DATA PROTECTION LAWS OF THE WORLD

Finland

DLA PIPER

FINLAND

Last modified 4 January 2023

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.

Finland has passed a supplementary implementation act of the GDPR, the Data Protection Act of Finland *(Tietosuojalaki)*, which entered into force on January 1, 2019.

Other key Finnish laws concerning data privacy and protection are: the Act on Electronic Communication Services 917 /2014 *(Laki sähköisen viestinnän palveluista)* of January 1, 2015, which aims to, inter alia, ensure the confidentiality of electronic communication and the protection of privacy; the Act on the Protection of Privacy in Working Life 759/2004 (‘Working Life Act’) *(Laki yksityisyyden suojasta työelämä ssä)*, which aims to promote the protection of privacy and other rights safeguarding the privacy in working life, and; the Act on the Processing of Personal Data in Criminal Cases and in connection with Maintaining National Security 1054 /2018 *(Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä)*, which entered into force on January 1, 2019 along with the Data Protection Act.

The Working Life Act includes some specific provisions on privacy issues relating to employment and work environments such as right to monitor employees’ email communication. The protection of employees’ privacy has traditionally been strict in Finland and Finland uses the national leeway provided in the GDPR with regard to processing of personal data in the context of employment and maintains the specific law concerning privacy in working life.

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 definitions in Finland are the same as in the GDPR and no additional local definitions have been included.

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.

In Finland The Office of the Data Protection Ombudsman (*Tietosuojavaltuutetun toimisto*) is the local supervisory authority. The Office of the Data Protection Ombudsman contains the Data Protection Ombudsman himself, two Assistant Data Protection Ombudsmen as well as various data protection experts and secretaries as public servants.

Post address: P.O. Box 800, 00531 Helsinki Finland

Visiting address: Lintulahdenkuja 4, 00530 Helsinki Finland

T +358 29 56 66700

tietosuoja@om.fi

www.tietosuoja.fi

The Data Protection Act specifies the Data Protection Ombudsman’s duties and rights under the GDPR regarding *e.g.,* audits, right to receive information and right to impose sanctions on entities.

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.

The Finnish Data Protection Act does not contain any provisions related to registration. The former Finnish Personal Data Act did contain some requirements for registration, but these have been repealed.

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 Finland the new Data Protection Act does not contain specific local requirements on data protection officers. However, few special national acts stipulate mandatory appointment of data protection officers.

For example, in Finland all functional units of healthcare and social welfare as well as pharmacies must appoint a data protection officer under the Act on Electronic Prescriptions 2007/61 *(Laki sähköisestä lää kemääräyksestä),* and under The Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007) *(Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä kä sittelystä)*.

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 defense 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 authorised 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 pseudonymisation.

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.

Finland has used the national leeway provided in GDPR article 6(1) subsection e) as well as GDPR article 9(2) subsections b), g), h), i) and j) regarding collecting and processing personal data in certain situations.

In Finland, personal data may be processed under GDPR article 6(1) e) when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, if:

it relates to information representing a person’s position, tasks and the processing thereof in the public sector entity, business life or other equivalent activity, the purpose of processing rests on the public interest grounds and it complies with the principle of proportionality;

- it is necessary in the operation of authorities in order to perform a task in public interest and it complies with the principle of proportionality;
- it is necessary for scientific or historical research or statistical purposes and it complies with the principle of proportionality; or
- the processing of research material, material related to cultural heritage and any description information thereof for archiving purposes is necessary on public interest grounds and complies with the principle of proportionality.

The processing of special categories of personal data under GDPR article 9(2) subsections b), g), h), i) and j) may be carried out in Finland if it concerns, by way of example:

- personal data of the insured person or a claimant within the operation of an insurance company to settle its liability;
- health and medical data in connection with certain operations of healthcare and social welfare service providers; or
- processing for scientific or historical research purposes or statistical purposes.

In addition to the above-mentioned processing activities, the national leeway has also been used in the Data Protection Act with respect to processing related to criminal convictions and offences as well as processing of national identification numbers. For example in relation to national identification numbers, processing is only allowed based on data subject consent or if it is necessary to unambiguously identify the data subject for: a) a task defined in law, b) realization of the rights and responsibilities of the data subject or data controller, or c) historical or scientific research or statistical purposes. Further, national identification numbers can be processed for e.g. credit, loan, insurance, debt collection, payment service and leasing purposes, in social or healthcare services, and in connection with employment relatioships.

The Working Life Act sets additional processing requirements to employment related data that an employer collects and processes of its employees. All employee personal data processed must at all times be directly necessary for the employee’s employment relationship. This necessity requirement cannot be bypassed even with the employee’s consent.

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.

The new Data Protection Act does not include additional clauses concerning transfer of personal data, *ie,* Finland has decided not to use the marginal national leeway provided in GDPR articles 46 and 49 as per now.

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 new Finnish Data Protection Act does not contain any direct additional requirements for the security of processing in the meaning of GDPR article 32. However, the Data Protection Act does specify the security measures to be taken if special categories of personal data are processed. These measures are mostly the same as included in the GDPR article 32 (*eg,* pseudonymization, encryption, personnel training, access management, log-on data usage), and according to the government proposal explanatory text serve more as examples of what measures must be taken rather than an exhaustive mandatory list despite the wording used.

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.

In Finland the general breach notification procedure follows the rules set by GDPR.

Personal data breaches must be reported to the Office of the Data Protection Ombudsman. The report can be made to the Office of the Data Protection Ombudsman through their website.

However, certain special national legislation does include additional requirements on breach notifications. The Act on Electronic Communication Services establishes an obligation for telecommunications operators to notify their subscribers, users and the Finnish Transport and Communications Authority (‘*Traficom*’) of significant information security violations or threats and of anything else that prevents or significantly interferes with communication services. In addition, under the Act on Electronic Communication Services, domain name registrars shall notify *Traficom* without undue delay of significant violations of information security in its domain name services and of anything that essentially prevents or disturbs such services.

The Act on Strong Electronic Identification and Electronic Signatures (2009/617) (*Laki vahvasta sähkö isestä tunnistamisesta ja sähköisistä luottamuspalveluista*) also states that an electronic identification service provider shall notify service providers using its services, identification device holders as well as *Traficom* of severe risks and threats to its data security.

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).

In Finland, the Data Protection Ombudsman and the Deputy Data Protection Ombudsmen supervise compliance with GDPR and the Finnish Data Protection Act. In addition, an Expert Committee provides statements on significant questions and matters related to data processing upon the request of the Data Protection Ombudsman.

The Data Protection Ombudsman may order a data controller or data processor to comply with certain articles of the GDPR as well as Section 18 of the Data Protection Act, which covers the Data Protection Ombudsman’s right to receive necessary information, and impose a default fine to make the order more effective. However, the default fine may not be imposed on a natural person due to them not complying with the section on the Data Protection Ombudsman’s right to receive information if the person is suspected of a crime and the information is related to the alleged crime.

Administrative fines defined in article 83 of the GDPR will be issued by a sanction board within the Office of the Data Protection Ombudsman. The sanction board consists of the Data Protection Ombudsman and the two Deputy Data Protection Ombudsmen and the decision shall be made as a majority decision. Finland has decided to use the provided national leeway and the Act regulates that the administrative fines cannot be issued to:

- state authorities;
- state-owned businesses;
- local authorities;
- independent public institutions;
- organs operating in connection with the Parliament;
- the Office of the President of the Republic; or
- the Evangelical Lutheran Church of Finland or the Orthodox Church of Finland or the parishes, associations of parishes or other bodies thereof.

In addition, criminal sanctions can ensue from breaches of data protection laws in Finland as the Criminal Code of Finland 39/1889 (*Rikoslaki*) includes several data processing, data privacy, confidentiality and data security related offences or crimes. Finland has also introduced a punishable offence, the data protection offence, to the Criminal Code of Finland based on the GDPR. If the controller or data processor commits a data protection offence, the punishment is a fine or up to one year of imprisonment. The Criminal Code also states that the prosecutor is obligated to hear the Data Protection Ombudsman before bringing charges against a controller or data processor for a data protection offence.

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.

The Act on Electronic Communication Services regulates direct marketing by electronic means in Finland. The Data Protection Ombudsman is the supervising authority also in compliance issues with the Act on Electronic Communications Services’ provisions concerning direct marketing.

Direct marketing to natural persons is only allowed by means of automated calling systems, facsimile machines, or email, text, voice, sound or image messages and only if the natural person has given his / her prior consent to it. Direct marketing using other means is allowed if the natural person has not specifically forbidden it. If, however, a service provider receives an email address, number or other contact information in relation to the sale of product or service, the service provider may normally use this contact information to directly market the service providers own products or services belonging to the same product group or that are otherwise similar to the natural person in question. The natural person must be able to easily and at no charge unsubscribe from or prohibit any direct marketing and the service provider must clearly inform the natural person of that possibility.

A service provider may use direct marketing with legal persons (businesses) unless they have specifically prohibited it. As with natural persons, legal persons must also be able to easily and at no charge unsubscribe from/prohibit any direct marketing and the service provider must clearly inform the legal person of that possibility. In addition, telecommunications operators and corporate or association subscribers are entitled, at a user’s request, to prevent the reception of direct marketing.

The Data Protection Ombudsman and the Finnish Customer Marketing Association have given their interpretations on B2B direct marketing using a legal person’s general contact information, such as an email address (e.g. info@company.com). If the B2B direct marketing is sent to a legal person’s employee’s personal work email (fistname.lastname@company.com), the person’s prior consent is required unless the marketed product or service is substantially related to the person’s work duties based on the person’s job description.

Email, text, voice, sound or image message sent for the purpose of direct marketing must be clearly and unmistakably be recognized as direct marketing. It is forbidden to send such a direct marketing message that:

- disguises or conceals the identity of the sender on whose behalf the communication is made;
- is without a valid address to which the recipient may send a request that such communications be ended;
- solicits recipients to visit websites that contravene with the provisions of the Consumer Protection Act 20.1.1978 /38 (*Kuluttajansuojalaki*).

If any processing of personal data is involved in the electronic direct marketing, the provisions of the applicable data protection laws (such as the Finnish Data Protection Act and the GDPR) will also apply.

ONLINE PRIVACY

The Act on Electronic Communication Services 917/2014 *(Laki sähköisen viestinnän palveluista)* regulates online privacy matters such as the use of cookies and location data.

Cookies

A service provider is allowed to save cookies and other data in a user’s terminal device, as well as use such data, only with the consent of the user. The service provider must also give the user clear and complete information on the purposes of use of cookies.

However, the above restrictions do not apply to use of cookies only for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

In April 2021, Helsinki Administrative Court ruled in its decision that the competent supervisory authority in cookie consent issues is Transport and Communications Agency Traficom, not the Office of the Data Protection Ombudsman. However, the Office of Data Protection Ombudsman remains competent supervisory authority in other cookie matters.

Traficom published in September 2021 a guideline “Instructions for service providers” updating its instructions on cookie implementation on consent collection. For consent to meet the requirements set in the GDPR, users must have the

opportunity to choose whether to accept or reject the terms offered. Consent can be given in a variety of ways, as long as it clearly indicates that the data subject accepts the proposal for the processing of their personal data. Valid consent cannot be given through silence, pre-ticked boxes or inactivity. Refusing and withdrawing consent must be as easy as giving consent. The controller must also be able to demonstrate the consent afterwards.

Location Data

The location data associated with a natural person can be processed for the purpose of offering and using added value services, if;

- the user or subscriber, whose data is in question, has given his / her consent;
- if the consent is otherwise clear from the context; or
- is otherwise provided by law.

In general, location data may only be processed to the extent necessary for the purpose of processing and it may not limit the privacy any more than absolutely necessary.

The added value service provider shall ensure that:

- the user or subscriber located has easy and constant access to specific and accurate information on his / her location data processed, purpose and duration of its use and if the location data will be disclosed to a third party for the purpose of providing the services:
- the above mentioned information is available and accessible to the user or subscriber prior him / her giving his/her consent;
- the user or subscriber has the possibility to easily and at no separate charge cancel the consent and ban the processing of his / her location data (if technically feasible).

The user or subscriber is entitled to receive the location data and other traffic data showing the location of his/her terminal device from the added value service provider or the communications provider at any time.

KEY CONTACTS

Markus Oksanen
Partner
T +358 9 4176 0431
markus.oksanen@fi.dlapiper.com

DATA PRIVACY TOOL

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