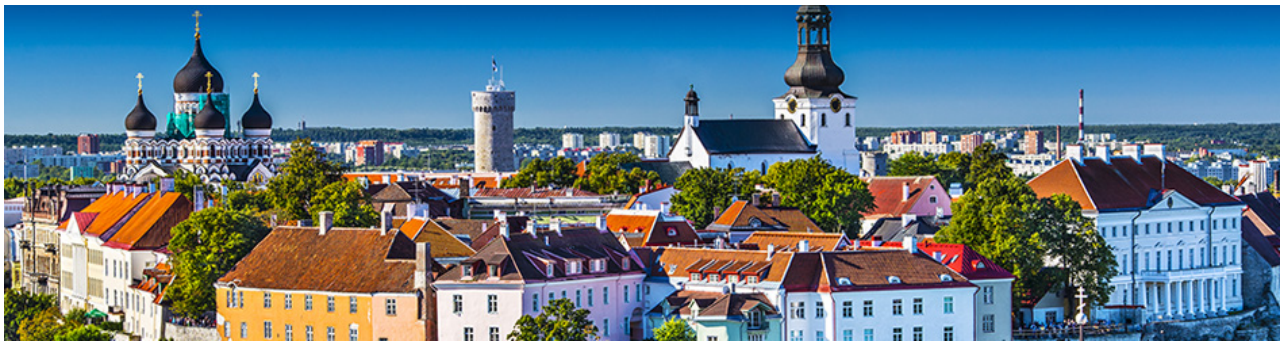
DATA PROTECTION LAWS OF THE WORLD

Estonia

DLA PIPER

ESTONIA



Last modified 19 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.

In Estonia, all derogations / additional requirements to the GDPR are provided in the new Personal Data Protection Act (PDPA) and the Personal Data Protection Implementation Act (Implementation Act).

The new PDPA was adopted by the Estonian parliament on December 12, 2018 and entered into force on January 15, 2019. The Implementation Act was adopted on February 20, 2019 and entered into force on March 15, 2019.

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 PDPA and the Implementation Act use the same definitions as the GDPR and do not foresee any new terms or terms defined differently from the GDPR.

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 PDPA specifies that in the meaning of Article 51(1) of the GDPR the independent supervisory authority of Estonia shall be the Estonian Data Protection Inspectorate (DPI). The PDPA further specifies the requirements for and appointing of the head of the DPI.

In addition to the tasks provided in Article 57 of the GDPR, the PDPA specifies that the DPI is competent to:

- raise awareness and understanding of the public, the controllers and processors about the risks of processing personal data, the standards and safeguards applicable to processing, and the rights related to the processing of personal data; The DPI may provide indicative guidance for this task;
- provide information to the data subject, upon request, about the exercise of his rights under this PDPA and, if necessary, cooperate with other supervisory authorities of the European Union Member States for this purpose;
- initiate, where necessary, misdemeanor proceedings and impose sanctions in the event where it is not possible to achieve compliance with the requirements provided by law or GDPR with the application of other administrative measures;

- cooperate with international data protection supervisory organizations and other data protection supervisory authorities and other competent authorities and persons of foreign states;
- monitor relevant trends insofar as they affect the protection of personal data, in particular the development of information and communication technology;
- participate in the European Data Protection Board;
- apply administrative coercion to the extent and pursuant to the procedure prescribed by law;
- submit opinions to the Estonian parliament, the Government of the Republic, the Chancellor of Justice and other institutions and the public on its own initiative or upon request on issues related to the protection of personal data;
- perform other duties arising from law.

In addition to the rights and powers under the GDPR the PDPA specifies that the DPI has the right to:

- warn the controller and the processor that the data processing activities are likely to violate the PDPA;
- demand the rectification of personal data;
- demand the deletion of personal data;
- demand restriction of processing of personal data;
- demand the termination of the processing of personal data, including destruction or archiving;
- implement organizational, physical and informational security measures for the protection of personal data without delay, if necessary, in accordance with the procedure provided for by the Substitutive Enforcement and Penalty Payment Act, if necessary, in order to prevent damage to the rights and freedoms of a person, unless personal data are processed by a public authority;
- impose a temporary or permanent restriction on the processing of personal data, including a prohibition on the processing of personal data;
- initiate state supervisory proceedings on the basis of a complaint or on its own initiative.

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.

Given that the GDPR does not provide for the registration of processing personal data, registries and systems will no longer exist. The PDPA specifies that pre-recorded data will remain as archived information about past activities for the term of up to five years after entry into force of the PDPA and upon expiry of the prior term (i.e. on 15 January 2024), pre-recorded data shall be erased.[1]

1: See Subsection 74(1) of the PDPA accompanied with Section 76 of the PDPA. PDPA is available in English here.

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.

In relation to DPOs, the PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

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 - *ie,* 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;
- 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 recognised 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. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. 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.

- Processing after data subject’s death. According to the PDPA the consent of the data subject is valid during the data subjects life and 10 years after the data subject’s death, unless otherwise provided by the data subject. If the data subject has died underaged, the data subject’s consent shall be valid for 20 years after his / her death. After the data subject’s death, the processing of his/her personal data is permissible upon the consent of one of the heirs of the data subject, unless:
    - 10 years have passed from the death of the data subject;
    - More than 20 years have passed from the death of an underaged data subject
    - Another legal basis for processing exists.

The aforementioned consent is not required when the processing includes only the data subject’s name, gender, time of birth and death, the fact of death, and the time and place of burial.

- Processing of personal data related to the breach of a contractual obligation. It is permitted to transfer personal data related to a breach of a contractual obligation to a third party, and the third party is permitted to process this personal data, with the purpose of assessing the creditworthiness of the data subject, or with another similar purpose, and only on condition that the controller or processor has checked the correctness of data, the legal basis for transfer and has registered the data transfer. Gathering data for the aforementioned purposes and transferring it to a third person is not permissible, if the data includes special categories of personal data, the data refers to the fact of being a victim of or committing an offence (before the public hearing, judgement or termination of proceedings), it would have a material adverse effect on the data subjects rights, or less than 30 days or more than 5 years has passed from the end of the breach of the obligation.

- Processing for journalistic purpose – GDPR article 85. It is permissible to process personal data without the data subject’s consent for journalistic purposes (primarily make information public in media) if public interest exists and such processing is done according to the principles of journalistic ethics. Such publicizing must not cause excessive damage to the rights of a data subject.

- Processing for the purposes of academic, artistic or literary expression – GDPR article 85. It is permissible to process personal data without the data subject’s consent for the purposes of academic, artistic or literary expression (primarily publication) if it does not cause excessive damage to the rights of the data subject.

- Processing of personal data in a public space. Unless the law specifies otherwise, in case of the recording of audio or photographic material in a public space, for the purpose of publicizing it, the consent of the data subject shall be replaced with the notification of the data subject in a form which enables him / her to acknowledge the fact of recording and to prevent himself / herself from being recorded. The notification obligation does not exist in case of public events, when the recording of these events for publicizing purposes can be reasonably expected.
- Processing for the purposes of scientific or historical research purposes or for the purposes of official statistics – GDPR article 89. It is permissible to process personal data for these purposes without the data subject’s consent in pseudonymized form or in a form that ensures at least equivalent level of data protection. De-pseudonymization or other measure of changing non-identifiable personal data to identifiable personal data is only permissible for further research or official statistics. The processor must name the person, who has access to the data that enables de-pseudonymization.
    - The processing of personal data without data subject’s consent in a form that the data subject is identifiable is only permissible when:
        - Pseudonymization would make it impossible to achieve the purposes of data processing, or they would be impracticably difficult to achieve;
        - The processor believes that an overwhelming public interest exists;
        - Based upon the processed personal data, the amount of data subject’s obligations are not changed and data subject’s rights are not excessively damaged in any other way.

- Where the scientific research is based on special categories of personal data, the ethics committee or the DPI will ensure the fulfillment of these obligations.

Analyses and researches of government institutions, done for the purposes of policy making, is also considered scientific research according to the PDPA.

- The processor or controller is entitled to limit data subjects’ rights stated in GDPR articles 15, 16, 18, 21 only to the extent that the enforcement of these rights would probably make the achievement of scientific or historical research purposes, or the purposes of official statistics, impossible or obstruct it considerably.
    - Processing for archiving purposes in the public interest – GDPR article 89. The processor or controller is entitled to limit data subjects’ rights stated in GDPR article 15, 16, 18, 19, 20, 21 only to the extent that the enforcement of these rights would probably make the achievement of the purposes of archiving in the public interest impossible or obstruct it considerably. Limiting data subjects’ rights is permissible to protect the records, their authenticity, credibility, integrity and usability.

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 defence 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 recognised 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.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

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.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

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.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

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).

Estonian law does not recognize administrative fines. This is also reflected in Recital 151 of the GDPR, stating that since the Estonian legal system does not allow for administrative fines as set out in the GDPR, the rules on administrative fines may be applied in Estonia in such a manner that the fine is imposed in misdemeanor proceedings if the applicable rules allow for the imposition of fines that are effective, proportionate and decisive.

Under the PDPA, the DPI may impose fines in misdemeanor proceedings of up to 20,000,000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Nevertheless, Estonia has been among the EU Member States imposing the lowest GDPR fines across the EU. This has been due to constraints arising from misdemeanor procedural law, which has resulted in virtually no misdemeanor fines being imposed for GDPR violations. Currently, most infringements have been dealt with in state supervision proceedings (i.e. administrative proceedings) which does not allow for the imposition of fines.

With regard to administrative proceedings, the DPI may issue precepts to data controllers and processors to order them to stop the infringing activities.

Upon failure to comply with a precept of the DPI, DPI may impose a non-compliance levy pursuant to the procedure provided for in the Substitutional Performance and Non-Compliance Levies Act. The upper limit for a non-compliance levy is 20,000,000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Further, if the precept issued by the DPI is not fulfilled, the DPI may turn to a superior agency, person or body of the processor of personal data for organization of supervisory control or commencement of disciplinary proceedings against an official.

Against the background of constraints arising from misdemeanor procedural law described above, the Estonian legislator initiated, in 2019, a draft law amending the Penal Code (which is also applicable to misdemeanor proceedings), in order to allow for more effective and decisive implementation of fines as required under EU law. The new law has now entered into force (as of 1 November 2023). The main changes that are relevant for the GDPR enforcement are the following:

- the statute of limitations for misdemeanor offences resulting from breaches of the GDPR has been prolonged from 2 years (which was the case prior to 1 November 2023) to 3 years, enabling the DPI to investigate potential infringements for a longer time;
- the general part of the Penal Code now explicitly states that the upper threshold of 400,000 euros for misdemeanor fines will not apply if lex specialis foresees fines that are calculated on a different basis and in a different amount, allowing to impose higher misdemeanor fines than 400,000 euros. Prior to the legislative amendments, the Penal Code stated that the maximum misdemeanor fine that could be applied under law was 400,000 euros. The interplay between the referred provision as lex generalis and the provisions implementing the GDPR fines as lex specialis has been unclear to this date and has not been interpreted by the courts within more than the 5 years that the GDPR has been applicable (and in offence proceedings, i.e., misdemeanor and criminal proceedings, such discrepancies in law must be interpreted in a way that is favorable to the person under investigation);
- the general provision regarding a legal person’s misdemeanor liability now states that a legal person is held liable if an infringement has been committed either: (a) by any natural person according to instructions given by the legal person’s body, its member, a senior official or a competent representative; or (b) due to the insufficient work organization or lack of supervision by the legal person. It is also clearly stated in the law that if a

legal person is obliged to act under the law, the legal person is responsible for its inactions or omissions irrespective of whether or not a natural person was also obliged to act. Prior to the legislative amendments, the Penal Code stated that a legal person could be held accountable only for an act that was committed in the interest of the legal person by its body, a member thereof or by a senior official or competent representative. Meaning that in misdemeanor proceedings arising from breaches of the GDPR, the DPI had to identify a natural person who has acted in the interests of a legal person and that this natural person has committed an act that fulfils all the criteria of a punishable offence.

The respective legislative amendments now significantly simplify imposing fines on legal person. Fines can now be applied based on these rules for such GDPR infringements that have been committed from 1 November 2023 onwards or that have continued from 1 November 2023 onwards.

As a stand-alone aspect from the above, the PDPA further specifies that the DPI is entitled to apply certain special state supervision measures to carry out the necessary state supervision, in addition the DPI is entitled to use the measures specified in Article 58 of the GDPR. The DPI may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of transmission of messages, unless identification of an end-user is otherwise impossible.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* 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.

Electronic marketing is regulated by the Electronic Communications Act. As a general rule, the data subject must be able to consent to the electronic marketing. The requirements for this consent depend on whether the addressee is a natural or a legal person, and whether there is an existing client relationship between the parties. Real time non-automated phone calls and regular mail are not considered electronic marketing under Estonian law.

The customer consent must be obtained separately from other terms of the contract between the parties – i.e. it cannot be obtained in the standard terms presented to the customer (*eg,* 'By accepting these terms you agree to receive our commercial communications at the email address provided to us'). In practice, a checkbox separate from the acceptance of the standard terms is often used to obtain this consent.

An opt-in consent is required if the addressee is a natural person, except in the case of an existing client relationship, where opt-out is permissible. The message itself must always include information to clearly determine the person on whose behalf the marketing is sent, clearly distinguishable direct marketing information and clear instructions on how to refuse to receive further direct marketing (*eg,* an unsubscribe link).

Reliance on an opt-out (for natural persons) in the framework of existing client relationships is subject to the following additional requirements:

- the same entity has obtained the contact details in the course of a sale;
- the direct marketing is in respect of similar goods or services;
- the recipient was given a possibility to opt out at the collection of his / her personal data;
- the message must include information to clearly determine the person on whose behalf the marketing is sent; and
- the message must include clearly distinguishable direct marketing information and the recipient is given a simple means in each subsequent email to opt out/unsubscribe.

If the addressee is a legal person, the opt-out system is applicable. There is no need to obtain a prior consent for direct marketing, but:

- the message must include information to clearly determine the person on whose behalf the marketing is sent;
- the message must include clearly distinguishable direct marketing information; and
- the recipient is given a simple means in each subsequent email to opt out / unsubscribe.

ONLINE PRIVACY

Traffic data and location data

Traffic data retention requirements apply only to communications undertakings. Providers of telephone or mobile telephone services and telephone network and mobile telephone network services, as well as providers of Internet access, electronic mail and Internet telephony services are required to preserve for a period of one year network traffic data, location data and associated data thereof which is necessary to identify the subscriber or user in relation to the communications services provided.

Cookies

Due to the opt-out system, consent to cookies is not needed. The law does not refer specifically to browser settings or other applications to be adopted in order to exercise the right to refuse.

The PDPA specifies, that if GDPR article 6(1)(a) is used with regard to providing information society services directly to a child, then the processing of the child’s personal data is permitted if the child is at least 13 years old. If the child is younger, then processing is permissible only if and in the extent to which the child’s legal representative has agreed to.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kaupo Lepasepp
Partner
Sorainen
T +372 6 400 939
kaupo.lepasepp@sorainen.com

Mihkel Miidla
Partner, Head of Technology & Data Protection
Sorainen
T +372 6 400 959
mihkel.miidla@sorainen.com

Liisa Maria Kuuskmaa
Senior Associate
Sorainen
T +372 6 400 900
liisa.kuuskmaa@sorainen.com

DATA PRIVACY TOOL

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