis.

The processing of electronic communication data may only be carried out by individuals who are under the control of telecommunications companies and in charge of invoicing or managing electronic communications traffic, user inquiries, reporting misconduct, marketing electronic communications services or value-added services, and the processing shall be limited to what is necessary for the benefit of such activities.

Electronic communication data stored and processed by a telecommunication company must be erased or anonymized when it is no longer needed for transmission of an electronic communication. However, telecommunications companies must keep a minimum record of data on users’ telecommunications for six months in the interest of criminal investigations and public safety.

Location Data

Location data and IP addresses are considered personal data under the Data Protection Act.

Information on the location of equipment in public electronic communications networks or electronic communications services may only be processed if it cannot be linked to individual users or with their informed consent. This does not apply to entities that provide emergency services and are officially recognized as such.

KEY CONTACTS

LOGOS Legal Services
www.logoslegalservices.com

Hjördís Halldórsdóttir
Attorney at Law, Partner
LOGOS
T +354 540 0300
hjordis@logos.is

Áslaug Björgvinsdóttir
Attorney at Law, Partner
LOGOS
T +354 540 0300
aslaug@logos.is

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.