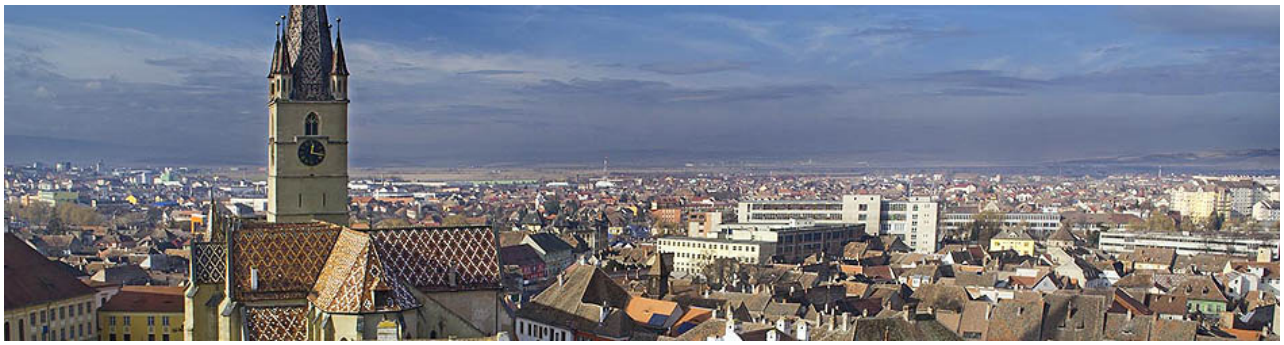
DATA PROTECTION LAWS OF THE WORLD

Romania

ROMANIA



Last modified 17 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 extraterritorial 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" (no payment is required) to such data subjects in the EU or "the monitoring of their behaviour" as far as their behaviour takes place within the EU.

Law no. 190/2018 on the measures for the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("Law no. 190/2018") was published in the Official Gazette no. 651/26.07.2018 and became applicable on July 31, 2018.

Law no. 190/2018 regulates, among others, the following activities, in addition to providing certain derogations and a framework related to the sanctions applicable to public authorities and public bodies:

- Processing of genetic data, biometric data or health data
- Processing of a national identification number
- Processing of personal data in the context of employment relationships
- Processing of personal data and of special categories of personal data within the performance of a task carried out in the public interest

DEFINITIONS

Personal data is defined as "any information relating to an identified or identifiable natural person." A low bar is set for identifiable – if the natural person can be identified using “all means reasonably likely to be used” 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** 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.**

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." 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.

Law no. 190/2018 does not provide any specific definitions with respect to personal data, as this term is already defined by the GDPR. However, the following relevant definitions are included:

- "Public authorities and bodies" means the Chamber of Deputies and the Senate, the Presidential Administration, the Government, the ministries, other specialized bodies of the central public administration, autonomous public authorities and institutions, local and county public administration authorities, other public authorities, as well as any institutions subordinated / coordinated by such authorities. Religious establishments, organisations and foundations of public service are considered public authorities / bodies.
- "National identification number" means the number by which an individual is identified in certain record systems and which has general applicability, such as: (i) personal identification number, (ii) serial number and identity card number, (iii) passport number, (iv) driving license, and (v) social health insurance number.
- "Remediation plan" means an annex to the report for finding and sanctioning misdemeanours, drafted by the National Supervisory Authority for Personal Data Processing (hereinafter referred to as ANSPDCP) setting remediation measures and terms.
- "Remediation measure" means a solution imposed by ANSPDCP in the remediation plan, in view of ensuring the compliance of the public authority/body with the obligations provided by the law.
- "Remediation term" means a time period of maximum 90 days calculated from the moment when the report for finding and sanctioning misdemeanours is communicated, in which the public authority/body may undertake remedial actions in order to correct any irregularities assessed by ANSPDCP and comply with its legal obligations.

All definitions included by the GDPR in Article 4 are applicable and have the same meaning as in Law no. 190/2018.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (similar to 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 GDPR.

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."

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. ead supervisory authority is therefore of somewhat limited use to multinationals.

The National Supervisory Authority For Personal Data Processing
(in Romanian 'Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal' or 'ANSPDCP')
28 30 Magheru Blvd
District 1, Bucharest
T +40 318 059 211
F +40 318 059 602
www.dataprotection.ro

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 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.

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, 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.

All obligations in respect of notifying ANSPDCP of the processing of personal data were repealed on May 25, 2018 (when GDPR came into force).

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer (DPO) 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, 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* of data protection law and practices, though it is possible to outsource the DPO role to a service provider.

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," 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.

The specific tasks of the DPO, set out in GDPR, include:

- 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.

In addition to the requirements provided by the GDPR in Articles 37 to 39, Law no. 190/2018 provides that a data protection officer (DPO) must be designated whenever the entity acting as controller is processing a national identification number, including by collecting or disclosing any documents enclosing such national identification number, when the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, in accordance with the provisions of Article 6 paragraph 1 letter (f) of the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

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

- 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")
- 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 for potentially years after a particular decision relating to processing personal data was rendered. Record-keeping, auditing and appropriate governance will all play 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 recognised 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, except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- 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.

Processing for a Secondary Purpose

Increasingly, organisations 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. 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, that is, 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.

The following information must be provided 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 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

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

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

Right to erasure ('right to be forgotten')

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

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

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

Right to object

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

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

- Necessary for entering into or performing a contract
- Authorized by EU or Member State law
- The data subject has given their explicit (*ie*, opt-in) consent

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

1. Processing genetic data, biometric data or health data

The processing of genetic, biometric or health data for the purpose of achieving an automated decision-making process or for profiling purposes is permitted only with the explicit consent of the data subject or if the processing is performed based on express legal requirements, with the obligation to implement adequate measures for the protection of the rights, freedoms and legitimate interests of the data subject. Law no. 190/2018 does not specify or provide any examples with respect to what type of measures should be implemented in view of the processing.

Law no. 190/2018 expressly allows the processing of health data for the purpose of public health, as defined under Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work. However, subsequent processing of such data may not be performed for other purposes by third parties.

2. Processing a national identification number

Law no. 190/2018 provides that processing a national identification number, including by collecting or disclosing any

documents enclosing such national identification number, may be carried out in the situations provided for in Article 6 (1) of the GDPR. However, where processing is based on the legitimate interests pursued by the controller or by a third party (i.e. Article 6 (1) (f) of the GDPR), the processing activities may be carried out only if the following guarantees have been implemented by the controller:

- Adequate technical and organizational measures to observe, in particular, the principle of data minimization and to ensure the security and confidentiality of personal data processing, according to the provisions of art. 32 of the GDPR;
- The appointment of a DPO;
- Establishment of retention terms in accordance with the nature of the personal data and the purpose of the processing, as well as specific deadlines in which personal data must be deleted or revised in order to be deleted;
- Regular training of the personnel processing personal data under the direct authority of the controller or processor.

3. Processing personal data in the context of employment relationships

The electronic monitoring and / or video surveillance systems of employees at the workplace based on the legitimate interests of the employer is / are permitted only if the following apply:

- The legitimate interests pursued by the employer are thoroughly justified and prevail over the interests or rights and freedoms of the data subjects;
- The employer has made the compulsory, complete and explicit prior information to the employees;
- The employer consulted the relevant trade union or, where applicable, the employees' representatives prior to the introduction of the monitoring systems;
- Other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proved their effectiveness;
- The retention duration of personal data is proportional to the purpose of processing, but not more than 30 days, except for situations expressly governed by law or in duly justified cases.

4. Processing of personal data for journalistic purposes or for the purpose of academic, artistic or literary expression

According to Law no. 190/2018, in view of ensuring a balance between the right to personal data protection, freedom of expression and the right to information, processing of personal data for journalistic purposes, or for the purposes of academic, artistic or literary expression may be performed if such processing refers to personal data which were manifestly made public by the data subject or which are strongly connected to the quality of public person of the data subject or to the public nature of the facts in which the data subject is involved, by derogation from the following chapters of the GDPR:

1. Chapter II – Principles
2. Chapter III – Rights of the data subject
3. Chapter IV – Controller and processor
4. Chapter V – Transfers of personal data to third countries or international organizations
5. Chapter VI – Independent supervisory authorities
6. Chapter VII – Cooperation and consistency
7. Chapter IX – Provisions relating to specific processing situations

5. Processing of personal data for scientific or historical research purposes, statistical purposes or archiving in the public interest purposes

According to Law no. 190/2018 Articles 15, 16, 18 and 21 of the GDPR do not apply in case personal data are processed for scientific or historical research purposes or statistical purposes, to the extent the rights mentioned in these Articles

are likely to render impossible or seriously impair the achievement of the objectives of the processing, and such derogations are necessary for achieving such objectives. These derogations are applied only with respect to archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and not with respect to other purposes for which the personal data may be used. Articles 15, 16, 18, 19, 20 and 21 GDPR do not apply in cases where personal data is processed for archiving purposes in the public interest to the extent that the rights mentioned in those Articles are likely to render impossible or seriously impair the achievement of the objectives of the processing, and such derogations are necessary for achieving such objectives. These derogations are applicable only with respect to scientific or historical research purposes and for archiving in the public interest purposes, and not with respect to other purposes for which the personal data may be used. Both these derogations are applicable only if appropriate safeguards for the rights and freedoms of data subjects are implemented, in accordance with Article 89(1) GDPR.

6. Processing of personal data and special categories of personal data by political parties, national minorities organisations and non-governmental organisations for the purpose of fulfilling their objectives

Processing of personal data and special categories of personal data by political parties, national minorities organisations and non-governmental organisations for the purpose of fulfilling their objectives can be done without the explicit consent of the personal data but with the application of the following:

- The information of data subjects on the processing of personal data;
- Guaranteeing the transparency of the information, of the communications and of the manner in which data subjects can exercise their rights;
- Guaranteeing the right to rectification and the right to erasure.

TRANSFER

Transfers of personal data by a controller or a processor to countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted when certain conditions are met.

The European Commission has the power to make an adequacy decision in respect of non-EU countries, determining that it provides for an adequate level of data protection, and thereby permitting personal data to be freely transferred to that country. 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, among other things, 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 any of the following apply:

- Explicit informed consent has been obtained
- The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
- 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
- The transfer is necessary for important reasons of public interest
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
- 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 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.

No specific provisions / derogations are provided by Law no. 190/2018 with respect to personal data transfers.

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

SECURITY

The GDPR does not prescribe 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 organisational 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:

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

No specific provisions / derogations are provided by Law no. 190/2018 with respect to the security measures to be undertaken by controllers / processors.

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."

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.

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.

The notification to the supervisory authority must include where possible:

- The categories and approximate numbers of individuals and records concerned
- The name of the organisation’s data protection officer or other contact
- The likely consequences of the breach and the measures taken to mitigate harm

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

No specific provisions / derogations are provided by the Law no. 190/2018 with respect to the notification of a personal data security breach. However, where data controllers notify a personal data breach to ANSPDCP, a special notification form must be filled out and submitted.

ENFORCEMENT

Fines

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

The European Commission intends 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 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 subsidiaries in some circumstances (broadly where there is participation or control), under a theory 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 of up to €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 any of the following:

- 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
- Certain orders of a supervisory authority

The lower category of fines of up to €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 any of the following:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- 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.

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers 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 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.

Individuals also enjoy the right to lodge a complaint with a supervisory authority.

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.

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

ANSPDCP is entitled to investigate any breach of the GDPR provisions *ex officio* or following a complaint filed by a prejudiced data subject. The procedure on how ANSPDCP investigations can be conducted is provided by ANSPDCP Decision no. 161/2018.

Law no. 190/2018 provides specific rules with respect to enforcement. Specifically, ANSPDCP may issue written warnings and apply fines.

Misdemeanours committed by public authorities / bodies can be sanctioned with a fine ranging between RON 10,000 (approx. EUR 2,100) to RON 200,000 (approx. EUR 42,000).

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.

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 by 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 processing of personal data for electronic marketing purposes is regulated under Law no. 506/2004, on the processing of personal data in the electronic communications sector implementing Directive 2002/58/CE ("Law no. 506/2004").

According to this law, it is forbidden to send commercial communications by using automatic call and communication systems that do not require the intervention of a human operator, by fax or by electronic mail or any other method employing publicly available electronic communications services, except where the subscriber or user of a publicly electronic communications service has expressly consented in advance to receive such communications.

However, in cases where a natural or legal person has directly obtained the email address of a client upon the sale or provision of a product or service, the natural or legal person may use the respective address for the purpose of sending commercial communications regarding similar products or services, provided that clients are clearly and expressly offered the possibility to oppose by way of an easily accessible and free-of-charge method, not only when the email address is collected but also with each commercial communication received, in a case where the customer has not initially objected.

ONLINE PRIVACY

The processing of traffic data, location data and the implementation of cookies is regulated under Law no. 506/2004.

Traffic data

Traffic data relating to subscribers and users processed and stored by the provider of a public electronic communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication, but no later than three years from the date of such a communication.

However, traffic data may be retained for the purpose of marketing the services offered to data subjects, or in view of the provision of value-added services, solely throughout the marketing period and provided that data subjects have previously consented to the processing of traffic data. Data subjects may withdraw such consent at any time. The provider of publicly available electronic communication services must inform data subjects in respect of the processed categories of traffic data, and the duration of processing, prior to obtaining their consent.

The processing of traffic data for billing purposes or the establishment of payment obligations for interconnection is permitted solely for a period of three years following the due date of the respective payment obligation. The provider of publicly available electronic communication services must inform data subjects in respect of the processed categories of traffic data and the duration of processing.

The processing of traffic data for the establishment of contractual obligations of the communication services subscribers, with payment in advance, is permitted solely for a period of three years following the date of the communication.

The processing of traffic data as mentioned above may be done only by persons acting under the authority of providers of public electronic communications networks or of publicly available electronic communications services for:

- Management of billing and traffic
- Dealing with enquiries of data subjects
- Prevention of fraud, or
- The provision of communication services or value added services,

and it is permitted only if it is necessary to fulfil such purpose.

Location data, other than traffic data

The processing of location data, other than traffic data is permitted when:

- Data is rendered anonymous

- Data subjects have explicitly and consented prior to such processing for the duration necessary for the performance of value added services, or
- The purpose of the value-added service is the unidirectional and nondifferentiated transmission of information towards users.

The provider of publicly available electronic communications services must inform the users or subscribers, prior to obtaining their consent, in respect of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent at any time. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the provider of publicly available electronic communications services must grant users the possibility, using a simple and free of charge means, of withdrawing consent or of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Cookies

The storing of cookies on user terminals is permitted, subject to the following cumulative conditions:

- Subscribers or users have expressly consented thereto (Law no. 506/2004 also provides that consent may be given by way of browser settings or other similar technologies)
- The information requirements provided by Data Protection Law have been complied with in a clear and user-friendly manner, to include references regarding the purpose of processing of the information stored by users.

Should the service provider allow the storing of third-party cookies within a user's computer terminal, the user will have to be informed about the purpose of such processing and the manner in which browser settings may be adjusted in order to refuse third-party cookies.

Consent is not required where cookies are:

- Used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- Strictly necessary for the provision of an information service expressly requested by the subscriber or the user.

Failure to comply with the requirements of Law no. 506/2004 is classified as a minor offence and is sanctionable with fines ranging from approx. EUR 1,000 to EUR 21,000 . In the case of companies whose turnover exceeds approximately EUR 1.05 million, the amount of fines may reach up to 2% of the respective company's turnover.

Upon request of the courts of law, of the criminal prosecution authorities or of the authorities competent in the area of national defence and security with the prior approval of the judge, providers of publicly available electronic communication services and providers of public electronic communications networks shall make available, as soon as possible, but no later than 48 hours, traffic data, data regarding user terminals, as well as geolocation data.

KEY CONTACTS

Corina Badiceanu
Managing Associate
T +40 372 155 853
corina.badiceanu@dlapiper.com

Andrei Stoica
Junior Associate
T +40 372 155 870
andrei.stoica@dlapiper.com

Irina Macovei
Counsel
T +40 732 222 109
irina.macovei@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.