DATA PROTECTION LAWS OF THE WORLD

Lithuania

DLA PIPER

LITHUANIA

Last modified 18 January 2024

LAW

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

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

Territorial Scope

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

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

The implementation of the GDPR has been achieved in the Republic of Lithuania. The Law on Legal Protection of Personal Data (hereinafter ‘Data Protection Law’) has been in force since July 16, 2018.

The Data Protection Law replaced the previous Law on Legal Protection of Personal Data which implemented the EU Data Protection Directive (Directive 95/46/EC).

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 Data Protection Law refers to the definitions provided by the GDPR. Only two definitions: ‘direct marketing’ and ‘institutions and authorities’ are defined differently in the Data Protection Law.

Under the Data Protection Law, 'direct marketing' means any activity consisting of offering goods or services or asking opinion on the goods or services offered, by post, telephone or other direct means.

'Institutions and authorities' means state and municipal institutions and authorities, enterprises and public institutions, financed from state or municipal budgets and state monetary funds and authorized by the Law on Public Administration of the Republic of Lithuania to perform public administration activities or to provide public or administrative services to persons or to perform other public functions.

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.

There are two supervisory authorities in Lithuania: the State Data Protection Inspectorate and the Inspector of Journalist Ethics. The State Data Protection Inspectorate is responsible for monitoring the application of the GDPR and the Data Protection Law as well as ensuring these acts are applied, except where it is within the competence of the Journalist Ethics Officer. The Journalist Ethics Officer performs the same functions where the personal data is processed for

journalistic purposes and for academic, artistic or literary expression, except for tasks and powers listed in Article 57(1) (j) to (l) and (n) to (t), Article 58(1) (b) to (c), Article 58(2) (e), (g), (h) and (j), and Article 58(3) (a), (c) and (e) to (j) of the GDPR.

In addition to the tasks established in the GDPR, the Data Protection Law authorizes the State Data Protection Inspectorate to perform the following tasks:

- To provide advice to data subjects, data controllers and processors on the protection of personal data and privacy protection, and also to develop methodological recommendations for the protection of personal data and to publish them publicly on their website
- To cooperate with personal data protection supervisory authorities of other countries, European Union institutions and international organizations and to take part in their activities
- To participate in the formation of state policy in the field of personal data protection and to implement it
- To implement the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its Protocols
- To perform other functions specified in the Data Protection Law and other legal acts

In addition to the powers established in the GDPR, the Data Protection Law authorizes the State Data Protection Inspectorate to:

- Receive all necessary information, copies of documents and duplicates, and copies of the data from the data controllers and data processors, state and municipal institutions and bodies, other legal and natural persons; as well as access to all data and documents which are necessary for the execution of tasks and functions of the State Data Protection Inspectorate
- During the investigation of the infringements to enter the premises of the person or entity which is subject to the inspection and to exercise similar actions with respect to related persons or entities
- Participate in meetings of the Parliament, the Government, and other state institutions when issues related to the protection of personal data or privacy are being considered
- Invite experts and consultants, to form working groups on examination of processing or protection of personal data, preparation of personal data protection documents and to deal with other issues which fall under the competence of the State Data Protection Inspectorate
- Provide recommendations and instructions to data controllers, data processors and other legal or natural persons regarding the processing of personal data or the protection of privacy
- Exchange information with other countries' personal data protection supervisory authorities and international organizations to the extent necessary for their functions
- Participate in court hearings when infringements of international, European Union or national law provisions on personal data protection issues are being considered
- Use technical measures during the investigation of infringements
- Receive oral and written explanations from legal entities and natural persons during the infringement proceedings and to demand that they arrive to provide explanations to the premises of the State Data Protection Inspectorate
- Use the information held by the State Data Protection Inspectorate, including personal data obtained during the investigation of infringements or received by the State Data Protection Inspectorate for other functions
- Involve police officers in order to ensure the possible use of violence and in order to maintain public order
- Perform other functions specified in the law

More information and contact details of supervisory authorities are available at:

- State Data Protection Inspectorate
- Inspector of Journalist Ethics

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 (*eg,* 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 data processing activities, registries and related systems no longer exist.

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
- 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 penalized 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
- 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.

The Data Protection Law does not determine any derogations from the requirements which are set in the GDPR regarding data protection officers.

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 (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 (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (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 (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (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
- 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
- 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
- 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, while 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
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.

The Data Protection Law contains provisions on specific conditions related to the processing of national identification number.

Article 3 of the Data Protection Law determines particularities of the processing of the personal code:

- Personal code can be processed if there is at least one of the conditions for the lawfulness of the processing of personal data referred to in Article 6(1) of Regulation (EU) 2016/679
- It is forbidden to disseminate the personal code
- It is forbidden to process personal code for direct marketing purposes

The Data Protection Law provides specific rules and exceptions regarding processing of personal data for journalistic, academic, artistic and literary purposes. When processing data for these purposes, Articles 8, 12-23, 25, 30, 33-39, 41-50 and 88-91 of the GDPR shall not be applicable.

The Data Protection Law also provides specific rules regarding processing of personal data in the employment context:

- It is forbidden to process the personal data of candidates and employees related to convictions and offences committed by the candidate or employee, unless such personal data are necessary to verify that a person meets the requirements of law or implementing legislation for the purpose of performing work or other duties.
- The data controller may collect personal data relating to qualifications, professional skills and business characteristics of a candidate applying for job from a former employer by duly informing the candidate, and from the existing employer by receiving consent of the candidate.
- The processing of video or audio data in the workplace and at the data controller's premises or in the areas where employees work, in the processing of personal data relating to the monitoring of employees' behavior, employees must be informed of such processing of their personal data in writing or by any other means which allow to prove the fact that the information referred to in Article 13(1) and (2) of Regulation (EU) 2016/679 has been provided.

The consent of a child for the use of information society services is deemed lawful where the child is at least 14 years old. Where the child is below the age of 14 years, such consent will be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility for the child.

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 (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay.

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 among others binding corporate rules, standard contractual clauses. 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 Data Protection Law provides that the State Data Protection Inspectorate must issue an authorization for the transfer of personal data to a third country or an international organization under Art. 46(3) of the GDPR or a substantiated written refusal to issue such an authorization within a maximum of 20 working days.

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
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding security.

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 Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding breach notification duties.

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 scrutinized 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).

The Data Protection Law sets out administrative fines which can be imposed on public institutions. The State Data Protection Inspectorate has the right to impose an administrative fine:

- Up to 0.5% of the annual budget of the institution in the current year or of the total annual revenue received in the previous year but not exceeding EUR 30000 for breach of the provisions referred to in the paragraphs a-c of Article 83(4) of the GDPR
- Up to 1% of the annual budget of the institution in the current year or of the total annual revenue received in the previous year, but not exceeding EUR 60000, for breach of the provisions referred to in the paragraphs a-e of Article 83(5) and Article 83(6) of the GDPR
- When a public authority or body carries on commercial business, according to sections 4-6 of Article 83 of the GDPR

The statute of limitation is two years from when the offence has been committed, and in case of continued offences, within two years after the offence has been identified.

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 to individuals in Lithuania must only be conducted in accordance with the Data Protection Law, the Electronic Communications Law and the Law on Advertising of the Republic of Lithuania (Advertising Law).

General requirements for direct marketing:

- The recipient (either natural person or legal person) has given his prior consent (under Lithuanian law, an opt-in principle applies, ie, the customer should actively express his willingness to receive commercial communication)
- The recipient’s consent must be obtained separately from other terms of the contract between the parties
- Consent cannot be obtained in the standard terms presented to the recipient (eg, “by accepting these terms you agree to receive our commercial communication to the email provided to us”). The consent must stand separately from other contractual terms, so that the data subject has an actual possibility to choose whether he or she wants to receive commercial communication from the company or not
- The company must ensure that recipients have been given a clear, free-of-charge and easily realizable possibility not to give their consent or refuse giving their consent for the use of this data for the above-mentioned purposes at the time of collection of the data and, if initially the recipient has not objected against such use of the data, at the time of each offer

No direct marketing should be carried out where the contact has requested not to receive unsolicited direct marketing.

Exemption: if the company has obtained electronic contact details in the process of selling a product or a service, it is allowed to use these details for direct marketing provided that the recipient (either natural person or legal person) is given an opportunity to refuse such marketing; this opportunity shall continue to be offered with each message.

Additional requirements under the Advertising Law:

- Direct marketing must be clearly recognizable as a commercial communication
- The person on behalf of whom this commercial communication is distributed must be clearly identified
- The content of the offer and conditions regarding receiving of the service must be formulated clearly and precisely

Each marketing communication is a separate violation, for which a penalty of up to EUR 3,000 may be imposed.

As mentioned above, the Data Protection Law provides a definition of direct marketing and prohibits the processing of personal code for direct marketing purposes.

ONLINE PRIVACY

Traffic Data

Traffic Data held by a public electronic communications services provider must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service
- consent has been given for the retention of the Traffic Data
- It is required for investigation of a grave crime

Traffic Data can only be processed by a CSP for:

- The management of business needs, such as billing or traffic
- Dealing with customer enquiries
- The prevention of fraud
- The provision of a value added service

Cookies

The use of cookies is permitted only if approved by the user (under Lithuanian law, an opt-in principle applies). However, consent is not required for cookies used for website technical structure and for cookies used for showing website content. Consent is not required for session ID cookies and for so called 'shopping basket' cookies (these exceptions do not apply if such cookies are used for collecting statistical information on use of the website).

Clear and exhaustive information on use of cookies, including information about the purpose of cookie related data processing, must be provided. This information should be provided in the privacy policy of the website. Consent to the terms of the website’s privacy policy or terms of use containing the information on use of cookies is considered insufficient. Consent though web browser settings may be considered adequate only if the browser settings allow choosing what cookies may be used and for what purposes. However, considering the nature of currently used web browsers consent through web browser settings is not considered appropriate under Lithuanian law.

Location data

Processing of location data triggers personal data processing laws. The data controller must have a legitimate basis for such personal data processing (*eg*, the data subject has given his consent; a contract to which the data subject is party is being concluded or performed; it is a legal obligation of the data controller under laws to process personal data; processing is necessary in order to protect vital interests of the data subject; etc.).

The Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding online privacy.

KEY CONTACTS

Sorainen
www.sorainen.com/

Stasys Drazdauskas
Counsel
Sorainen
T +370 52 685 040
stasys.drazdauskas@sorainen.com

Irma Kirklytė
Counsel
Sorainen
T +370 52 685 040
irma.kirklyte@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.