DATA PROTECTION LAWS OF THE WORLD

Bulgaria

DLA PIPER

BULGARIA

Last modified 21 December 2023

LAW

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

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

Territorial Scope

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

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

Bulgaria implemented the EU Data Protection Directive 95/46/EC with the Personal Data Protection Act (In Bulgarian: *Закон за защита на личните данн и*), promulgated in the State Gazette No. 1 of January 4, 2002, as amended periodically (Act). The Act came into force on January 1, 2002.

In view of the entry into force of Regulation (EU) 2016/679 (General Data Protection Regulation – 'GDPR'), the Personal Data Protection Act was amended by a law for amendment and supplementation which was promulgated in the State Gazette No. 17 of February 26,2019.

The Personal Data Protection Act as amended (hereinafter referred to as the 'Personal Data Protection Act) serves a twofold purpose – it effectively implements the GDPR into national legislation and also transposes Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The Personal Data Protection Act complements the GDPR by providing regulation to matters in the field of personal data processing that have not been explicitly covered by the GDPR, or where the GDPR has left room for the exercise of legislative discretion. As the regulation has direct effect and is applicable in all EU member-states without the need of adopting a designated legislative act, the Bulgarian legislator has adopted the approach of directly referring to and implementing the GDPR without repeating the core provisions of the regulation in the Personal Data Protection Act.

Under the Personal Data Protection Act the role of supervising authority is shared between the Commission for Personal Data Protection and the Inspectorate to the Supreme Judicial Council, the latter having competence only with regards to data processing by courts, prosecution offices and criminal investigative bodies in their capacity as judicial authorities. The Personal Data Protection Act further regulates the legal remedies in cases of violation of personal data law, the accreditation and certification in the field of personal data protection, the administrative liability and the administrative measures in cases of violations of its provisions.

Pursuant to an amendment in the Personal Data Protection Act which came into force in May 2023, the Commission for Personal Data Protection was also designated as the competent controlling body under the Bulgarian Whistleblower Protection Act.

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.

Definition of personal data

The definition of personal data set forth before by the Personal Data Protection Act was repealed following the implementation of the GDPR and it explicitly refers to the definition of personal data under art. 4 of the GDPR (§1 of the Supplementary provisions of the Personal Data Protection Act).

Personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of sensitive personal data

The Personal Data Protection Act refers explicitly to the definition under the GDPR which applies following its direct effect in all EU member states.

NATIONAL DATA PROTECTION AUTHORITY

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

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

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

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

The Bulgarian data protection authority (DPA) is the Personal Data Protection Commission (In Bulgarian: *К омисия за защит а на личните дан ни*, the 'Commission').

2 Professor Tsvetan Lazarov, Sofia 1592
Bulgaria

kzld@cpdp.bg
www.cpdp.bg

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 organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The requirement for registration of data controllers before the Commission for Personal Data Protection was repealed with the implementation of the GDPR.

Pursuant to the Personal Data Protection Act, the Commission for Personal Data Protection maintains the following public registers:

- register of data controller and data processors who have appointed data protection officers containing the name of the data controller / data processor, the name of the appointed data protection officer and its contact details;
- register of the accredited certifying bodies under art. 14 containing information on the name and the contact details of the certifying body and on the period of validity of its accreditation;
- register of codes of conduct which includes the name of the code, the name of the editor and the relevant certification body, information about the sector concerned and its content.

The Commission shall also support (a) an internal register of established breaches of the GDPR and the Personal Data Protection Act, (b) a register of the measures taken in accordance with art. 58, para 2 of the GDPR, and (c) a register of the personal data destroyed on a monthly basis by providers of public electronic communication networks and / or services in accordance with art. 251g of the Electronic Communications Act. These registers, however, are not public.

In accordance with the Rules of Procedure of the Commission for Personal Data Protection and its Administration, the above-mentioned registers are held in electronic format and should be updated regularly.

DATA PROTECTION OFFICERS

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

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

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

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

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

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

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

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

The Personal Data Protection Act does not set an explicit requirement to appoint a data protection officer ("**DPO**"), thus the general requirement pursuant to the GDPR applies. Pursuant to the Personal Data Protection Act, data controllers are obliged to communicate the personal details and contact details of the DPO, as well as any subsequent replacements, before the Commission for Personal Data Protection, and will also have to publish their contact details. An approved notification form, which was recently updated by the Commission for Personal Data Protection, is available online (only in Bulgarian language).

COLLECTION & PROCESSING

Data Protection Principles

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

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

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

Legal Basis under Article 6

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

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

Special Category Data

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

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

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

Criminal Convictions and Offences data

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

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

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

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

Transparency (Privacy Notices)

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

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

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

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

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

Rights of the Data Subject

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

Right of access (Article 15)

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

Right to rectify (Article 16)

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

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

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

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

Right to restriction of processing (Article 18)

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

Right to data portability (Article 20)

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

Right to object (Article 21)

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

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

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

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

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

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

The Personal Data Protection Act does not repeat the core provisions of the GDPR relating to collection and processing of personal data in its body. However, following the direct effect of the GDPR in all EU member states, the provisions of the regulation in this respect shall be applied in all cases of data collection and processing. The Personal Data Protection Act explicitly previews that in case the data subject provides his / her personal data to a data controller or a data processor in breach of Art. 6, para (1) (legal grounds for processing) and Art. 5 (principles for data processing) GDPR, the data controller / data processor should have to immediately return the data or delete / destroy the data within one month of becoming aware of the breach (art. 25a of the Personal Data Protection Act).

The Personal Data Protection Act also introduces additional rules relating to specific data processing situations:

- Conditions applicable to child's consent in relation to information society services – The Personal Data Protection Act introduces a lower age of the data subject, under which the consent of a parent or a guardian would be required for the lawful processing of personal data of a child in cases of direct provision of information society services. Under the Personal Data Protection Act if the data subject is under 14 years old, a consent by a parent exercising the parental rights or by guardian of the data subject is required for the lawful processing of the data.
- Processing of personal identification number – Under the Personal Data Protection Act, public access to personal identification number / personal identification number of a foreigner ('PIN/PINF') shall be granted only if required by law. Data controllers providing electronic services should undertake appropriate technical and organizational measures to prevent the PIN/PINF from being the sole identifier for the use of their services.
- Processing and freedom of expression and information — Where personal data is processed for the exercise of freedom of expression and information, including for journalistic purposes and for the purposes of

academic, artistic or literary expression, the data controller should assess the lawfulness of such processing in each particular case. The Personal Data Protection Act sets a number of assessment criteria to be used by data controllers / processors in the assessment of the lawfulness of processing such as the type of the personal data processed, the impact of the public disclosure on the privacy of the data subject and his / her reputation etc. However, the Bulgarian Constitutional Court (Decision Nr.8 dated November 15,2019) declared the assessment criteria set forth by the Personal Data Protection Act to be unconstitutional. More particularly, the criteria were found to be unclear and therefore creating unpredictability and legal uncertainty and restricting disproportionally the freedom of expression and information. Based on this decision, the above-mentioned criteria do no longer apply. The balancing test between the freedom of expression and the right to information and the protection of personal data shall me made on a case-by-case basis taking into consideration the specific circumstances and interests in presence. Further guidance in this respect was provided in a recent decision of the Supreme Administrative Court (Decision Nr. 11636 dated November 16, 2021), which clarified how the balance between these competing rights shall be assessed in each individual case.

- Processing in the context of employment – The Personal Data Protection Act regulates explicitly certain matters related to personal data processing in the context of an employment relationship. Employers may take copy of employee's identification documents, driving license or residence document only if required by law. In addition, according to a statement by the Commission for Personal Data Protection information for the criminal background of the employees can also be processed by employers only if explicitly provided for by law. Other legal grounds, such as consent or the legitimate interest cannot be applied for the processing of criminal records information. Most recently, the Commission for Personal Data Protection has adopted several opinions concerning the processing of employee health data by employers in the context of Covid-19; in particular, the latter provide that employers:
    - cannot request information from a remote-working employee whether he / she (or any of his / her family members) has tested positive for Covid-19; such information can only be disclosed voluntarily by the employee;
    - may provide anonymized information to their employees about established Covid-19 cases in the company (i.e. without revealing the identity of the infected employee(s));
    - can order / organize Covid-19 group testing of employees, without processing or having access to the test results - since the latter contain sensitive health data, they can only be processed by competent health authorities;
    - may process only aggregated data for the vaccination status of the employees, gathered voluntary and on anonymous basis by the appointed Labour Medicine Office (a third party service provider in the field of occupational medicine, that each employer shall appoint) for the purposes of risk assessment of the health and safety conditions at the workplace.

Employers should adopt rules and procedures for:

- the use of breach reporting system;
- restrictions on the use of internal company resources;
- introduction of systems for control access, working time and labor discipline.

These rules and procedures shall contain information on the scope, obligations and methods with respect to their application. The Personal Data Protection Act recognizes that the business purpose of the employer and the nature of the related work processes shall have to be taken into account upon the adoption of the rules and procedures. The rules and procedures will have to be brought to the attention of the employees.

Employers shall have to further determine a retention period for the personal data collected during the recruitment process, which however may not be longer than six months, unless the candidate consented to a longer period. Where the employer has, for recruitment purposes, requested original or notarized copies of documents certifying the physical and mental fitness of the applicant, the required degree, or the length of service for the previous positions occupied, the employer should return the submitted documents within six months of the conclusion of the recruitment procedure unless otherwise provided by specific law.

- Personal data processing by way of large-scale surveillance of publicly accessible areas – Under the Personal Data Protection Act data controllers and data processors shall adopt internal rules for the processing of personal data through systematic large-scale surveillance of publicly accessible areas, including via video surveillance. These rules should put in place appropriate technical and organizational measures to ensure the protection of data subjects' rights and freedoms. The Personal Data Protection Act provides a definition for 'large-scale' — a systematic monitoring and / or processing of personal data of an unlimited number of data subjects. The rules for personal data processing through large-scale surveillance of publicly accessible areas shall define the legal grounds and objectives for the introduction of a monitoring system, the location, scope and means of monitoring / surveillance, retention periods for the information records and their deletion, the right of review by the persons being subject to surveillance, the means of informing the public about the monitoring carried out, as well as the restrictions on granting access to such information to third parties. The minimum requirements for data controllers / data processors with respect to the aforementioned obligations shall be published on the website of the Commission for Personal Data Protection.

Processing of personal data of deceased persons

The Personal Data Protection Act stipulates, that when processing the personal data of deceased persons data controllers shall have to take appropriate measures to prevent the rights and freedoms of others and the public interest from being adversely affected. In such cases, the data controller may retain the data only if there is a legal basis therefor. In addition, data controllers shall provide upon request access to the personal data of a deceased person, including a copy thereof, to his / her heirs or other persons with legal interest.

The controller shall provide information on action taken without delay and in any event within one month as of the receipt of the request. That period may be extended with two further months where necessary. In case there is a delay, the controller shall provide the reasons for the delay.

Where the request has been made by electronic form, the information shall be provided by electronic means, where possible, unless otherwise requested by the data subject.

If the controller does not act on the request, the controller shall inform without delay and at the latest within one month of receipt of the request of the reasons for not taking action and the possibility of lodging a complaint with a supervisory authority and seeking judicial remedy.

TRANSFER

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

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Korea, the United Kingdom, Eastern Republic of Uruguay and New Zealand. Following the invalidation of the EU – US Privacy Shield by the European Court of Justice, on December 13th, 2022 the European Commission initiated the process to adopt a new adequacy decision for the USA. The draft decision will undergo an EU approval process, including obtaining an opinion from the European Data Protection Board and European Parliament. The European Commission will also need to seek approval of the new adequacy framework from a committee composed of representatives of EU Member States.

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 appropriate safeguards include among others binding corporate rules and standard contractual clauses. On 4 June 2021 the

European Commission adopted new set of standard contractual clauses for transfers outside the EU/EEA. Data controllers and processors have term until 27 December 2022 to renegotiate their existing data processing agreements based on the old set of standard contractual clauses in order to reflect the new clauses adopted by the European Commission.

The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

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

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

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

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

The Personal Data Protection Act does not derogate from the provisions of the GDPR regarding data transfer and does not introduce any additional rules or requirements in this respect. Following the direct effect of the GDPR in all EU member states, the provisions of the regulation relating to this matter shall be applied in all cases of data transfer.

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 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:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

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

The Personal Data Protection Act does not derogate from the provisions of the GDPR regarding security of personal data and does not introduce any additional rules or requirements in this respect.

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 organisation’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 Personal Data Protection Act does not derogate from the provisions of the GDPR regarding data breach notification and does not introduce any additional rules or requirements in this respect. Following the direct effect of the GDPR in all EU member states, the provisions of the regulation relating to this matter shall be observed. The Commission for Personal Data Protection adopted an internal framework of instructions for evaluation and assessment of submitted data breaches reports, including a methodology for risk assessment in case of established data breaches. The authority further approved a template of data breach notification, which controllers may use. The template is available online in Bulgarian language only.

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 functions of supervision and control of the compliance with the GDPR in Bulgaria are shared between the Commission for Personal Data Protection and the Inspectorate to the Supreme Judicial Council, the latter having competence only with regards to data processing by courts, prosecution offices and criminal investigative bodies in their capacity as judicial authorities.

The competences of the Commission are further defined by reference to art. 57 and 58 of the GDPR. Apart from performing the powers under the GDPR, the Commission is also entitled to:

- analyze and carry out overall supervision and ensure compliance with the GDPR, the Personal Data Protection Act and the legislative acts in the area of personal data protection;
- issue secondary legislation in the area of personal data protection;
- ensure the implementation of the decisions of the European Commission on the protection of personal data and the implementation of binding decisions of the European Data Protection Supervisor;
- participate in international cooperation between data protection authorities and international organizations on personal data protection issues;
- participate in the negotiation and conclusion of bilateral or multilateral agreements on matters within its competence;
- organize, coordinate and conduct training in the field of personal data protection;
- issue administrative acts related to its authority in the cases provided for by law;
- adopt criteria for the accreditation of certification bodies;
- bring proceedings before the court for breach of the GDPR;
- issue mandatory instructions, give instructions and recommendations regarding the protection of personal data;
- impose coercive administrative measures.

The internal Rules of Procedure of the Commission further clarify its tasks, procedures and rules for work of its administration, as well as rules for the proceedings before the Commission.

The Personal Data Protection Act does not derogate from the provisions of the GDPR regarding administrative sanctions, but directly refers to the amounts of fines and pecuniary sanctions set out by the GDPR and the respective criteria for their determination. The Personal Data Protection Act specifies that all sanctions shall be imposed in the BGN equivalent of the EUR amounts set by the GDPR.

For other violations under the Personal Data Protection Act the data controller / data processor shall be subject to a fine or a pecuniary sanction of up to BGN 5000.

A complaint against a decision of the Commission may be withdrawn until the expiry of the period for appealing the said decision. Otherwise, the Commission's decisions are subject to appeal before the Administrative Court Sofia within 14 days of receipt. Decisions of the Administrative Court are subject to appeal before the Supreme Administrative Court which decisions are final.

In case of a violation of his / her rights under the GDPR and the Personal Data Protection Act, every data subject is entitled to refer the matter to the Commission for Personal Data Protection within six months of becoming aware of the breach, but no later than two years from the date of the violation. In addition, data subjects shall be entitled to appeal the actions and acts of the data controller / data processor directly before the administrative courts or the Supreme Administrative Court, except where there are pending proceedings before the Commission for the same matter if a decision regarding the same breach has been appealed and there is not yet a court decision in force. The transfer or distribution of computer or system passwords which results in the illegitimate disclosure of personal data constitutes a crime under the Bulgarian Criminal Code (promulgated in the State Gazette No. 26 of April 2, 1968, as amended periodically) and the penalty for such a crime includes imprisonment for up to three years.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

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

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

The Personal Data Protection Act does not introduce any rules relating specifically to e-marketing. As the legal grounds for processing of personal data under the GDPR are also applicable in the area of e-marketing, the explicit consent of the data subject is likely to be the most suitable ground for the purposes of e-marketing. In certain cases, such processing may also be justified by legitimate interest — according to Recital 47 of the GDPR, direct marketing could be based on legitimate interest, to the extent that: (i) it is targeted only to existing customers; and (ii) the customers can reasonably expect to receive direct e-marketing communications. Still, the possibility to rely on legitimate interest for the purposes of e-marketing would need to be assessed on a case-by-case basis.

In addition, although the repeal of the provision of the Personal Data Protection Act regulating the right of the data subject to object to any data processing for the purposes of direct marketing and does not explicitly refer to the respective provision of the GDPR, following the direct effect of the regulation, data subjects shall still be entitled to object before the data controller or the data processor to their personal data being processed for the purposes of e-marketing.

The Bulgarian Electronic Communications Act explicitly requires, when it comes to direct marketing to natural persons, the opt-in mechanic to be mandatorily applied. After the natural person's consent is provided, the person shall always be given the opportunity to opt out from the direct marketing network and refuse his / her personal data to be further processed for such purposes.

ONLINE PRIVACY

Directive 2002/58 (E-Privacy Directive) is transposed into the Bulgarian Electronic Commerce Act. In 2011 the intention of the legislator was to introduce the amendments of Art. 5(3) under Directive 2009/136. However, the final adopted text still replicates the old wording before Directive 2009/136. The amendment itself was widely interpreted as implementing the text of Directive 2009/136 without, however, introducing the updated text.

Currently, instead of requiring the user's consent, the relevant text in the Electronic Commerce Act states that users should be provided with clear and comprehensive information in accordance with Art.13 of the GDPR and they must be given the opportunity to refuse the storage or access to such information (i.e. opt-out regime).

KEY CONTACTS

Wolf Theiss

www.wolftheiss.com/

Anna Rizova
Partner
Wolf Theiss
T +359 2 8613703
anna.rizova@wolftheiss.com

DATA PRIVACY TOOL

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