CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

CEE
LEGAL MATTERS

www.ceelegalmatters.com

TABLE OF CONTENTS

CHAPTER CONTENTS

KINSTELLAR

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

BULGARIA

Milka Nikolova,
Of Counsel, Head of Telecommunications in Sofia
milka.nikolova@kinstellar.com
+359 876 210 097

Vilislava Kolarova,
Junior Associate
vilislava.kolarova@kinstellar.com
+359 878 763 060

CEE
LEGAL MATTERS

www.ceelegalmatters.com

What are the main data protection-related pieces of legislation and other regulations in Bulgaria?

The main act regulating the protection of personal data in Bulgaria is 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 (General Data Protection Regulation or GDPR). With effect from 25 May 2018, the GDPR takes precedence over national legislation and sets forth the main concepts and principles of data protection. It governs the rights and obligations of data controllers, data processors, and data subjects, sets out the rules for international data transfers, and regulates the competence of data protection authorities, as well as remedies, liability, and sanctions in the field of data protection.

The most important piece of national legislation complementing the GDPR is the Personal Data Protection Act (PDPA). The PDPA provides the implementing rules of the GDPR, sets forth certain derogations, and transposes Directive (EU) 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties (Law Enforcement Directive). The provisions of the PDPA are further detailed in the related secondary legislation governing the procedural rules of the data protection authority – the Regulations for the Activities of the Commission for Personal Data Protection and the Instruction for the Practical Implementation of the Supervisory Powers of the Commission for Personal Data Protection.

The PDPA does not codify all relevant data protection rules in Bulgaria. Therefore, in addition to the PDPA provisions, a number of other rules, regulated by sector-specific legislation, apply. Such rules are set out in the Electronic Communications Act and E-Commerce Act, the Act on the Protection of Persons Who Report or Publicly Disclose Information on Infringements, the Health Act, the Anti-Money Laundering Act, the Public Information Access Act, and a number of other laws. In terms of sanctions and enforcement, the Administrative Procedure Code and the Administrative Penalties and Sanctions Act are also applicable.

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, etc., or equivalent)?

Following the entry into force of the GDPR, the definitions of key data protection terms under Bulgarian law, such as personal data, data processing, data processor, data controller, and consent, have been superseded by the corresponding definitions under the GDPR. The PDPA does not define "data subject" and "special category of data," but due to the direct applicability of the GDPR in Bulgaria, the same concepts apply under the GDPR. For businesses operating in Bulgaria, this shift ensures a higher level of consistency and uniformity in data protection practices. The harmonization brought about by the GDPR means that companies can now navigate data protection obligations with greater clarity and predictability.

Which entities fall under the data privacy regulations in Bulgaria?

The key players in the field of data protection are controllers, processors, and joint controllers. Properly identifying and understanding the role of the organization as controller, processor, or joint controller is crucial to ensure compliance with data protection laws, as each role comes with distinct rights and responsibilities. Thus:

- An organization that determines the purposes and means of data processing is a controller. Controllers bear the most extensive responsibilities under the data protection law. They must adhere to all data protection principles and demonstrate compliance. Controllers are in charge of implementing data protection by design and by default obligation, appointing a data protection officer, keeping records of processing activities, and implementing appropriate technical and organizational measures to ensure data security. They are also subject to a number of other obligations, such as notifying the data protection authority and, in some cases, the data subject in the event of a personal data breach, carrying out a data protection impact assessment, and, in certain circumstances, prior consultation with the supervisory authority. In addition, data controllers are responsible for ensuring that any processors they engage comply with data protection requirements.
- An organization that processes data on behalf of a controller, without determining the processing purposes, has the role of processor. While processors have fewer responsibilities than controllers, they still have some obligations of their own. The relationship between controllers and processors is governed by a written contract, the mandatory minimum content of which is specified in the GDPR and which sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and other details. Processors carry out processing on the basis of documented instructions from the controller and are not permitted to appoint another processor without

prior specific or general written authorization from the controller.

- Apart from acting as a controller or processor, an organization may determine the purposes and means of processing together with another controller. In this case, it is considered a joint controller – a role that did not exist in Bulgarian law prior to the GDPR. Joint controllers must clearly define their respective roles and responsibilities in an arrangement that is transparent to the data subjects.

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

Although the GDPR and the PDPA set forth the overreaching principles of the data protection law, these primary pieces of statutory legislation do not codify the data protection rules in Bulgaria. Under Bulgarian data protection law, there are sectors and types of data that are subject to specialized regulations or laws tailored to address their unique characteristics, risks, or requirements. Examples of such sectors are the electronic communications sector and the processing carried out in the context of employment relations. Those rules are specific to the sector and supplement or prevail over the general rules of data protection law.

Electronic communications sector

The data protection rules applicable to the sector of electronic communications are set forth primarily in the Electronic Communications Act. Some of the sector-specific rules are those concerning traffic data retention and disclosure, data breach notification, and the exceptions concerning communications confidentiality.

In Bulgaria, electronic communications providers are subject to the obligation to retain certain traffic data for a period of six months. This data includes the information necessary to trace and identify the source and type of connection, its direction, date, time, and duration, and to identify the end user's terminal device and the identifiers of the cells used. Access and disclosure of such data are strictly limited to specific law enforcement and disaster control authorities as detailed in the law. Electronic communications providers may retain and disclose this data for the purposes of, among others, facilitating the investigation of serious crimes, national security purposes, locating people at risk or in emergency situations, and in the cases of searching for persons declared wanted by the state. At the end of the six-month period, the service providers must delete the retained traffic data. Moreover, the traffic data retention obligation gives rise to specific reporting obligations: electronic communications providers must report certain data retention and disclosure activities to the Bulgarian Commission for Personal Data Protection. This includes monthly reports on the data deleted during the preceding month and an annual statistical report on data disclosures requested by competent authorities.

In the event of a personal data breach, electronic communications providers must notify the Bulgarian Personal Data Protection Commission within 24 hours of becoming aware of the breach – a notably shorter timeframe compared to the 72 hours stipulated by the GDPR. Moreover, under certain circumstances, the affected individual must also be notified. Specific notification rules and procedures deviating from the GDPR and provided by Regulation (EU) 611/2013 apply in respect of personal data breach notifications in the sector.

To protect the confidentiality of communications and related traffic data, Bulgarian law prohibits listening to, recording, storing, or otherwise intercepting or tracking communications by parties other than the sender and recipient, unless express consent has been obtained. However, there are specific exceptions for the regulated activities of electronic communications providers. For instance, these prohibitions do not apply when storage is necessary for technical reasons or is an integral part of providing the service, and when the technical parameters of the service are verified by authorized persons. In such cases, providers must delete the stored communications data immediately after the reason for storage ceases to exist.

Processing in the context of employment relations

The PDPA establishes specific national rules for processing employee personal data, in some cases including data on criminal convictions and offenses. As data controllers, employers must adopt the following internal rules and procedures if the relevant activities are in place: (i) for use of whistleblowing systems (currently subject to additional rules under whistleblowing legislation); (ii) for restrictions in internal resource usage; and (iii) when introducing systems for access control, working time and working discipline. These rules and procedures must include detailed information about their scope of application, the obligations they impose, and the methods for practical application. They should be tailored to the specific business activities of the employer and the specific nature of the work, ensuring that they do not infringe upon employees' rights. Employees must be informed about these rules and procedures.

Pursuant to the PDPA, employers must set a storage period for personal data collected during recruitment and selection processes. This period cannot exceed six months unless the applicant consents to a longer retention period. After the expiration of the retention period, employers are required to delete or destroy the stored personal data and return any original documents provided by the data subject.

Under the data protection law, personal data relating to criminal convictions and offenses is not a special category of data, but its processing is limited to the cases where it is carried out under the control of an official authority or where the processing is authorized by the EU or Bulgarian law. In the employment context, Bulgarian law provides for such exceptions in certain cases, for example: (i) under the Private Security Activities Act with respect to employees carrying out functions as heads of private security activities and as security guards; (ii) under the Discrimination Protection Act with respect to the members of the Commission for Protection of Discrimination; (iii) under the Insurance Code with respect to members of the management and controlling bodies of insurance and re-insurance companies; (iv) under the Currency Law with respect to organizations carrying out transactions with currency in cash; (v) under the Road Transportation Act with respect to heads of the transportation activities of passenger and cargo transport services providers; (vi) under the Anti-Money Laundering Act with respect to the managing director, member of a management or supervisory body, or partner in a company carrying out intermediation activities in sales of real estate. Given the GDPR's prohibition on processing data relating to criminal convictions and offenses, the number of exemptions for processing such data in the context of employment law has increased significantly in recent years in order to facilitate employers.

What rights do data subjects have under the data protection regulations in Bulgaria?

As of 2019, the section of the PDPA governing the rights of natural persons has been repealed, and currently, the rights of data subjects are regulated by the GDPR. Therefore, data subjects in Bulgaria enjoy the same rights as other individuals protected by the EU data protection laws. These rights include:

- the right to be informed (the right to know how personal data is being used);
- the right of access (the right to access personal data held about data subject);
- the right to rectification (the right to have inaccurate data corrected);
- the right to erasure (the right to have personal data deleted);
- the right to restrict processing (the right to limit the processing of subjects' data);
- the right to data portability (the right to transfer data to another service provider);
- the right to object to data processing;
- the right not to be subject to automated decision-making, including profiling; and
- the right to judicial or administrative remedy, including to seek compensation for violations of data protection rights.

In addition to the GDPR provisions, Bulgarian law details how data subjects can make requests regarding their data. Such requests must be in writing (irrespective of in hard copy or in the form of an electronic document) unless the controller has established an alternative method. As a minimum, the request must include:

- the name, address, unique nationality number, or other identification data of the natural person;
- a description of the request;
- the preferred form for obtaining the information;
- an address for correspondence;
- the date and the data subject's signature; and
- if submitted by a proxy, relevant authorization documents must be attached.

To balance individual rights with other critical interests, Bulgarian law provides specific derogations that may limit data subject rights in certain circumstances. Organizations acting in Bulgaria must consider those derogations to better navigate the balance between data protection compliance and other essential legal and societal obligations. Among such critical interests are national security; public policy; the prevention, investigation, and prosecution of crimes and violations of codes of ethics of regulated professions important economic or financial interests, such as the state budget and fiscal matters, public health, and social security; independence of the judiciary system; and enforcement of civil claims. In cases where exercising data subject rights poses a risk to these interests, controllers, and processors may refuse to fully or partially honor data protection requests and are not required to notify the data subject of a data breach. In addition, under the PDPA, the controller or processor may refuse to honor, in whole or in part:

- all of the abovementioned data subjects' rights, except for the right not to be subject to a decision based solely on automated processing, including profiling, when processing concerns (i) personal data for journalistic purposes, for academic, artistic, or literary expression and if carried out for the exercise of freedom of expression and the right to information; or (ii) personal data for the purpose of creating a photographic or audio-visual work by filming a person in the course of their public activity or in a public place;
- the rights of access, rectification, restriction of processing, and the right to object if the processing of personal data is for the purposes of the National Archive Fund of the Republic of Bulgaria or for statistical purposes.

What is the territorial application of the data privacy regime in your jurisdiction?

The territorial application of data protection laws is governed by the GDPR rather than local Bulgarian legislation. This depends, on the one hand, on the establishment of the data controller or data processor and, on the other hand, on the nature of the processing activities. The GDPR applies regardless of whether the processing occurs within or outside the EU, under the following circumstances:

- The processor or controller is established in an EU Member State.
- The processor or controller is established in a non-EU Member State, but where the EU Member State law applies by virtue of public international law (such as in Bulgarian diplomatic and consular missions abroad).

The location of the establishment is crucial, as it typically determines where the controller or processor conducts its business and the local laws that must be observed. However, the GDPR also extends its reach to data controllers and processors that are not established in the EU, but that process the personal data of EU citizens. This is applicable when the processing activities are related to:

- offering of goods or services to data subjects in the EU; or
- monitoring of data subject's behavior as far as their behavior takes place within the EU;

In addition to the GDPR, the PDPA includes specific derogations, rules implementing the GDPR, and provisions transposing the Law Enforcement Directive. In the absence of extra-territorial provisions, these national data protection rules apply solely within Bulgaria or in areas where Bulgarian laws are enforced by international law (e.g., Bulgarian diplomatic and consular missions abroad, Bulgarian-flagged ships sailing in international waters, and similar situations governed by international law).

What are the key factors and considerations to adhere to when engaging in the processing of personal data within your jurisdiction?

The key factor is the proper identification and consideration of the organization's role as a controller, processor, or joint controller. Correctly determining this role is crucial, as it defines the organization's specific data protection rights and responsibilities. Below are key obligations for controllers that must be considered:

- adhering to data processing principles (such as lawfulness, transparency, purpose limitation, data minimization, and storage limitation as set forth in the GDPR) when processing personal data;
- appointing a data protection officer, if required;
- managing the data protection risk by ensuring data protection by design and by default, conducting data protection impact assessment, undertaking prior consultation with the data protection authority, and implementing suitable technical and organizational measures;
- ensuring accountability through measures demonstrating compliance with data protection laws, including keeping records of processing activities, adhering to the approved code of conduct or data protection certification mechanism, as well as employing other means for ensuring accountability;
- managing relations with the data protection authority by cooperating when the authority exercises its powers and complying with the statutory obligations for data breach notification;
- regulating the relations among joint controllers by defining in an arrangement the respective responsibilities for GDPR compliance of each joint controller and making those arrangements accessible to data subjects;
- appointing an EU representative, if the organization lacks an EU establishment and processes the data of EU residents;
- taking responsibility for controller-processors relations by using processors providing sufficient guarantees for GDPR compliance and formalizing the relationship in a contract;
- ensuring compliant data processing in an international context by taking measures to ensure that transfers of personal data outside the EU provide adequate protection, through adequacy decisions, appropriate safeguards, binding corporate rules, or other means.

All these obligations are governed by the GDPR, not by local Bulgarian legislation. Although certain processing operations concerning these obligations may call for the application of local derogations or national Bulgarian law rules, businesses can rely on the uniform set of key data protection obligations established by the GDPR throughout the EU.

What are the regulations and best practices concerning the retention and deletion of personal data in Bulgaria?

The PDPA provides a few rules on data retention that are specific to the GDPR. If a controller or processor becomes aware that it is retaining data contrary to the principles of the GDPR or without a legal basis, it must either return the data to the data subject within one month of becoming aware of the retention or, if this is impossible or involves a disproportion-

ate effort, erase or destroy the data. In addition, any employer acting as a data controller must determine a retention period for personal data relating to job applicants, which may not exceed six months, unless the job applicant has consented to the retention for a longer period. Sector-specific legislation provides for some sector-specific statutory retention periods (e.g., 50 years for payroll records, ten years for accounting records and financial statements, including tax control, and five years for reports on occupational accidents) and for some specific retention rules (see for example the traffic data retention obligations of electronic communications providers discussed above). Apart from this, Bulgarian data protection law does not provide for general rules on data retention and therefore data controllers need to develop retention policies based on the general principle of the GDPR on storage limitation and the specific sectoral legislation, if any.

At the end of the retention period, retained data would generally be erased (if in electronic form) or destroyed (if on a physical medium). The PDPA defines "erasure" as the irreversible deletion of information from the relevant medium and "destruction" as the irreversible physical destruction of the tangible information medium. Otherwise, there are no specific local rules for erasure or destruction. Therefore, similarly to retention activities, when deleting or destroying personal data, the organization acts in accordance with the GDPR rules.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

The Commission for Personal Data Protection (CPDP) is the statutory authority that supervises the protection of personal data in Bulgaria. The CPDP is an independent supervisory authority consisting of a chairman and four members. The authority performs the tasks set out in Art. 57 (e.g., handling complaints from a data subject, raising awareness among the public, data controllers, data processors, and data subjects, cooperating with other supervisory authorities, advising national institutions on data protection issues) and has the powers set out in Art. 58 of the GDPR (e.g., to conduct investigations, request information, issue orders, warnings, and reprimands, impose fines, accredit certification bodies, advise controllers during the prior consultation process, and others). In addition, it exercises general supervision and ensures compliance with the GDPR and the PDPA, issues regulations and administrative acts in the field of personal data protection, ensures the implementation of binding decisions of the European Data Protection Board, and carries out other activities, unless the law entrusts supervision to the Inspectorate of the Supreme Judicial Council.

The Inspectorate of the Supreme Judicial Council supervises the protection of personal data when the data processor is the court, the public prosecutor, and the investigating authorities when they act in their judicial capacity for the purpose of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in Bulgaria, and under what conditions?

With respect to the appointment of a data protection officer (DPO), Bulgarian data protection law does not provide for any rules that differ from the GDPR. Therefore, the obligation to appoint a DPO arises for the controller where:

- the processing is carried out by a public authority or body, with the exception of courts acting in their judicial capacity; or
- its activities, by their nature, scope, and purposes, require regular and systematic monitoring of data subjects on a large-scale; or
- its core activities consist of the large-scale processing of special categories of data and personal data relating to criminal convictions and offenses.

Neither the PDPA through its provisions nor the CPDP in its practice has clarified concepts such as "systematic," "core activities," or "significant number." Therefore, in assessing the requirement to appoint a data protection officer, controllers and processors in Bulgaria closely follow the Guidelines on Data Protection Officers issued by Working Party 29 and endorsed at the first plenary meeting of the European Data Protection Board. However, an issue specific to Bulgaria arose before the CPDP in relation to the obligation to keep a register of designated DPOs. Due to the different understanding of whether the DPO must be a natural person or whether such obligations can be fulfilled by legal persons, the CPDP had to unify the practice of controllers and processors and issue a specific publication on the matter. In its position, the data protection authority (DPA) did not explicitly exclude the possibility of a legal entity or other organization providing services related to the functions of the DPO, but considered that the functions of the DPO can only be performed by an individual. Therefore, the DPA has expressed the opinion that controllers and processors who have delegated the functions of the DPO to legal entities under a service contract must designate a specific individual responsible for performing the functions of the DPO for a particular controller or processor.

How should data breaches be handled in your jurisdiction?

The activities of processors and controllers with respect to data breaches are regulated by the GDPR, and the PDPA

does not provide for further implementing or deviating from local rules. With respect to data breaches, the CPDP generally advises controllers and processors to comply with the requirements of Article 33 of the GDPR and Guidelines 9/2022 on personal data breach notification issued by the European Data Protection Board. However, in order to raise awareness among both the public and obligated entities, the CPDP has published an information brief summarizing the main obligations relevant in the event of a data breach. The briefing covers issues such as what a data breach is, types of data breaches, what actions should be taken when notification to the supervisory authority or data subjects is required, what technical and organizational measures should be taken to minimize the likelihood of a breach occurring, and others. In addition, the CPDP has developed a personal data breach notification form which, while not mandatory, is designed to help controllers better navigate the information they need to provide in relation to the breach and to facilitate the fulfillment of this obligation.

What are the potential penalties and fines for non-compliance with data protection regulations in Bulgaria?

Due to the direct application of the GDPR, the grounds for the imposition of administrative sanctions and the constituent elements of the offenses are laid down in the GDPR, not in local legislation. GDPR allows for two tiers of administrative fines based on the severity and nature of the infringement:

- The lower tier of sanctions envisages administrative fines of up to EUR 10 million or, in the case of legal entities, 2% of their total worldwide annual turnover for the preceding financial year, whichever is higher. This tier of sanctions extends to violations such as failure to comply with the obligations related to the processing of children's personal data, the tasks of a DPO, implementation of data protection by design and by default, and others.
- A higher tier, of administrative fines of up to EUR 20 million or, in the case of legal entities, 4% of their total worldwide annual turnover for the preceding financial year, whichever is higher, applies to more serious violations, including breaches of the basic principles for processing, including conditions for consent, infringements of data subjects' rights, infringements related to international transfers of personal data, and others.

In addition to the GDPR measures, the PDPA provides for a local rule pursuant to which, for violations that are not amongst the ones explicitly listed in the PDPA, a controller or processor of personal data shall be subject to an administrative sanction of up to BGN 5,000 (approximately EUR 2,500). For repeated violation i.e., committed within one year from the date of a final CPDP decision by virtue of which the authority has imposed a sanction for the same type of breach, the administrative sanction is doubled.

Some breaches of data protection rules may qualify as crimes under Bulgarian law. As an example, the use of data from a payment instrument without the consent of the owner qualifies as a crime and it is punishable with imprisonment of two to eight years. The unlawful acquiring, storage, or disclosure of traffic data is a crime punishable with imprisonment of up to three years or probation.

Are there any noticeable patterns or trends in how enforcement is carried out in Bulgaria?

Despite operating in an environment with relatively low data protection awareness, the CPDP has not been among the more active data protection regulators. This inactivity is largely due to insufficient financial and human resources and the unique situation of the chairman and some commission members who hold long-expired mandates (nearly five years). Typically, when a data protection violation is identified, the CPDP imposes administrative sanctions ranging from BGN 1,000 (approximately EUR 500) to BGN 10,000 (approximately EUR 5,000). Larger sanctions are rare (with isolated instances in 2019, 2021, and 2022) and usually involve breaches affecting a large number of data subjects.

According to the CPDP's 2023 annual report, during 2023 the data protection authority imposed administrative fines at the amount of BGN 90,900 (approximately EUR 45,450) based on 37 penal deeds and 12 settlement agreements with the controller. Given the figures in the annual report of the European Data Protection Board for the same year, the CPDP appears to be a conservative regulator, imposing administrative fines frequently – only Germany, Spain, Italy, and Hungary issued fines more often. However, the average amount of the fine remains very low, compared to other jurisdictions. In addition, corrective measures together with administrative sanctions were imposed only in five of the cases.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in Bulgaria?

Emerging technologies like the IoT, AI, and blockchain are revolutionizing our ability to collect, process, and derive new and even predictive information from vast and diverse datasets. While these technologies offer numerous benefits, they also introduce significant privacy and data protection challenges as vast amounts of personal information are collected and processed in increasingly sophisticated and opaque ways.

AI, in particular, presents several potential risks, including opaque decision-making processes, privacy invasions, and the

potential for these technologies to be used unlawfully. Additionally, AI can perpetuate biases and lead to discrimination based on gender, race, ethnic or social origin, religion, political beliefs, property status, disability, age, or sexual orientation. To counterbalance these risks, effective application of data protection and privacy principles is a must.

Bulgarian data protection law aligns with the GDPR and does not provide additional rules specifically for data processing involving AI, IoT, or blockchain. However, all stakeholders – data controllers, data subjects, and regulators – are aware of the risks of these technological advancements.

To support the practical implementation of data protection requirements in the context of AI and big data trends, the Bulgarian regulator has developed several informational materials for both data subjects and controllers. These resources address the challenges of facial recognition, big data profiling, and best practices for using cloud services. They highlight key GDPR obligations and the associated risks and challenges of emerging technologies. While these publications are not legally binding, they provide insight into the CPDP's stance on these issues.

In its 2023 annual report, the Bulgarian data protection authority presented as a focus area for 2024 the conduct of data protection impact assessments when planning data processing activities involving AI. Additionally, there will be efforts to raise awareness among data subjects about the implications of increased data integration and faster exchanges between economic operators within the EU, driven by the Digital Services Act and the Digital Markets Act.

Are there any expected changes in data protection on the horizon in the next 12 months in Bulgaria?

Based on the recent draft laws submitted to the Bulgarian Parliament, amendments to personal data processing regulations in the Bulgarian electronic communications sector are on the horizon. The Court of Justice of the European Union in judgment C-350/21 ruled that general and non-selective retention of traffic and location data for law enforcement purposes, even if limited to six months and even if providing some safeguards, is incompatible with EU law. This judgment necessitates changes in Bulgarian laws, to ensure that data retention is strictly necessary and proportionate. In response to this judgment, on February 28, 2024, several Members of Bulgaria's parliament proposed amendments to the Electronic Communications Act to align it with EU law. Key proposals include:

- limiting traffic data retention by electronic communications providers for a period of ten days in un-encrypted form and for an additional 160 days in encrypted form, using asymmetric encryption;
- obligation of the competent law enforcement authorities to keep a non-public centralized registry, detailing the legal basis of access requests, court order identifications, documents used in proceedings, authorized officials, and other relevant information;
- obligation of the competent law enforcement authorities to notify, under certain conditions, the individuals whose traffic data has been retained, such as when criminal proceedings are terminated or when data has been used for preventing serious crime.

In addition to legislative updates, there is a long-overdue need to change the composition of the data protection authority in Bulgaria. The current CPDP chairman was elected in 2014 and should have been re-elected or replaced in 2019. Two members re-elected in 2014, are now ineligible for a third term. One new member needs to be elected to complete the commission, and another member was due for replacement or re-election in 2019. However, none of these changes have occurred. Instead, the law has been amended to allow elected members to remain in office until new appointments are made. This extension beyond the statutory mandate, even if legally provided for an unspecified term, makes the commission politically vulnerable and potentially undermines its independence.

At the time of writing, it is uncertain whether the proposed draft legislation will be enacted, having in mind the general elections in June 2024. It is anticipated that a new chairman and new members of the CPDP will only be elected after the elections, following a political agreement. ■

ROWAN® LEGAL

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

CZECH REPUBLIC

Michal Nulicek
Partner
nulicek@rowan.legal
+420 603 180 360

Filip Benes
Senior Associate
benes@rowan.legal
+420 725 159 045

CEE LEGAL MATTERS

www.ceelegalmatters.com

What are the primary data protection-related laws and regulations in the Czech Republic?

Since the Czech Republic is an EU Member State, Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 (GDPR) is the major regulation applicable in this area.

In terms of national law, the relevant act is Act No. 110/2019 Coll., on the Processing of Personal Data, which, for example, provides for exceptions to the general legal framework where the GDPR allows it and implements Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016.

Some data protection-related topics are covered by specific regulations, such as Act No. 127/2005 Coll., on Electronic Communications, which applies to the use of cookies and other tracking technologies, telemarketing, and data retention. The rules for sending commercial communications in emails or by SMS are stipulated by the so-called Anti-Spam Act, Act No. 480/2004 Coll., on certain Information Society Services.

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, or equivalent)?

The definitions apply in principle to the extent defined in the GDPR.

Which entities fall under the data privacy regulations in the Czech Republic?

In general, all entities, including governmental bodies that process personal data, fall under the GDPR or under Act No. 110/2019 Coll., on the Processing of Personal Data.

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

The general framework is set out in the GDPR and Act No. 110/2019 Coll., on the Processing of Personal Data. However, there are sectoral legal regulations that impose an obligation on the affected entities to process personal data (e.g., AML laws, legislation relating to the provision of health services and the maintenance of medical records, legal duties of confidentiality).

What rights do data subjects have under the data protection regulations in the Czech Republic?

Data subjects have the same rights as provided by the GDPR. Act No. 110/2019 Coll. introduces certain exceptions and nuances regarding processing for journalistic purposes or for the purposes of academic, artistic, or literary expression. The first one is the exemption from the rights to rectification, erasure, and restriction of processing, which are governed by separate legislation.

The second exception concerns the limitation of the right to object. This right may be revoked only against a specific disclosure or publication of personal data. The data subject must provide reasons demonstrating that, in the specific case, the legitimate interest in protecting their rights and freedoms outweighs the interest in disclosure or publication.

What is the territorial application of the data privacy regime in your jurisdiction?

There is no deviation from the GDPR in the Czech legislation. The GDPR applies to the EU and compliance with it in the Czech Republic is supervised by the Office for Personal Data Protection.

Within a one-stop-shop regime, the Czech data protection authority oversees compliance with data protection laws within the country, ensuring that controllers and processors seated in the Czech Republic handle personal data in accordance with the regulations.

What are the key factors and considerations to adhere to when engaging in personal data processing within your jurisdiction?

There are no distinct or specific key factors and considerations applicable to the processing of personal data in the Czech Republic.

The main obligation is to define the purposes of the processing, to draft privacy policies for the affected data subjects (e.g., customers, employees), and to prepare other documentation.

Are there regulations and best practices concerning the retention and deletion of personal data in the Czech Republic?

The Czech DPA requires controllers to inform data subjects of the retention period in a way that is comprehensible to the average consumer. While the period does not need to be precisely defined, it is essential to outline the criteria that guide its determination.

Moreover, some retention periods are also stipulated by pertinent laws.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

The Office for Personal Data Protection (Urad pro ochranu osobnich udaju) is the supervisory authority with general competence regarding data protection in the Czech Republic.

However, other supervisory authorities may also be active in certain areas. This is the case of the Czech Telecommunications Office, which is the competent authority for compliance with telemarketing rules. In the case of employee monitoring, the competent authority is the State Labor Inspection Office.

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in the Czech Republic, and under what conditions?

Article 37 of the GDPR sets out the conditions under which an organization must appoint a data protection officer. These conditions remain the same in the Czech Republic. This means that the appointment of a data protection officer is necessary for public authorities and public bodies or when data subjects are regularly and systematically monitored on a large scale or sensitive data such as health data or data relating to criminal convictions and offenses is processed.

How should data breaches be handled in your jurisdiction?

The procedure in the event of a data breach is identical to that set out in the GDPR. The controller is obligated to notify the breach of personal data to the supervisory authority within 72 hours after having become aware of it. If the breach is likely to result in a high risk for data subjects, the controller must also inform them.

In addition, in some cases, sectoral legislation sets out additional requirements for notifying supervisory authorities. Companies, particularly those operating critical infrastructure, may be required to report data breaches to the National Cyber and Information Security Agency, and financial institutions are in some cases required to notify data breaches to the Czech National Bank.

What are the potential penalties and fines for non-compliance with data protection regulations in the Czech Republic?

For failure to comply with data protection regulations, data controllers or processors may be subject to administrative fines of up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year.

The highest fine imposed by the Czech DPA as of April 2024 was EUR 14.1 million.

The Czech Republic utilized the possibility to set different fines for public authorities and public bodies. According to Act No. 110/2019 Coll., the supervisory authority will refrain from imposing a fine on them.

Are there any noticeable patterns or trends in how enforcement is carried out in the Czech Republic?

As noted above, the competent supervisory authority is the Office for Personal Data Protection. The primary mechanism for overseeing and enforcing GDPR compliance is through inspections and audits.

These inspections are initiated either pursuant to a predetermined inspection plan or in response to a complaint lodged by an individual regarding their personal data or following a data breach.

Current decision-making trends indicate that the supervisory authority consistently adheres to the guidance provided by the European Data Protection Board in determining penalties for GDPR violations. Consequently, the assessment of fines is rigorously guided by the turnover criterion in compliance with the EDPB's guidelines.

The traditional area in which the Czech DPA is active is compliance with the rules on transmitting commercial communications, as this is also where it receives the most complaints. In the Czech Republic, commercial communications can only be transmitted with or without prior consent to one's own customers and only if other conditions are met.

Over the past two years, the DPA has also been very active in monitoring and regulating the use of cookies on websites.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in the Czech Republic?

The Czech Republic is currently preparing to adopt European regulations governing artificial intelligence (AI Act) and the disclosure of personal and non-personal data (Data Act). Consequently, we expect increased activity in this area.

Are there any expected changes in data protection on the horizon in the next 12 months in the Czech Republic?

Changes directly relating to data protection are not anticipated within the next 12 months in the Czech Republic. However, the Digital Economy Bill is currently under discussion. This legislation is expected to enact significant modifications concerning the transmission of commercial communications and regulations governing the dissemination of commercial communications via electronic channels.

This new legislation is expected to establish a maximum duration during which commercial communications can be transmitted to customers without their prior consent. This marks a departure from the current scenario where no statutory time limit exists, leaving it to data controllers to establish the duration in accordance with other principles of data protection legislation. ■

DRAKOPOULOS

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

GREECE

Michalis Kosmopoulos
Partner
mkosmopoulos@drakopoulos-law.com
+30 2106836561

Angie Alevizou
Senior Associate
aalevizou@drakopoulos-law.com
+30 2106836561

CEE
LEGAL MATTERS

www.ceelegalmatters.com

What are the main data protection-related pieces of legislation and other regulations in Greece?

The legislation governing the protection of personal data in Greece focuses initially on the implementation of the General Data Protection Regulation (EU) 2016/679 (GDPR). Greek Law 4624/2019 transposed measures for the adaptation of national data protection legislation to the GDPR. It also incorporated Directive 2016/680/EU 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 offenses or the execution of criminal penalties, and on the free movement of such data.

Furthermore, regarding the protection of personal data and privacy in the electronic communications sector, Greek Law 3471/2006 embodies Directive 2002/58/EC as amended by Directive 2009/136/EC. Regarding the air carriers' obligations with respect to passenger records, Greek Law 4579/2018 transposes into national law Directive 2016/681/EU on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offenses and serious crime.

In addition, Greek Law 5002/2022 refers to the procedure for lifting the confidentiality of communications, cybersecurity, and protection of personal data of citizens, and Greek Law 4577/2018 transposing the NIS Directive (EU 2016/1148), imposes system and network security obligations on businesses in the fields of energy, transport, credit, financial infrastructure, health, water and digital infrastructure, e-commerce, and information society services.

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, etc., or equivalent)?

The definitions that prevail in the Greek jurisdiction are the public body, the private body, and the competent supervisory authority. The first definition refers to public authorities, independent and regulatory administrative authorities, legal persons governed by public law, first and second-tier local authorities and their legal persons and undertakings, state or public undertakings and bodies, legal persons governed by private law which are owned by the state or subsidized by at least 50% of their annual budget or whose management is determined by the state.

The second definition applies to a natural or legal person or association of persons without legal personality that does not fall within the concept of a public body, while the third definition identifies the Hellenic Data Protection Authority as the supervisory authority.

Other than the above, Greek Law 4624/2019 reflects the definitions referred to in the GDPR.

Which entities fall under the data privacy regulations in Greece?

The provisions of the Greek Law 4624/2019 apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data that form part of a filing system or are intended to form part of a filing system by public bodies or private bodies, unless the processing is carried out by a natural person in the course of an exclusively personal or domestic activity.

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

As mentioned above, there are distinct regulatory regimes for data in the sectors of electronic communications, cybersecurity, air carriers' obligations regarding passenger records, energy, transport, credit, financial infrastructure, health, water and digital infrastructure, e-commerce, and information society services, and public works, as well as for the identification of owners and users of mobile telephony equipment and services in the Greek jurisdiction.

What rights do data subjects have under the data protection regulations in Greece?

Strengthening and setting out in detail the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements, leads to the effective protection of personal data. By virtue of articles 35, 52, and 53 et seq. of Greek Law 4624/2019, the data subjects have the following rights:

- The right to information/transparency, i.e., the right to know who is processing their data, what categories of data they are using, and why.
- The right to access, i.e., the right to request access to the personal data that an organization has about them.
- The right to rectification, i.e., the right to have the data rectified, if their data is inaccurate and/or incomplete.
- The right to erasure ("right to be forgotten"), i.e., the right to have their personal data erased under specific conditions, such as when their data is no longer necessary, they have withdrawn their consent, their data has been unlaw-

fully processed, etc.

- The right to restriction of processing, i.e., the right to obtain restriction of processing where the accuracy of their personal data is contested, the processing is unlawful, the controller no longer needs the personal data for the purposes of the processing, they have objected to automated processing.
- The right to object, i.e., the right to object to the processing of their personal data by an organization, provided that it does not apply to a public body if there is an overriding public interest in the processing that overrides the interests of the data subject or if a provision of law requires the processing to be carried out.
- The right to non-automated individual decision-making, i.e., the right to object where a decision is based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them.
- The right to lodge a complaint with the Hellenic Data Protection Authority, if they believe that the processing of personal data concerning them by competent authorities for the purposes referred to in Article 43 infringes their rights.

In the context of criminal investigations and proceedings, the right to information on the processing, access, correction or deletion, and restriction of personal data are exercised in accordance with the provisions of the Code of Criminal Procedure, special procedural provisions, and the Code on the Organization of Courts and the Status of Judicial Officers.

What is the territorial application of the data privacy regime in your jurisdiction?

The provisions of Article 3 of Greek Law 4624/2019 on the territorial application of the data privacy regime apply to public bodies. For private bodies, Greek Law 4624/2019 shall apply where the controller or processor processes personal data within the Greek territory, the personal data are processed in the context of the activities of an establishment of the controller or processor within the Greek territory, or where, although the controller or processor does not have an establishment in a Member State of the European Union or in another Contracting State of the European Union, the personal data are processed in the context of the activities of an establishment of the controller or processor within the Greek territory, or where the controller or processor does not have an establishment in a Member State of the European Union or in another Contracting State of the European Union.

What are the key factors and considerations to adhere to when engaging in the processing of personal data within your jurisdiction?

Any processing of personal data should be carried out in accordance with the provisions of Greek Law 4624/2019 which, as mentioned above, transposes Regulation (EU) 2016/679 and Directive 2016/680/EU into Greek law. In particular, a controller and/or processor should comply with the key principles and factors such as transparency, the lawful basis for processing, purpose limitation, data minimization, proportionality, retention, accuracy, data security, and accountability.

What are the regulations and best practices concerning the retention and deletion of personal data in Greece?

The provisions of Greek Law 4624/2019 stipulate that personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be retained for longer periods of time if they have been stored for the purposes of scientific or historical research or for statistical purposes in the public's interest and provided that the appropriate technical and organizational measures are applied.

Additionally, data subjects have the right to erasure in situations where: (i) the data are no longer needed for their original purpose; (ii) the data subject has withdrawn its consent for processing, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the Controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU or national data protection law. Additionally, Article 33 of the Greek Law 4624/2019 stipulates that, if certain conditions are met, the erasure of the data may be replaced by the mere restriction of their processing.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

The Hellenic Data Protection Authority (HDPA) is the Greek supervisory authority responsible for monitoring the application of Greek Law 4624/2019 and, more generally, the GDPR. It ensures compliance with data protection laws and regulations and publishes from time-to-time guidance, opinions, and decisions on information rights and data protection in Greece.

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in Greece, and under what conditions?

According to the provisions of Greek Law 4624/2019 and, in particular, Article 37, which fully implements the General Data Protection Regulation (EU) 2016/679, controllers and processors must appoint a Data Protection Officer (DPO), when:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- The core activities of the controller of the processor consist of (a) processing operations requiring regular and systematic monitoring of data subjects on a large scale and (b) processing on a large scale of special categories of data (such as health data or data revealing ethnic origin) or personal data relating to criminal convictions and offenses.

The mandatory appointment of a DPO for public authorities or bodies is also provided for in Article 6 of Greek Law 4624/2019. Businesses are free to appoint a DPO in cases where they are not legally obliged to do so. If an organization voluntarily appoints a DPO, the same requirements of the GDPR concerning their designation, position, and tasks apply as if the organization were required to appoint a DPO.

The DPO is responsible for advising the controller or processor on their obligations under the GDPR, monitoring compliance with the GDPR and the policies of the organization in relation to the protection of personal data, including assignment of responsibilities, awareness-raising, and training of relevant staff as well as acting as a point of contact for data subjects and the supervisory authority (HDPA).

How should data breaches be handled in your jurisdiction?

In Greek jurisdiction, the handling of data breaches follows specific procedures outlined by the country's alignment with the GDPR. When a data breach occurs, namely a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed, organizations should take immediate action to mitigate its impact and comply with legal obligations.

Firstly, the organization must assess the nature and extent of the incident. This involves determining what data was compromised, how it happened, and the potential consequences for the individuals affected.

Then, the controller must, without undue delay and no later than 72 hours after having become aware of the breach, notify the HDPA providing detailed information about the incident, including its causes, the types of data involved, and the number of individuals affected. This obligation also applies to the processor, who must notify the controller promptly after becoming aware of the data breach. The notification should be clear and concise, detailing the nature of the breach, the categories of persons affected, the potential consequences, and any actions taken to address and mitigate the breach.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the breach to the data subject without undue delay and in accordance with Article 34 of GDPR. However, in certain circumstances and by virtue of Article 33(5) of Greek Law 4624/2019, the above obligation shall not apply to the extent that the notification would entail the disclosure of information that, according to the law or by reason of its nature, due to overriding legitimate interests of third parties, should remain confidential.

It is an indisputable fact that the handling of data breaches in Greek jurisdiction requires swift action, transparency, and compliance with GDPR requirements and national data protection laws. All organizations affected must take immediate steps to contain the breach and prevent further unauthorized access to or disclosure of personal data. This may include implementing security measures, such as modification of passwords, encryption data, or temporarily shutting down affected systems. A thorough investigation might be also necessary to understand the root causes of the breach and identify any weaknesses in the company's data protection practices.

What are the potential penalties and fines for non-compliance with data protection regulations in Greece?

According to the accountability principle, failure to demonstrate compliance with the data protection regulations in Greece is considered a breach of the obligations set forth by the GDPR. According to Article 83 of the GDPR, failure of the organization to comply with the requirements provided in the data protection regulations in Greece may expose it to administrative fines of up to EUR 20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Such administrative fines may be imposed, in particular, for any breach of the basic principles of data processing, pursuant to Article 5 (Principles relating to processing of personal data), 6 (Lawfulness of processing), and 9 (Processing of special categories of personal data) of the GDPR, as well as of the data subjects' rights pursuant to Articles 12 to 22 of the GDPR.

Moreover, failure to comply with the obligations under Arti-

cles 25 to 39 of the GDPR (on the Role and obligations of Controllers and Processors, Security of Personal Data, and Data Processing Impact Assessment) may expose the organization to administrative fines of up to EUR 10 million or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Fines on public entities are limited by Article 39 of Greek Law 4624/2019 to up to EUR 10 million depending on the severity and duration of the breach.

Besides the above, civil claims against the entity and or criminal sanctions against the entity's legal representative may also apply.

Are there any noticeable patterns or trends in how enforcement is carried out in Greece?

In Greece, the enforcement of data protection regulations has followed a pattern that aligns closely with the GDPR. Emphasis is given to transparency and accountability. Organizations operating in Greece are required to be transparent about their data processing activities and inform individuals about how they collect and use their personal data.

The HDPA is empowered to advise the controllers/processors on data protection matters, issue opinions, guidelines, recommendations, template documents, and complaint forms, ensuring adherence to the data protection legislation. It also has investigative powers to conduct investigations and audits on compliance with the data protection legislation, to request and receive from controllers/processors all necessary information, and to have access to their premises and data processing equipment. Another trend is the increasing focus on data security measures. With the increasing number of data breaches globally, including in Greece, the HDPA has been vigilant in enforcing measures to protect personal data from unauthorized access, disclosure, alteration, or destruction. Companies and organizations implement appropriate technical and organizational measures to safeguard the confidentiality, integrity, and availability of personal data. Moreover, there is a trend toward collaboration and cooperation with other EU data protection authorities. Given the cross-border nature of data flows, especially within the EU, the Greek authorities work closely with their counterparts in other member states to ensure consistent enforcement of the data protection laws and to address the challenges posed by international data transfers.

Overall, data protection enforcement in Greece reflects a commitment to upholding individuals' privacy rights and holding organizations accountable for the protection of personal data. The trends suggest a proactive approach aimed at promoting compliance, enhancing data security, and fostering trust in the digital economy.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in Greece?

Emerging technologies have significant implications for data protection considerations in Greece. For instance, AI technologies offer innovative ways to collect, process, and utilize data, but they also introduce new challenges and risks in ensuring the privacy and security of individuals' personal information.

On July 27, 2022, the Greek Government introduced Greek Law 4961/2022 "on emerging information and communication technologies, the reinforcing of digital governance and other provisions". Pending any changes due to the adoption of the AI Act by the European Union, the new law introduces the first coherent legislative framework for emerging technologies, setting obligations for public bodies as well as natural persons and private entities that produce, distribute, utilize, and make use of these technologies.

In order to regulate the use of emerging technologies, each public body must maintain a register of the AI systems it uses and has the right to use AI systems only by virtue of a specific provision by law, except for the Ministries of National Defense and Citizen Protections. Additionally, before using an AI system, each public body has the obligation to execute an algorithmic impact assessment to assess the risks that may arise for the rights, freedoms, and legitimate interests of the persons affected by such an AI system. Each public body publicly discloses information, inter alia, about the commencement of operation and the operating parameters of the AI system under consideration as well as the decisions taken or supported by it.

As regards private entities, Greek Law 4961/2022 sets the conditions for the use of AI in the employment context. In particular, prior to the initial use of an AI system, which affects the decision-making process concerning employees, existing or prospective, and has an impact on their conditions of employment, selection, recruitment, or evaluation, each company shall provide the employee with the relevant information. The relevant obligation also applies to digital platforms with respect to natural persons linked to them by employment contracts independent service provisions or project agreements. Any violation of this obligation is subject to penalties imposed by the Labor Inspectorate.

Moreover, Greek Law 4961/2022 imposes legal obligations on manufacturers, importers/distributors, and operators of IoT devices. More specifically, manufacturers should accompany IoT devices with a declaration of compliance with the technical safety specifications, indicated in the law, as well as instructions for use and safety information. Importers and

distributors should verify that the IoT devices they import or distribute are accompanied by a relevant declaration of compliance, while IoT operators should appoint an IoT security officer to monitor the security measures of IoT technology devices and maintain a register of IoT devices, updated on an annual basis. Lastly, each IoT operator should conduct an impact assessment of the planned personal data processing operations related to the operation of the IoT technology device.

It should be clearly stated that the provisions of Greek Law 4961/2022 on emerging technologies do not affect the rights and obligations provided for in the GDPR and Greek Law 4624/2019 on the protection of personal data. Therefore, a relevant reference has been included in Article 3, ensuring that the proposed provisions do not affect, in any way, the rights and obligations deriving from the GDPR and Greek Law 4624/2019 for the protection of personal data and privacy. In an effort to monitor compliance with the new technologies, the new law also establishes the National Cybersecurity Certification Authority in accordance with Article 58 of Regulation (EU) 2019/881.

Overall, Greece can harness the potential of emerging technologies while safeguarding individuals' rights to data privacy and security. Greek Law 4961/2022 boosts the digital transformation of the country's public and private sectors, while new regulations are expected upon adoption of the EU AI Act.

Are there any expected changes in data protection on the horizon in the next 12 months in Greece?

While there might not be imminent legislative changes specific to the Greek data protection landscape in the next 12 months, ongoing developments at the EU level, particularly with the adoption of the AI Act, are likely to have an impact on Greece as well. The importance of maintaining a proactive approach to data protection compliance should remain a key priority for businesses and stakeholders in Greece. ■

provaris
VARGA & PARTNERS

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

HUNGARY

Tamas Bereczki
Partner
bereczki.tamas@provaris.hu
+36 30 220 2428

Adam Liber
Partner
liber.adam@provaris.hu
+36 20 524 4959

Eliza Nagy
Associate
nagy.eliza@provaris.hu
+36 70 674 7068

CEE
LEGAL MATTERS

www.ceelegalmatters.com

What are the main data protection-related pieces of legislation and other regulations in Hungary?

In Hungary, two key pieces of legislation govern data protection: the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), directly applicable in Hungary, and the national Hungarian Information Self-Determination and Freedom of Information Act (Privacy Act). While the GDPR provides a broad framework for data protection, the Privacy Act specifically regulates data processing for purposes such as law enforcement, national defense, and national security. The Privacy Act supplements the GDPR's provisions with national implementing measures. The Privacy Act mandates the application of the GDPR provisions to manual data processing activities, even if they are not part of a filing system.

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, etc., or equivalent)?

In accordance with the GDPR and the Privacy Act, the primary definitions within these legislations are as follows:

Personal data can be considered as any information relating to an identified or identifiable natural person. A natural person is identifiable if they 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.

Data processing is any operation or set of operations that is performed on personal data or sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

A data controller can be a natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. On the other hand, a data processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

Sensitive data refers to all data falling within the special categories of personal data, including, personal data revealing racial or ethnic origin, political opinion, religious belief or worldview, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Within sensitive data, genetic data is related to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of that natural person, and which result, in particular, from an analysis of a biological sample from the natural person in question. Furthermore, biometric data result from specific technical processing related to the physical physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Criminal personal data can be connected to the data subject and are related to criminal records, generated by organs authorized to conduct criminal proceedings or to detect criminal offenses, or by the prison service during or prior to criminal proceedings, in connection with a criminal offense or criminal proceedings. Regarding the processing of Criminal personal data, the rules relating to the conditions for processing sensitive data are applicable to such data processing.

Consent of the data subject is a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her.

Which entities fall under the data privacy regulations in Hungary?

Given that the GDPR applies directly in Hungary, any natural, legal person, public authority, agency, or other body must comply with its provisions if the territorial scope under Article 3 of the GDPR encompasses their activities.

The Privacy Act is applicable to any natural or legal person or organization without legal personality. However, these entities only fall under the Privacy Act if they process for national security, national defense, or law enforcement purposes.

The GDPR and the Privacy Act do not apply to the processing activities of natural persons exclusively serving their own personal purposes.

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

In Hungary, certain sectors, including healthcare, public administration, business advertising, and financial services, among others, are subject to additional data protection regulations, typically more stringent in nature. While some acts solely regulate the retention periods of personal data processed under them, others provide additional protection for data subjects.

Act I of 2012 on the Labor Code (Labor Code) offers specific protections for employees' personal rights. Under this law, employers in Hungary are limited to requesting personal data that is directly relevant to establishing, performing, terminating employment relationships, or enforcing claims as outlined in the Labor Code. Act XCIII of 1993 on Labor Safety (Labor Safety Act) governs the processing of employee personal data by the employer in the event of occupational accidents.

Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data (Health Data Act) governs the processing and protection of personal health data, implementing a comprehensive regulatory framework. This legislation addresses various aspects of health personal data processing, including the provision of voluntary and obligatory data. Additionally, the Health Data Act outlines the rights and obligations of patients, ensuring they receive detailed information regarding their health status, recommended examinations, and associated benefits and risks.

In Hungary, the business advertising sector operates under stringent data protection regulations as well. Act XLVIII of 2008 on Essential Conditions of and Certain Limitations to Business Advertising Activity (Business Advertising Act) stipulates that direct advertisements may only be communicated to natural persons only if the addressees of the advertisement gave their preliminary consent, clearly and expressly, to being contacted in this way. Furthermore, the consent must include the name, place of birth, and date of birth of the recipient, as well as the categories of personal data for which the recipient has given consent to be processed.

Data collected while performing tasks outlined in Act LIII of 2017 on preventing and Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act) may solely be used for preventing money laundering and terrorist financing. Service providers are mandated to retain and be authorized to process this information for eight years following the termination of the business relationship or execution of the transaction order.

There are several sector-specific acts that specify exact retention and deletion periods processing under the sector-specific act. For example, in the financial sector, Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises states that client complaints and their replies shall be retained for five years and contracts with clients for mediation services and mediated financial services contracts shall be retained for three years. Act CL of 2017 on the Rules of Taxation outlines retention periods of tax-related documents for taxpayers and employers and Act C of 2000 on Accounting sets requirements regarding retention periods for businesses regarding their annual report, inventory, and any accounting documents.

What rights do data subjects have under the data protection regulations in Hungary?

Data subjects in Hungary have various rights under the GDPR and the Privacy Act. They are entitled to receive transparent information about the processing of their personal data, including purposes, legal basis, and recipients of their data. Additionally, they have the right to access their personal data, they can also request rectification of inaccuracies or incompleteness, and the erasure of their personal data under certain conditions (the "right to be forgotten"). Furthermore, data subjects have the right to request restrictions on processing and data portability, and to object to certain processing activities. Moreover, data subjects have the right not to be subject to decisions based solely on automated processing, including profiling. The Privacy Act also grants the relatives of a deceased person the ability to exercise the right of erasure and to obtain a restriction on processing upon request, made within five years following the death.

What is the territorial application of the data privacy regime in your jurisdiction?

Hungarian data protection law is applicable if either: (i) The controller's main establishment is located in Hungary or the controller's only place of business within the EU is in Hungary. (ii) The controller's main establishment is not located in Hungary or the controller's only place of business within the EU is not in Hungary, but the controller's or its processor(s)'s data processing operation(s) relate to (a) the offering of goods or services to data subjects located in Hungary, irrespective of whether a payment by the data subject is required; or (b) the monitoring of data subjects' behavior, which occurs in Hungary.

What are the key factors and considerations to adhere to when engaging in the processing of personal data within your jurisdiction?

As a preliminary step, it is recommended to conduct a thorough examination of the relevant data protection legislation prior to initiating any data processing activities. In Hungary, this may involve reviewing the directly applicable GDPR, the Privacy Act, and potentially other sector-specific regulations. Additionally, it is essential to keep a close eye on the decisions the National Authority for Data Protection and Freedom of Information (NAIH) has made concerning data processing activities because the authority gives valuable interpretation of the GDPR's provisions.

One of the most common violations of the GDPR is the lack of transparency, therefore, it is crucial to appropriately inform the data subjects of the processing. Related to this, strict ad-

herence to the documentation requirements set by the GDPR is essential. For example, if the controller states that the legal basis for the processing is in its legitimate interest, it shall be well supported and documented by the controller, because, as a general rule, the controller is responsible for any tasks resulting from data processing. When preparing documentation for data processing it is also crucial to look at the NAIH's possible interpretation and relevant cases. The NAIH has issued a national list of activities, when data protection impact assessments are mandatory, which shall be considered when engaging in the processing of personal data in Hungary.

Furthermore, it is also important to follow sector-specific data processing rules because they may outline additional requirements and stringent regulations for the activities in question. For example, under the GDPR, explicit consent from the data subject is mandatory for automated individual decision-making and processing of special categories of personal data. Meanwhile, in Hungary, as per the Business Advertising Act, explicit consent from recipients of direct marketing is required.

What are the regulations and best practices concerning the retention and deletion of personal data in Hungary?

The GDPR, directly applicable in Hungary, the "storage limitation" principle mandates that personal data cannot be stored for longer than is necessary for the purposes for which the personal data are processed. Controllers must specify the storage period or the criteria for determining retention periods in privacy notices. Additionally, various sector-specific acts in Hungary govern retention periods and deletion requirements. Controllers in these sectors must adhere to these regulations to meet sector-specific data protection standards, which require individual examination.

The NAIH offers valuable non-binding guidance on personal data retention and deletion in Hungary. For instance, when interpreting GDPR regulations, the NAIH emphasized that data controllers must furnish evidence of compliant deletion of personal data. This entails documenting details such as serial numbers and IMEI numbers in the record, enabling clear identification of the medium and the erasure method used. If competent authorities request evidence of personal data erasure, and the controller has documented the erasure as described above, they may share this record as proof of compliance.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

In Hungary, the NAIH enforces data protection and freedom of information regulations.

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in Hungary, and under what conditions?

Under the GDPR, appointing a Data Protection Officer is obligatory in specific scenarios: when processing is conducted by a public authority or body (excluding courts), when activities involve extensive processing of special or criminal personal data, or when there's regular and systematic monitoring of data subjects on a large scale.

Similarly, within the scope of the Privacy Act, designating a Data Protection Officer is mandatory if the controller or processor carries out duties vested by the state or other public duties as specified by law, except for courts. Additionally, the Privacy Act allows for other acts to mandate Data Protection Officer designation for certain controllers and processors, although there are currently no examples of this in Hungarian law.

How should data breaches be handled in your jurisdiction?

In Hungary, two primary legislations govern data breaches. When data processing falls under the Privacy Act, the Privacy Act applies to the breach. Similarly, if data processing falls under the GDPR, the GDPR governs the breach.

Under the GDPR, if a data breach poses a risk to individuals' rights and freedoms, the controller must report it to the supervisory authority, in Hungary to the NAIH, within 72 hours of becoming aware of it. Controllers must document all data breaches, including relevant facts, effects, and remedial actions taken. If a breach is likely to result in high risks to individuals, the controller must promptly inform affected individuals, providing clear information about the breach and necessary measures.

Under the Privacy Act, breaches must be reported to the NAIH without undue delay, but no later than 72 hours after becoming aware of them, unless they pose no risk to individuals' rights. If a breach significantly affects individuals' rights, the controller must promptly notify them, unless the Privacy Act states otherwise.

Both legislations require similar mandatory information to be provided in breach notifications to the NAIH. The Hungarian supervisory authority provides an electronic platform for reporting data breaches, which may be utilized to ensure compliance with relevant legislation in the event of a breach.

What are the potential penalties and fines for non-compliance with data protection regulations in Hungary?

Fine calculation under the GDPR is the responsibility of the NAIH in Hungary, governed by the GDPR, the Privacy Act, and the Sanctions Act. The NAIH, as a supervisory authority, follows the five-step methodology of the European Data Protection Board, which includes the following considerations:

- Identification of the processing operations: Initially, the NAIH identifies the data processing operations to be evaluated and assesses the interrelations between any concurrent infringements, as stipulated in Article 83(3) of the GDPR.
- Starting point determination: Next, the NAIH establishes the starting point for fine calculation based on the classification under Article 83(4)-(6) of the GDPR, the seriousness of the infringement, and the turnover of the undertaking.
- Evaluation of aggravating and mitigating circumstances: In the subsequent stage, the NAIH considers both aggravating and mitigating circumstances related to the behavior of the data controller or processor, past or present, and adjusts the fine accordingly.
- Legal Maximums: The authority then sets the legal maximums for various types of infringements.
- Final Assessment: Finally, the NAIH analyses the calculated fine to ensure it aligns with the principles of effectiveness, dissuasiveness, and proportionality. While adjustments may be made to reflect these principles, it's crucial that the final fine amount remains within the bounds of the legal maximum as outlined by law.

Over recent years, there has been a trend of escalating fines imposed by the NAIH. The pinnacle of this trend unfolded in 2021, when a bank, using an artificial intelligence system without justification, unlawfully analyzed the voices of its customers, which helped track the emotions of its customers via phone customer service. The NAIH imposed a HUF 250 million fine for the personal data breach, which is approximately EUR 630,000.

In a more recent case, the developer entity responsible for the exclusive system used by public schools received a fine of HUF 110 million, approximately EUR 280,000, from the NAIH. This was due to insufficient security measures for the processed personal data within the system, as well as the developers' failure to promptly notify the data controllers, namely the public schools, of the data breach. The NAIH reported that the personal data of over 20,000 individuals was accessible to unauthorized parties.

Are there any noticeable patterns or trends in how enforcement is carried out in Hungary?

In recent years, responding to the challenges brought by digitalization has become increasingly significant. As of January 2022, the NAIH has been authorized to "block" websites – temporarily render them inaccessible – operated by unknown entities engaged in unlawful data processing, causing significant harm to individuals.

Over the past years, the number of data protection authority proceedings, as well as the number and amounts of fines, have been on the rise. In 2022, the NAIH issued its largest fine to date, a HUF 250 million penalty for the unlawful application of artificial intelligence.

Furthermore, the NAIH is initiating more and more procedures, both upon request and ex officio, concerning political campaigns, healthcare documentation, forensic expert activities, and marketing data processing. Instances of camera surveillance have also become increasingly common in recent years.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in Hungary?

The rise of artificial intelligence (AI) presents significant challenges to data protection considerations in Hungary. As of now, there is no specific legislation governing AI in the country, leaving organizations to navigate within the framework of the GDPR, guidance from the European Data Protection Board, and directives from the NAIH.

The NAIH's decision 85-3/2022 addressed some of these challenges, where a bank utilized artificial intelligence to understand and analyze customer moods during phone calls. The decision emphasizes the importance of transparency in such AI applications, especially the need for clear privacy notices and the provision of consent or the right to object. Moreover, legitimate interest as a legal basis was found lacking, highlighting the necessity for proper legal grounds for AI deployment. Additionally, the bank also used artificial intelligence to monitor and evaluate employees through these phone calls. The NAIH emphasizes that such data processing can only be done in a reliable and human-centered manner with very strong guarantees and proper planning. Addressing these challenges, the forthcoming EU Artificial Intelligence Act (AI Act) will directly be applicable to Hungary as well. The AI Act aims to prohibit AI applications that threaten citizens' rights, such as biometric categorization systems and emotion recognition in workplaces and schools. It will also tackle issues like social

scoring and AI manipulation of human behavior.

Similarly, the rapid increase of IoT devices generated a vast amount of new data, leading to emerging data protection risks. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), which came into effect in January 2024, addresses these concerns by outlining roles and responsibilities in IoT data processing. It grants users rights to access, use, and port data generated through IoT devices and establishes rules for data sharing between businesses and public sector bodies. While Hungary has yet to see any data protection cases involving IoT data processing, the Data Act provides a robust framework to safeguard users and promote the EU's data economy.

In recent years, the emergence of blockchain technology has raised data protection concerns in Hungary. Consequently, the NAIH has provided clear guidelines in 2017, which aim to address critical aspects such as the processing of personal data, the applicability of GDPR regulations in terms of territorial and substantive scope, roles during processing, and other related matters. The NAIH has provided insights into blockchain technology's implications for data protection, particularly in its application within transactions involving virtual currencies like Bitcoin. A primary concern lies in the decentralized nature of blockchain, which lacks centralized oversight. The NAIH's clarifications emphasize that when blockchain incorporates personal data, individual users take on the role of data controllers. Consequently, the user adding data to the blockchain gains exclusive control over their stored information within the block, determining its subsequent usage. Moreover, if this control is transferred to another user, the recipient inherits exclusive rights over the data and assumes the role of the data controller. In this case, the legal basis for processing personal data might be the consent of the data subject or the legitimate interest of the user. Furthermore, another concerning matter is whether the blockchain enables the profiling of users. The NAIH states that this question can only be answered after further examination of the specific blockchain in question.

Are there any expected changes in data protection on the horizon in the next 12 months in Hungary?

Considering data protection enforcement trends in Hungary, it's anticipated that the NAIH will provide practical interpretation and guidance on new technologies impacting data protection regulations. With fines increasing for GDPR violations, organizations are recognizing the importance of prioritizing data protection across all operational areas, particularly in light of emerging technologies.

The expected publication of the AI Act by the end of May 2024 is projected to offer comprehensive guidance on AI systems over the next two years. Additionally, the interplay between the Data Governance Act, the GDPR, and applicable Hungarian national laws may be subject to guidance from the NAIH. It's hoped that this legislation will contribute to reducing data breaches resulting from the unlawful use of artificial intelligence, thereby strengthening overall data protection measures.

Expectedly, within the next 12 months, several acts will come into force in Hungary aimed at bolstering the country's digital transformation and enhancing innovation in public administration practices. Notably, Act C of 2021 on the Land Registry and Act CIII of 2023 on the digital state and certain rules for the provision of digital services are among these anticipated legislations.

With these advancements poised to impact individuals' daily lives, new data protection concerns are likely to arise, necessitating reflection in sector-specific legislation. It is anticipated that electronic data processing and automated decision-making, particularly by government bodies concerning individuals, will see a surge in the coming year. Consequently, these emerging innovations will demand specific data processing regulations within the framework of these new legislations. ■

WALLESS

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

LITHUANIA

Guoda Sileikyte
Associate Partner
guoda.sileikyte@walless.com
+370 620 63676

CEE
LEGAL MATTERS

www.ceelegalmatters.com

What are the main data protection-related pieces of legislation and other regulations in Lithuania?

Lithuania adheres to 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 (GDPR). The GDPR is a comprehensive data protection law enacted by the European Union (EU) to ensure the privacy and security of personal data for all EU citizens. As a member state of the EU, Lithuania complies with GDPR requirements, implementing stringent measures to protect individuals' data rights. This includes obtaining explicit consent for data collection (when other data processing legal grounds cannot be applied), ensuring transparency in data usage, and providing mechanisms for individuals to access, rectify, or delete their personal data. Lithuania's commitment to the GDPR reflects its dedication to upholding high standards of data privacy and protection in line with EU regulations.

Additionally, the main national data protection-related legal acts in Lithuania are:

- Law on Legal Protection of Personal Data of the Republic of Lithuania, dated June 30, 2018, No XIII-1426 (Law on Legal Protection of Personal Data);
- Law on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Acts, Execution of Punishments or for the Purposes of National Security or Defense, dated June 30, 2018, No XIII-1435 (Law on Data Protection for Crime Prevention and National Security);
- Code of Administrative Offences of the Republic of Lithuania, dated June 25, 2015, Nr XII-1869 (Code of Administrative Offences);
- Law on Cyber Security of the Republic of Lithuania, dated December 11, 2014, No XII-1428 (Law on Cyber Security);
- Law on Electronic Communications of the Republic of Lithuania, dated April 15, 2004, No IX-2135 (Law on Electronic Communications);
- Orders of the Director of the State Data Protection Inspectorate (SDPI);

Also, it is always useful to check and assess methodological information (e.g., guidelines, recommendations, instructions) adopted and published by the SDPI. Although these guidelines do not constitute legislation and are not legally binding on entities, they provide highly useful practical information. Adherence to these guidelines is strongly recommended when conducting business activities related to personal data in Lithuania.

Lithuania's alignment with the GDPR and its data protection legal framework helps maintain coordinated practices for companies that already operate in other EU countries, streamlining their operations and compliance efforts across different jurisdictions. However, it remains essential for companies to review their policies to ensure they meet specific Lithuanian practices and regulatory nuances, thereby achieving full compliance within the local context.

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, etc., or equivalent)?

In Lithuania, the legislation closely aligns with the GDPR, incorporating key definitions such as data processing, data processor, data controller, data subject, personal data, sensitive personal data, and others, thereby maintaining conformity with established EU standards on data protection and privacy. Since the Law on Legal Protection of Personal Data came into force on July 16, 2018, references to the Law on the Legal Protection of Personal Data of the Republic of Lithuania in Lithuanian laws and regulations are construed as references to the GDPR and, where applicable, the Law on the Legal Protection of Personal Data. For instance, although the Law on the Legal Protection of Personal Data provides several definitions for clarification purposes as they are understood in Lithuania, these definitions do not contradict those stated or otherwise described in the GDPR:

- Direct marketing – any activity the purpose of which is to offer goods or services to persons by post, telephone, or any other direct means and/or to seek their opinion on the goods or services offered;
- Public authorities and bodies – state and municipal authorities and bodies, enterprises and public bodies financed from state or municipal budgets and state monetary funds and authorized to perform public administration or to provide public or administrative services to persons or to perform other public functions in accordance with the procedure laid down by the Law on Public Administration of the Republic of Lithuania.

The Law on Data Protection for Crime Prevention and National Security also indicates several main definitions as they are understood in the scope of national security matters, such as personal data, personal data breach, biometric data, and data processing, e.g.:

- Personal data – any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an iden-

tifier such as a name, a personal identification number, location data, and an online identifier, or to one or more factors specific to their natural, physiological, genetic, mental, economic, cultural or social identity;

- Biometric data – personal data relating to the physical, physiological, or behavioral characteristics of a natural person which, after specific technical processing, allow for the accurate identification or confirmation of that natural person, such as facial images or dactyloscopic data;
- Data processing – any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, sorting, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination with other data, restriction, erasure or destruction.

The analysis of primary definitions outlined in Lithuanian legislation reveals a close alignment with the GDPR as its data protection provisions apply completely. These definitions serve to enhance the understanding and implementation of data protection measures in specific contexts such as crime prevention and national security. Overall, the comprehensive definitions outlined in Lithuanian legislation reflect a commitment to safeguarding personal data and upholding privacy rights in accordance with EU regulations, particularly the GDPR.

This alignment offers significant benefits to entities looking to invest or operate in Lithuania. By ensuring consistency with the GDPR, Lithuania provides a stable and predictable regulatory environment, reducing the complexity and cost of compliance for businesses already familiar with EU standards. This legal coherence fosters trust and confidence among international investors and business partners, assuring them that data protection practices meet the highest European standards. Moreover, businesses operating in Lithuania can leverage this robust data protection framework to enhance their reputation and competitiveness in the global market, knowing that they are operating within a jurisdiction that prioritizes data privacy and security.

Which entities fall under the data privacy regulations in Lithuania?

Entities subject to data privacy regulations in Lithuania encompass a broad spectrum, including but not limited to government agencies, businesses, organizations, public authorities, and individuals who engage in the processing of personal data within the jurisdiction. These regulations apply universally across sectors and industries, ensuring comprehensive protection and compliance with data privacy laws. However, the scope is neither broader, nor narrower than to those entities, to whom the GDPR requirements apply.

In essence, all companies must adhere to data privacy regulations, as there is no company that does not process personal data. Whether handling customer information, employee records (all companies have at least one employee), or business contacts, every organization engages in some form of personal data processing. Compliance with data privacy laws is essential to protect individuals' rights, maintain trust, and avoid legal penalties. Therefore, it is imperative for all businesses to implement robust data protection measures and ensure they are consistently updated in line with current regulations.

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

As mentioned, Lithuania falls under the jurisdiction of the GDPR, meaning that its data protection regulations are fully applicable. Adherence to the data processing principles detailed in Article 5 of the GDPR, along with the clear and transparent communication of information to individuals regarding the processing of their personal data as stipulated in Articles 13 and 14, are essential aspects to consider when engaging in data processing activities in Lithuania.

Additionally, the Law on the Legal Protection of Personal Data outlines several specific features of the processing of personal data, which may slightly differ from other jurisdictions in the EU, e.g.:

- Usage of personal identification number. It is prohibited to make the personal code public and to process it for direct marketing purposes.
- Data relating to criminal convictions and offenses. There is a general prohibition on processing the personal data of a candidate applying for a position or performing work functions and an employee relating to criminal convictions and offenses, except in cases where these personal data are necessary to check whether a person meets the requirements set out in laws and implementing legislation to perform duties or work functions.
- Collection of personal data from former/current employees. The controller may collect personal data relating to the qualifications, professional abilities, and personal qualities of a candidate applying for a post or job function from a former employer, after having informed the candidate. However, from a current employer such personal data be collected only with the consent of the candidate.
- Monitoring of employees. When processing personal data linked to monitoring employees' behavior, location, or movement, these employees must be informed about such processing in writing or in another means that establishes

the fact of notice about such processing.

- Children's personal data. For the purpose of obtaining consent for information society services, the child must be at least 14 years old.

What rights do data subjects have under the data protection regulations in Lithuania?

The rights afforded to data subjects under data protection regulations in Lithuania closely mirror those outlined in Section III of the GDPR. These rights are supposed to grant data subjects significant control over their personal data, ensuring its protection and privacy.

- Right to access – data subjects have the right to obtain confirmation from data controllers as to whether or not personal data concerning them is being processed, and if so, access to that personal data and certain related information.
- Right to rectification – data subjects have the right to request the rectification of inaccurate personal data concerning them. They also have the right to have incomplete personal data completed.
- Right to erasure (right to be forgotten) – data subjects have the right to request the erasure of personal data concerning them without undue delay under certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected or when the data subject withdraws consent.
- Right to restriction of processing – data subjects have the right to request the restriction of processing of their personal data under certain circumstances, such as when the accuracy of the personal data is contested by the data subject.
- Right to data portability – data subjects have the right to receive the personal data concerning them, which they have provided to a data controller, in a structured, commonly used, and machine-readable format, and have the right to transmit that data to another controller without hindrance.
- Right to object to processing – data subjects have the right to object, on grounds relating to their particular situation, at any time to processing personal data concerning them, including profiling based on those provisions.
- Right to withdraw consent – where processing is based on consent, data subjects have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- Right to lodge a complaint – data subjects have the right to lodge a complaint with the SDPI if they consider that the processing of personal data infringes the GDPR.

The SDPI has issued valuable methodological information for data subjects, what rights they have related to their personal data processing, and how they can exercise these rights (e.g., Guidance for Employees of the Protection of Personal Data in the Context of the Employment Relationship (2023), Personal Data Protection Guidelines for Data Subjects (2019), Personal Data Guidelines for Youth (2019), Personal Data Protection Guidelines for the Elderly (2019), etc.).

What is the territorial application of the data privacy regime in your jurisdiction?

The territorial scope of the data privacy regime in Lithuania aligns with the GDPR. It extends not only to organizations physically established within Lithuania but also to those outside its borders if they process the personal data of individuals within Lithuania in connection with their business scope, e.g., offering goods or services. This means that regardless of their location, entities processing the personal data of individuals within Lithuania must adhere to Lithuanian data protection laws, ensuring compliance with the GDPR and safeguarding the rights of individuals irrespective of geographical boundaries.

What are the key factors and considerations to adhere to when engaging in the processing of personal data within your jurisdiction?

The implementation of data processing principles delineated in Article 5 of the GDPR, alongside transparent disclosure of information to data subjects regarding personal data processing, as articulated in Articles 13 and 14 of the GDPR, are pivotal factors and considerations governing data processing engagement.

Furthermore, the Law on Legal Protection of Personal Data establishes specific standards, which may exhibit minor discrepancies from those in other EU countries. Moreover, Lithuania persists in encountering reports of data breaches; hence, due attention must be accorded to the adoption of organizational and technical data security measures.

What are the regulations and best practices concerning the retention and deletion of personal data in Lithuania?

In Lithuania, regulations and best practices concerning the retention and deletion of personal data are primarily governed by the GDPR and the national data protection laws that complement it. The SDPI has also issued valuable methodological information for small and medium-sized businesses, as well as comprehensive Guidelines for Data Controllers and Data Processors under the Security Measures for Personal Data Pro-

cessed and Risk Assessment, dated June 18, 2020. These guidelines include various recommendations for data controllers and data processors concerning data protection and data security, specifying the requirements they must fulfill to comply with the GDPR and applicable data security standards, including those related to the retention and deletion of personal data.

Here are some key aspects that data controllers and (or) data processors after verifying their risk assessment as indicated in the previously mentioned guidelines, should take into consideration, together with those stipulated in the GDPR, when conducting business in Lithuania:

- Before any data storage medium is removed, all data on it must be destroyed using dedicated software that supports reliable data destruction algorithms. If this is not possible (e.g., DVD media), the physical destruction of the data medium without the possibility of recovery must be carried out a physical destruction of the data medium;
- paper and portable data media (e.g., DVD media) on which personal data has been stored, must be destroyed with dedicated shredders or other mechanical means;
- before removing media, multiple passes of software-based overwriting must be performed for all media to be removed;
- if third-party services are used for secure data destruction and disposal of data media or paper documents, an appropriate service agreement must be concluded and records destroyed must be logged;
- after data deletion, additional measures should be taken, for example, the removal of unwanted magnetic information (demagnetization) may be performed;
- if a third party handles secure destruction of records, it should ideally be done on the controller and/or processor's premises to prevent data transfer. If not feasible, it can be done elsewhere under the controller's supervision.

The SDPI has issued several decisions infringement, inter alia, related to the retention period, e.g.:

- On April 20, 2023, the SDPI fined a company EUR 20,000. The company had suffered a data breach in which the personal data of 50,000 data subjects was compromised. During its investigation, the SDPI found that the company had failed to implement appropriate technical and organizational measures to protect personal data. These included the lack of adequate access controls and authentication of IT system administrators in the controller's information systems. Also, the SDPI found that the company failed to set an appropriate retention period for personal data.
- On January 24, 2023, the SDPI fined a company EUR 8,000. The controller failed to properly fulfill the data subject's right to access their personal data processed by the company. The controller partially provided information about the processing of the data subject's personal data, but the data subject was not given the opportunity to verify the legal basis for the processing of their personal data, the specific data being processed, the purposes of the processing, the retention period, etc.

These decisions underscore the importance of implementing robust data protection measures, setting appropriate data retention periods, and ensuring transparency with data subjects regarding their personal data. Companies can use these examples to review and improve their own data protection practices to avoid similar infractions and penalties.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

Lithuania is unique in its approach to data protection, featuring two supervisory authorities responsible for enforcing data privacy regulation: the State Data Protection Inspectorate (SDPI) and the Office of the Inspector of Journalists' Ethics (OIJE).

The SDPI serves as the primary regulatory authority, overseeing compliance with data protection laws, including the GDPR and national legislation. Its duties encompass providing guidance to organizations, addressing complaints from data subjects, conducting investigations into data protection breaches, and imposing sanctions for non-compliance. The SDPI's work is essential in safeguarding the rights and freedoms of individuals concerning the processing of their personal data in Lithuania.

Complementing the SDPI, the OIJE focuses on ensuring adherence to ethical standards in journalism. It oversees the conduct of journalists and media organizations to maintain professional ethics, accuracy, and integrity in reporting. The OIJE is responsible for overseeing the GDPR when personal data are processed for journalistic purposes or for purposes of academic, artistic, or literary expression. This includes monitoring how personal information is shared on social media and through mass media outlets such as television, radio, podcasts, newspapers, and websites. Data subjects who believe their rights have been violated in these contexts can approach the OIJE to initiate an investigation or handle a complaint.

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in Lithuania, and under what conditions?

In Lithuania, there are no disparate regulations governing the appointment of a Data Protection Officer (DPO) across different organizations or sectors. The requirement for appointing a DPO in Lithuania aligns with the provisions stipulated

in the GDPR. The GDPR delineates the criteria determining when a DPO must be appointed, and these criteria uniformly apply across all EU member states, including Lithuania. Consequently, the conditions mandating organizations to designate a DPO in Lithuania remain in harmony with the requirements set forth in the GDPR. This uniformity aims to ensure consistent levels of data protection throughout the EU and to facilitate the seamless implementation and enforcement of data protection laws across member states.

In essence, according to the GDPR, organizations must appoint a DPO in the following circumstances:

- public authorities and bodies (if the processing is carried out by a public authority or body, except for courts acting in their judicial capacity);
- regular and systematic monitoring of data subjects on a large scale: When the core activities of the organization involve regular and systematic monitoring of data subjects on a large scale. This may include online behavior tracking, profiling for marketing purposes, or monitoring employee activities;
- large-scale processing of special categories of data or data relating to criminal convictions and offenses. When the organization's core activities consist of large-scale processing of special categories of data (sensitive data) or data relating to criminal convictions and offenses it shall appoint a DPO.

The appointment of a DPO is intended to ensure compliance with data protection regulations and to act as a point of contact for data subjects and supervisory authorities.

How should data breaches be handled in your jurisdiction?

In Lithuania, the handling of data breaches must adhere to the stringent regulations set forth in the GDPR as well as relevant national data protection legislation. These regulations establish clear protocols for organizations to follow in the event of a data breach, emphasizing the importance of prompt detection, thorough investigation, and timely notification of affected individuals and supervisory authorities. Furthermore, the SDPI offers valuable guidance through its Recommendation on Procedures for Detecting, Investigating, Reporting, and Documenting Personal Data Breaches, issued on July 2, 2018. This recommendation outlines detailed procedures for managing data breaches, including steps for assessing the severity of the breach, documenting findings, and implementing corrective measures to prevent future incidents. The SDPI has also established the means how the report should be provided to the SDPI:

- by filling in the e-service form on the e-Government Gateway;
- by using the e-delivery system;
- sending documents signed by e-signatures to ada@ada.lt;
- presentation of the document by registered mail or on-the-spot delivery at the premises of the SDPI.

Effective handling of data breaches in Lithuania requires organizations to adopt a proactive and comprehensive approach to data security. This entails not only responding swiftly to breaches when they occur but also implementing robust preventive measures to minimize the risk of breaches in the first place. By closely following the guidelines established by the GDPR, national legislation, and the SDPI, organizations can ensure compliance with legal requirements while also safeguarding the rights and privacy of individuals affected by data breaches. Additionally, maintaining transparency and open communication throughout the breach response process is essential for building trust with data subjects and regulatory authorities, reinforcing Lithuania's commitment to upholding high standards of data protection and security.

What are the potential penalties and fines for non-compliance with data protection regulations in Lithuania?

Based on the GDPR, fines for data protection violations may amount to EUR 20 million or up to 4% of the undertaking's total worldwide annual turnover in the previous financial year, whichever is higher. However, the two largest fines imposed so far in Lithuania have been EUR 110,000 and EUR 61,500.

Penalties for non-compliance with the GDPR, and other data protection regulations in Lithuania are relatively lower compared to some other EU member states. While GDPR violations can still result in fines as defined in the GDPR, the amounts tend to be less severe in Lithuania than in countries with stricter enforcement. However, it's essential for businesses and organizations to prioritize GDPR compliance to avoid potential penalties and maintain trust with customers. Compliance not only protects individuals' data rights but also helps build a positive reputation in the increasingly data-conscious market landscape.

Top 5 penalties and fines for non-compliance with data protection regulations in Lithuania imposed by the SDPI:

- On November 29, 2021, the SDPI imposed an administrative fine of EUR 110,000 for the publication of the company's personal data of its customers – personal data of 110,302 users of the company's service was disclosed and made public. It was decided that the company failed to ensure adequate management and control of the security of personal data and failed to assess, manage, and

control the risk of loss of confidentiality of personal data contained in the database file.

- On May 16, 2019, during an inspection, the SDPI discovered that the controller processed excessive data beyond the required scope. Additionally, it was found that payment data became publicly accessible online due to insufficient technical and organizational safeguards in July 2018, affecting 9,000 payments across 12 banks from various countries. The SDPI determined that a data breach notification under Article 33 of the GDPR was necessary, but the controller failed to report it. Consequently, a fine of EUR 61,500 was imposed.
- On June 21, 2021, a sports club received a fine of EUR 20,000 for requiring customers to scan their fingerprints to access gym services, without offering alternative identification methods. Moreover, the data controller was found to lack operational records and unlawfully processed employees' fingerprints without a legal basis or data protection impact assessment.
- On April 20, 2023, the SDPI imposed a fine of EUR 20,000 in relation to a data breach. The company had suffered a data breach in which the personal data of 50,000 data subjects was compromised. During its investigation, the SDPI found that the company had failed to implement appropriate technical and organizational measures to protect personal data. These included the lack of adequate access controls and authentication of IT system administrators in the controller's information systems. Also, it was found that the company failed to set an appropriate retention period for personal data.
- In February 2021, a fine of EUR 15,000 was imposed on the Centre of Registers, which infringed the GDPR clauses requiring it to ensure the integrity, availability, and resilience of its systems and services for the permanent processing of data and to be able to restore the conditions for, and the availability of, the access to personal data in the event of a physical or technical incident within the time limits set by law.

Worth mentioning that where the data controllers perform direct marketing activities with legal entities (B2B) without having a proper legal basis, according to the current practice of the SDPI, the violations of this issue may result in consequences rather under the Law on Electronic Communications than the GDPR. According to Article 83 of the Code of Administrative Offences, violation of the processing of personal data and the protection of privacy under the Law on Electronic Communications shall be punishable by a fine of between EUR 150 and EUR 580 for individuals and between EUR 300 and EUR 1,150 for CEOs or other responsible persons of legal entities. Repeatable offenses may result in a fine for individuals from EUR 550 to EUR 1,200, and, for CEOs or other responsible persons of legal entities, from EUR 1,100 to EUR 3,000. Since it is a current practice, however, there are no guarantees that this practice may not change.

From prevailing trends, it is evident that the SDPI is adopting a stance of providing guidance and leadership rather than solely focusing on punitive measures when it comes to GDPR infringements. While maximum fines for violations have not been frequently imposed, there is a noticeable shift towards a more responsible approach to data protection. This shift is reflected in the gradual increase in fines over time. It suggests that the SDPI is prioritizing proactive measures such as guidance, education, and support to help organizations improve their data protection practices. This approach aims to foster a culture of compliance and accountability, encouraging organizations to prioritize data protection while mitigating the risks of future breaches.

Are there any noticeable patterns or trends in how enforcement is carried out in Lithuania?

The SDPI typically announces its inspection plan in the first quarter of each year. Due to limited resources, such yearly inspection plans usually target no more than 50 entities. The plans are primarily based on the number of complaints received in previous years or are linked to corrective measures previously imposed by the SDPI. Additionally, while the nationally approved first-year good practice of business supervision does not encompass data protection inspections, the SDPI generally excludes businesses operating for less than a year from its yearly inspection schedule.

Despite conducting relatively few scheduled inspections, the SDPI is obligated to investigate every complaint received and review every notification of a data breach, particularly concerning data leaks. The SDPI facilitates amicable settlement procedures for data subject complaint investigations, serving as a mediator between the data subject and data controller to facilitate a mutually agreeable resolution.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in Lithuania?

As an EU member state, Lithuania is now tasked with implementing the recently adopted Artificial Intelligence Act (AI Act). The AI Act is a key element of the EU's policy to foster the development and uptake across the single market of safe and lawful AI that respects fundamental rights. As explained by the Commission, the AI Act also seeks to address the use of general-purpose AI (GPAI) models. GPAI models not posing systemic risks will be subject to some limited requirements, for example with regard to transparency, but those with

systemic risks will have to comply with stricter rules. This new regulation will apply two years after its entry into force, with some exceptions for specific provisions. As to Lithuania, the AI Act will serve as the basis for any forthcoming national regulatory measures aimed at advancing the development of artificial intelligence within Lithuania.

Additionally, the EU Data Act, which entered into force on January 11, 2024, enables a fair distribution of the value of data by establishing clear and fair rules for accessing and using data within the European data economy, a necessity heightened by the growing prevalence of the IoT. Thanks to this regulation, connected products will have to be designed and manufactured in a way that empowers users (businesses or consumers) to easily and securely access, use and share the generated data.

These EU regulations will be the background for related regulatory discussions in Lithuania. On one hand, the Lithuanian regulators are aware that over-regulation of emerging technologies may limit the use of innovation in the country and lead to a loss of competitive advantage. On the other hand, an overly liberal approach can lead to particularly severe consequences when it is difficult or too late to regulate measures that seriously violate human rights, including the right to privacy and personal data protection.

Moreover, Lithuanian highlights the necessity for high-quality, readily available data for emerging technologies and their research. As pointed out in the Lithuanian Artificial Intelligence Strategy, the AI system's precision increases with the quality of the data set. Data inaccuracies and flaws can result in biased AI models, which can have unethical or discriminating effects.

This is why one of the important goals of Lithuania is to ensure that data used for emerging technologies complies with the European Union's FAIR ("findable, accessible, interoperable, and reusable") Data Management principles.

Are there any expected changes in data protection on the horizon in the next 12 months in Lithuania?

The draft Amending Law on Legal Protection of Personal Data is being debated in the Lithuanian Parliament (Seimas). Changes are expected in two areas:

- Processing of personal data relating to criminal convictions and offenses. According to businesses' requests to have the possibility to process necessary personal data relating to criminal convictions and offenses of candidates applying for a position or performing work functions and an employee, amendments have been introduced establishing conditions that such personal data may be processed according to the legitimate interests of the employers, if:
  - a written balance test is performed, and exact roles are identified,
  - approved roles are publicized on the employer's website,
  - data relating to criminal convictions and crimes are submitted by the candidate applying for a post or executing work functions, or the employee themselves;
- Procedure for publishing SDPI decisions. It is intended to publish such decisions publicly on SDPI's website no later than five working days from the date of adoption. It is worth mentioning, that when the decision relates to identified compliance with relevant regulations, the name of the data controller (processor) shall not be published. Decisions of the SDPI shall be published for a period of 10 years. ■

Linklaters

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

POLAND

Szymon Sieniewicz
Head of TMT/IP
szymon.sieniewicz@linklaters.com
+48 22 526 5042

Malgorzata Czubernat
Junior Associate
malgorzata.czubernat@linklaters.com
+48 22 528 6156

CEE
LEGAL MATTERS

www.ceelegalmatters.com

What are the main data protection-related pieces of legislation and other regulations in Poland?

The primary legal framework governing data protection in Poland is established by 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 (General Data Protection Regulation) (GDPR). The GDPR became directly applicable in all Member States of the EU on May 25, 2018. It constitutes the cornerstone of privacy regulations in Poland.

The GDPR allows the Member States in more than 50 areas to introduce domestic data protection laws to supplement the GDPR. To ensure the application of the GDPR in Poland, the Polish Parliament adopted several national acts, specifying many different aspects of data protection. Such acts include, inter alia, the Act of 10 May 2018 on Personal Data Protection, as amended (Data Protection Act) and the Act of 21 February 2019, amending certain laws to ensure the implementation of the GDPR in Poland (2019 GDPR Implementation Act). The 2019 GDPR Implementation Act amended Polish sectoral laws, such as labor, consumer protection, insurance, banking, and telecommunication laws. In total, it amended 162 different acts.

Consequently, Polish law provides several specificities on top of the GDPR requirements, concerning, inter alia, the processing of employees' data, specific principles for conducting marketing activities, the obligation to translate (or implement) some of the privacy documents into the Polish language (i.e. privacy notices, especially directed at consumers, employees, and job applicants), the obligation to notify the appointment of a data protection officer (DPO) to the Polish data protection authority (Polish DPA) and specific retention periods. Polish law also introduces additional (criminal) penalties for unlawful personal data processing.

Moreover, the Polish DPA has established and made public a list of processing operations that are subject to the requirement for a data protection impact assessment (DPIA List).

Please find below a list of the most relevant local regulations regarding various aspects of data protection in Poland:

- Data Protection Act;
- 2019 GDPR Implementation Act;
- Act of 26 June 1974 Labor Code;
- Act of 4 March 1994 on the Company Social Benefits Fund;
- Act of 18 July 2002 on the Provision of Services by way of Electronic Means;
- Act of 16 July 2004 Telecommunication Law;
- Act of 6 June 1997 Criminal Code;
- Act of 29 August 1997 Banking Law;
- Act of 1 March 2018 on Counteracting Money Laundering and Financing Terrorism;
- Act of 11 September 2015 on Insurance and Reinsurance Activities;
- Communication of the Polish DPA of 17 June 2019 on the list of the processing operations which are subject to the requirement for a data protection impact assessment;
- Various national acts specifying retention periods, such as Act of 29 August 1997 Tax Ordinance.

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, etc., or equivalent)?

Primary definitions are set out directly in the GDPR.

Personal data

Under the GDPR, personal data is defined as any information relating to an identified or identifiable natural person.

This is a broad term and includes a wide range of information. The GDPR expressly states it includes online identifiers such as cookies.

Data processing

Under the GDPR, processing means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data processor

Under the GDPR, processor means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

Data controller

Under the GDPR, controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State

law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject

Under the GDPR, data subject means an identified or identifiable natural person. 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.

Special category of personal data

Special category personal data under the GDPR includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health, and natural person's sex life and sexual orientation.

Consent

Under the GDPR, consent means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Which entities fall under the data privacy regulations in Poland?

Territorial scope of application of the GDPR

The GDPR applies to the processing of personal data in the context of the establishment of a controller or processor in the EU.

It also contains express extra-territorial provisions and will apply to controllers or processors based outside the EU that: (i) offer goods or services to individuals in the EU; or (ii) monitor individuals within the EU. Controllers and processors caught by these provisions will need to appoint a representative in the EU, subject to certain limited exemptions.

The European Data Protection Board has issued Guidelines on the territorial scope of the GDPR (3/2018).

Concepts of controllers and processors

The GDPR contains the concept of a controller, who determines the purpose and means of processing, and a processor, who just processes personal data on behalf of the controller.

The European Data Protection Board has issued Guidelines on the concepts of controller and processor in the GDPR (7/2020).

Both controllers and processors are subject to the rules in the GDPR, but the obligations placed on processors are more limited.

Manual and electronic records

The GDPR applies to both electronic records and structured hard-copy records.

National derogations

The GDPR does not apply to law enforcement activities which are instead subject to the Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive). The GDPR also does not apply to areas of law that are outside the scope of Union law, such as national security, and does not apply to purely personal or household activity.

Furthermore, the Data Protection Act excludes the application of the GDPR in several fields. Fully exempt are the activities of special forces as well as the processing of personal data by entities of the public finance sector if such processing is necessary for the execution of tasks that are aimed at ensuring national security.

The GDPR is also partially excluded from application in the scope of editing, preparing, or publishing press materials, and in the scope of literary or artistic activities (e.g., there is an exemption to the obligation to provide privacy notices).

Moreover, data controllers conducting public services are exempted from complying with certain obligations to provide privacy notices and respond to subject access requests where it is related to the performance of public duties, and exercising these provisions may breach the protection of classified information or prevent or significantly obstruct the proper execution of a public service.

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

Specific sectors

Specific sectors have distinct regulatory regimes within Polish jurisdiction. Sectoral laws (e.g., for banks, telecommunications operators, and healthcare service providers) impose additional

security obligations on data controllers. They include, inter alia, the following:

- Healthcare sector:
  - Medical Activities Act of 15 April 2011;
  - Act on Patients' Rights and the Commissioner for Patients' Rights of 6 November 2008;
  - Act on the Healthcare Information System of 28 April 2011; and
  - Act on Clinical Trials of Medicinal Products for Human Use of 9 March 2023;
- Telecommunication sector: Telecommunication Law of 16 July 2004;
- Energy sector: Energy Law Act of 10 April 1997;
- Financial sector: Payment Services Act of 19 August 2011; Act on Counteracting Money Laundering and Terrorist Financing of 1 March 2018; Act on the Principles of Obtaining Information About the Criminal Record of Persons Applying for Employment and Persons Employed in Entities of the Financial Sector of 12 April 2018; Financial Instruments Trading Act of 29 July 2005;
- Insurance sector: Insurance and Reinsurance Activity Act of 11 September 2015;
- Banking sector: Banking Act of 29 August 1997.

Employees' data

Act of 26 June 1974 Labor Code (Labor Code) includes a list of categories of personal data of employees and job applicants that can be processed by employers or potential employers. The consent of an employee or a job applicant may constitute a valid legal basis for personal data processing in some cases and would fall within the scope provided for in the Labor Code.

The Labor Code also includes specific provisions for employee monitoring. It is strictly prohibited to monitor the premises entrusted to trade union organizations. It is also prohibited to monitor sanitary rooms, cloakrooms, canteens, and smoking rooms unless the monitoring in these rooms is necessary to ensure the safety of employees, the security of the property, the production control, or to keep the confidentiality of the information, disclosure of which could expose the employer to harm.

E-mail monitoring and other forms of employee monitoring are also allowed, but specific rules set out in the Labor Code must be followed.

Further, the recent amendments to the Labor Code introduced a legal basis for conducting sobriety tests of employees and provided rules for the processing of sensitive personal data in the form of information on the results of sobriety tests (data concerning health).

The Labor Code also includes specific provisions regarding remote working (the employer is obliged to define procedures for the protection of personal data by employees working remotely and to provide instruction and training in this regard, where necessary).

The protection of employees' personal data is also specified by other Polish laws. For example, the processing of employees' personal data for the purposes of running the company social benefits fund is regulated by Act of 4 March 1994 on the Company Social Benefits Fund (Company Social Benefits Fund Act). Among other things, the Company Social Benefits Fund Act imposes conditions on allowing only persons with written authorization to process certain categories of personal data and an obligation to review and erase personal data collected for the purposes of running the company social benefits fund at least once per calendar year, if processing them is no longer necessary.

In addition, legislation concerning processing information about criminal offenses in the financial sector has been in force since June 2018. It gives employers from the financial and banking sector an explicit right to check criminal records with respect to certain employees and job applicants, including employees employed in, and job applicants applying for, a position requiring access to confidential data or making high-risk decisions. It includes a broad list of financial sector entities that fall within the scope of its application and sets out the specific requirements for processing information about criminal offenses of job applicants and employees.

What rights do data subjects have under the data protection regulations in Poland?

Data subjects in Poland generally have the same rights as those under the GDPR.

Right to access information

Data subjects have a right to access copies of their personal data by making a written request to the controller. The initial request is free, though a charge can be made for subsequent requests. Controllers can refuse the request if it is manifestly unfounded or excessive. The right to obtain a copy of personal data should not adversely affect the rights and freedoms of others. The response must be provided within a month, though this can be extended by two months if the request is complex.

Right to data portability

Data subjects also have a right to data portability where the condition for processing personal data is consent or the performance of a contract. It entitles individuals to obtain any personal data they have "provided" to the controller in a machine-readable format. Individuals can also ask for the data to be transferred directly from one controller to another. There is no right to charge fees for this service.

Right to be forgotten

A data subject can ask that their data be deleted in certain circumstances. However, those circumstances are relatively limited, for example where the processing is based on consent, that consent is withdrawn and there are no other grounds for processing. Even where the right does arise, there are a range of exemptions, for example where there is a legal obligation to retain the data.

Objection to direct marketing

A data subject can object to their personal data being processed for direct marketing purposes at any time. This includes profiling to the extent related to direct marketing.

Other rights

The GDPR contains a range of other rights, including the right to have inaccurate data rectified. There is also a right to object to processing being carried out in the performance of a public task or under the "legitimate interests" condition.

Finally, there are controls on making decisions based solely on automated decision-making that produce legal effects or similarly significantly affect the data subject.

What is the territorial application of the data privacy regime in your jurisdiction?

In Poland, the territorial application of the data privacy regime is primarily governed by the GDPR, which is directly applicable in all EU Member States, including Poland. The GDPR has an extraterritorial scope and applies not only to entities based within the EU but also to organizations outside the EU if they process the personal data of individuals who are in the EU in connection with:

- the offering of goods or services to such individuals in the EU, regardless of whether a payment is required;
- the monitoring of their behavior, as far as their behavior takes place within the EU.

In summary, the territorial application of the data privacy regime in Poland covers entities operating within Poland, Polish entities processing data outside of Poland, and non-Polish entities processing personal data of individuals located in Poland in the context of offering goods, services, or monitoring their behavior.

What are the key factors and considerations to adhere to when engaging in the processing of personal data within your jurisdiction?

When planning processing activities in Poland, it is essential to consider several key factors. These include regulations concerning employees' personal data, the need to maintain some documentation in the Polish language, and the requirement to inform the Polish DPA of an appointment of a DPO. Furthermore, the appointment of a DPO carries additional responsibilities. Controllers are also obliged to conduct the data protection impact assessment (DPIA) under circumstances specified by the Polish DPA. Additionally, compliance with specific data retention periods mandated by Polish law, and obligations related to marketing activities, which are detailed below, ought to be factored in.

Use of Polish language in data protection documentation

The obligation to provide information to data subjects in Polish results from the Act of 7 October 1999 on the Polish Language, according to which any communication with the consumers must be in Polish. This means that privacy notices directed at consumers in Poland must be prepared or translated into Polish. The same applies to employment relationships. Moreover, according to the Transparency Guidelines under Regulation 2016/679 issued by the Article 29 Working Party, if the controller directs information to data subjects who speak another language or languages, a translation in that language or those languages should be provided by the controller.

Moreover, under the Data Protection Act, the Polish DPA may request to translate GDPR documentation into Polish at the expense of the party in the course of the proceedings. It is therefore recommendable for Polish entities to prepare and implement internal privacy documentation in the Polish language.

Obligation to notify the appointment of a DPO to the Polish DPA

Under Article 10 of the Data Protection Act, an entity that appoints a DPO shall notify the Polish DPA of the appointment within 14 days of the appointment. The Data Protection Act specifies what information must be included in such notification.

Additional obligations regarding DPO appointment

Under the Data Protection Act, an entity that appoints a DPO shall make the DPO's name, surname, and e-mail address or telephone number available on its website immediately after such appointment or, if it does not maintain its own website, in a manner publicly accessible at the place of business.

DPIA List

The Polish DPA has published the DPIA List to specify what processing activities require conducting a DPIA. For example, in Poland, using systems for monitoring employees' working time and the flow of information in the tools they use (e-mail, Internet) or customer profiling systems to identify purchase preferences requires conducting a DPIA. The DPIA List should be taken into account while carrying out a risk assessment for Polish entities.

Marketing Activities

In order to legally process personal data as part of marketing activities carried out in Poland, in addition to the GDPR, the provisions of the following national laws must be taken into account: (i) Act of 18 July 2002 on the Provision of Services by way of Electronic Means (ECA) and (ii) Act of 16 July 2004 Telecommunication Law (TL). Moreover, over the years, there have been numerous interpretations and decisions published by competent authorities (Polish DPA, the President of the Office of Electronic Communications, and the President of the Office of Competition and Consumer Protection), which have clarified the requirements for individual consents collected for marketing purposes.

Article 172(1) of the TL and Articles 10(1) and (2) of the ECA, require consents for, respectively:

- the use of telecommunications terminal equipment and automatic calling systems for direct marketing purposes; and
- the sending of commercial information addressed to a designated recipient who is a natural person by means of electronic communication.

With regard to the criteria that these consents should meet, the ECA and the TL refer to data protection legislation. This means that the consents collected from Poland should satisfy the requirements set out in the GDPR. However, in Poland, there have been several decisions clarifying what the various supervisory authorities consider to be "valid consent." For example, it follows that the different channels of communication used for direct marketing purposes (SMS, e-mail, etc.) should be specified, and data subjects should be allowed to consent to each of the channels of communication separately.

Moreover, the use of cookies is subject to the conditions set out in Article 173 of the TL. According to this provision, the use of cookies is allowed provided that:

- the user is informed in advance, in an unambiguous, easy, and understandable manner, of the purpose of storing and accessing the information collected through cookies and of the possibility of changing the cookie settings via the software installed on the user's terminal equipment;
- the user consents to the use of cookies; and
- the installation or use of cookies will not result in any configuration changes on the user's terminal equipment or on the software installed on that equipment.

Although under Article 173(2) of the TL consent for cookies can be given via browser settings, the Polish DPA has taken the view that such consent should be actively obtained by the controller (therefore, reliance on the user's browser settings is not a recommended solution).

The ECA also specifies in Article 18 the categories of personal data that may be processed in connection with the provision of electronic services, including for the conclusion of contracts and for the purposes of advertising, market research, and research into customer behavior and preferences to improve the quality of the service provided by the service provider, and introduces consent requirements for certain of these processing activities.

Specific retention periods

It is also necessary to consider retention periods resulting from various Polish laws, which will be further described below.

What are the regulations and best practices concerning the retention and deletion of personal data in Poland?

There are specific retention periods resulting from numerous Polish laws. The most relevant retention periods result from laws regarding personal data collected in the context of employment/HR, taxes, accounting, concluding contracts, court proceedings, etc. Retention periods usually result from specific Polish laws, therefore it is not possible to implement a group data retention policy without adjusting it to Polish law requirements first. Determining all relevant retention periods requires a case-by-case analysis including mapping and examining processing activities. Organizations should document their data retention and deletion policies, clearly stating the criteria for determining retention periods and the procedures for data deletion or anonymization. When data is no longer needed, it should be securely deleted or anonymized so that it can no longer be associated with an individual.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

The Data Protection Act appointed a new supervisory authority in Poland, namely the President of the Office of Personal Data Protection. This Office replaced the Inspector General for Personal Data Protection which office ceased to exist as of May 25, 2018.

The President of the Office of Personal Data Protection (Office of Personal Data Protection)
ul. Stawki 2
00-193 Warsaw
https://uodo.gov.pl/

The President of the Office of Personal Data Protection represents Poland on the European Data Protection Board.

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in Poland, and under what conditions?

The conditions for the necessity of appointing a DPO in Poland derive from Article 37 of the GDPR. Both controllers and processors must appoint a data protection officer if: (i) they are a public authority; (ii) their core activities consist of regular and systematic monitoring of data subjects on a large scale; or (iii) their core activities consist of processing special category personal data on a large scale (including processing information about criminal offenses).

DPOs must also be appointed where required by national law. However, Poland has not made such an appointment mandatory in the private sector in any additional circumstances.

How should data breaches be handled in your jurisdiction?

A personal data breach must be notified to the relevant supervisory authority unless it is unlikely to result in a risk to data subjects. The notification must, where feasible, be made within 72 hours. If the personal data breach is a high risk for data subjects, those data subjects must also be notified.

Specific laws on data breach notifications apply to the electronic communications sector under the national laws implementing the Privacy and Electronic Communications Directive (ePrivacy Directive) and to operators of essential services and digital service providers under national laws implementing the Network and Information Systems (NIS) Directive. The regulatory landscape in this regard is set to evolve soon, with the Polish Parliament actively working on legislation to implement the NIS2 Directive. This forthcoming legislation will broaden the scope of responsibilities, introducing enhanced notification requirements for a wider range of organizations.

Pursuant to the Data Protection Act, the President of the Office of Personal Data Protection may introduce an online system enabling controllers to report personal data breaches. The President of the Office of Personal Data Protection has created such a system that enables notification of personal data breaches in electronic form.

What are the potential penalties and fines for non-compliance with data protection regulations in Poland?

Administrative Fines

The GDPR is intended to make data protection a boardroom issue. It introduces an antitrust-type sanction regime with fines of up to 4% of annual worldwide turnover or EUR 20 million, whichever is greater. These fines apply to breaches of many of the provisions of the GDPR, including failure to comply with the six general data quality principles or carrying out processing without satisfying a condition for processing personal data.

A limited number of breaches fall into a lower tier and so are subject to fines of up to 2% of annual worldwide turnover or EUR 10 million, whichever is greater. Failing to notify a personal data breach or failing to put an adequate contract in place with a processor falls into this lower tier.

Fines can only be imposed where there is an intentional or negligent infringement of the GDPR, see CJEU judgment in the Deutsche Wohnen case (C-807/21).

The Data Protection Act lowers the level of these administrative fines for public authorities. The fines for public authorities cannot exceed PLN 100,000 (approximately EUR 23,000).

The Data Protection Act also introduces criminal fines that can be imposed on an individual as a result of a criminal conviction for criminal offenses related to data protection, such as unlawful data processing or hindering inspection proceedings. Their value is determined by the Criminal Code.

Criminal sanctions

The Data Protection Act also provides that persons who process personal data unlawfully or without authorization face a criminal fine, restriction of personal liberty, or imprisonment of up to two years (three years if such processing concerns special categories of data).

A criminal fine, restriction of personal liberty, or imprisonment of up to two years may also be imposed as a criminal sanction for hindering inspection proceedings.

Compensation

Data subjects have a right to compensation in respect of material and non-material damage. This requires more than a mere infringement of the GDPR and there must be actual material or non-material damage; however, there is no minimum threshold of seriousness before compensation is available, see CJEU judgment in the Oesterreichische Post case (C-300/21).

Are there any noticeable patterns or trends in how enforcement is carried out in Poland?

Trends in enforcement

To date, the majority of GDPR fines issued in Poland have targeted businesses in the industry and commerce, media, telecoms and broadcasting, finance, and insurance sectors. However, the Polish DPA has not limited its oversight to these sectors specifically. In Poland, the predominant reasons for GDPR penalties have been the lack of adequate legal grounds for data processing (as per GDPR Articles 5 and 6), shortcomings in information security (Article 32), or the inadequate execution of the obligation to notify of data breaches (Articles 33 and 34).

Sectoral inspection plans

Further, the Polish DPA announces annually the sectoral inspection plans. Every year, the authority indicates which business sectors or specific processing operations will be subject to increased regulatory scrutiny and potential enforcement for failure to comply. This year, the plan includes three points, one of which relates to public authorities processing personal data in the Schengen Information System (SIS) and Visa Information System (VIS). However, the other two points of the plan are relevant to businesses across all sectors in the private sector. The list includes entities processing personal data using Internet (web) applications. The Polish DPA specifies that it will verify the method of securing and sharing personal data processed in connection with the use of these web applications. The Polish regulator will also focus this year on verifying the correct fulfillment of information obligations by private sector entities.

Highest GDPR fines in Poland

The three most substantial fines issued in Poland to date – against Fortum Marketing and Sales Polska S.A., Morele.net, and Virgin Mobile Polska sp. z o.o. – were due to the companies not having robust organizational and technical protections, which resulted in unauthorized access to stored personal data. The most severe penalty imposed under the GDPR in Poland thus far is the PLN 4.9 million fine (about EUR 1.08 million) levied on Fortum Marketing and Sales Polska S.A. after a security breach exposed the personal data of 137,314 individuals. This breach was facilitated by unauthorized access to a server, a situation that could have been prevented with proper security measures, which the company's processor failed to implement. The Polish DPA has established that the controller, failing to properly verify the processor, should bear responsibility for the breach. Judgment is currently pending before the Supreme Administrative Court, with the final verdict yet to be confirmed.

In September 2019, Morele.net was fined EUR 660,000 for insufficient organizational and technical safeguards, which according to the President of the Office of Personal Data Protection did not prevent the violation of the integrity of the Morele.net platform against organized hacker attacks in November and December 2018. As a result of these attacks, personal data (including PESEL number) of over 2.2 million of Morele.net's clients were stolen, and hackers carried out attempts to extort fake payments. Morele.net appealed the decision and it was eventually annulled by the Supreme Administrative Court in February 2023. In the Court's view, the mere effect of the attack (successful hacking of the company's IT systems) is not proof that the data controller did not implement appropriate safeguards. In addition, the Court noted that the President of the Office of Personal Data Protection should have appointed an expert witness in the proceedings. The President of the Office of Personal Data Protection reconsidered the case and imposed an even higher fine on the controller in the amount of EUR 810,000 in February 2024, which is so far the second-highest fine imposed in Poland under the GDPR.

In December 2020, Virgin Mobile Polska was fined EUR 460,000 for failing to implement appropriate technical and organizational measures that would ensure an adequate level of IT security. Owing to this, they suffered a data breach whereby the personal data of 114,963 customers was accessed by an unauthorized person, in the scope of name and surname, PESEL registration number, series and number of ID card, telephone number, and NIP number. Due to the scope of the personal data disclosed, the breach resulted in a high risk to the rights and freedoms of natural persons.

Statistics from the Polish DPA's annual report

According to the annual report published by the Polish DPA in 2023:

- in 2022, the Polish DPA received 6,995 complaints from data subjects;
- the proceedings were completed in 6,479 cases, of which 1,830 resulted in administrative decisions;
- Polish DPA received 12,722 reports of data breaches (a similar number compared to 2021);

- Polish DPA imposed 20 administrative fines, in the total amount of PLN 7,850,861;
- sector inspections were carried out at 40 entities, eight of which were initiated as a result of learning of the data breach by the Polish DPA.

New Head of the Office

With the recent appointment of a new individual for the function of the President of the Office of Personal Data Protection, future enforcement practices may diverge, reflective of the new leadership's priorities and viewpoints.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in Poland?

Emerging technologies like Artificial Intelligence (AI), the Internet of Things (IoT), and blockchain are significantly influencing data protection considerations in Poland, as they do globally.

Artificial intelligence

AI systems have the ability to analyze and process large volumes of data, encompassing personal information, which empowers them to learn, make choices, and provide insights. At the same time, AI systems bring various issues regarding privacy, including but not limited to, valid consent, adherence to data minimization principles, and the implications of automated decision-making. Moreover, AI poses significant challenges to the rights of individuals, such as the right to erasure (the right to be forgotten). Addressing these concerns will predominantly require interpretation and application of the GDPR and the forthcoming Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (AI Act) which has been recently adopted by the European Parliament and should enter into force in the coming weeks.

According to the press release of the Polish DPA, the Polish supervisory authority is in the process of developing guidance for the design and adjustment of national legislation to meet data protection standards in relation to AI systems utilization. This guidance is intended to be a resource for the parliament during legislative deliberations regarding AI.

IoT

IoT services depend on the exchange of data between interconnected devices or between these devices and central infrastructure. Consequently, compliance with the privacy laws necessitates the consideration of multiple requirements. One of the main considerations is the fact that smart devices usually need access to data collected by other devices via the IoT and vice versa. Such access might, however, increase the risk of data breaches.

The Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (EU Data Act) imposes new obligations on those providing "connected products" (i.e., devices that collect data and communicate that data via an electronic communications service) and related services. The obligations generally relate to "product data" (which is data intended to be retrieved from the connected product) and service data.

In Poland, authorities have not yet responded to the challenges resulting from IoT and it is yet to be determined whether the government will pursue a path toward tighter regulation of IoT business models, as has been done, for example, in the UK.

Blockchain

The decentralized structure of blockchain networks and the enduring nature of the data recorded on them present two main categories of challenges for personal data processing with this technology.

The primary challenge involves clarifying roles in accordance with the GDPR. The definition of these roles will significantly influence how responsibilities and liabilities are distributed among participants within the blockchain network, and this allocation will vary based on the conceptual framework adopted.

The second challenge is associated with upholding the rights of individuals whose data are being processed. This includes the right to be informed about who is processing their data, in what manner, and for what duration. There is also the right to have the data rectified or to stop the processing. The immutable nature of data stored on the blockchain complicates, and in some cases may preclude, the fulfillment of these rights.

Poland is planning to enact a cryptocurrency law to align with the provisions of EU Regulation 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MICA Regulation), which governs cryptocurrency markets. This upcoming legislation aims to bolster customer and investor safeguards and uphold the cryptocurrency market's integrity. The Polish DPA has reviewed a preliminary draft of the law and highlighted certain areas that require further clarity, particularly concerning the personal data

protection of market participants.

Despite the EU's cryptocurrency regulation directly referencing the GDPR, the Polish DPA suggests that incorporating specific personal data protection management guidelines into national law could be beneficial. Such provisions would minimize ambiguity when determining the roles and obligations of entities processing personal data. For instance, there is a need for clarity regarding the mandatory data protection impact assessment stipulated in Article 35 of the GDPR, as well as the implementation of suitable technical and organizational measures as per Article 25 of the GDPR, especially considering the extensive data processing that occurs with emerging technologies like distributed ledger technology.

Are there any expected changes in data protection on the horizon in the next 12 months in Poland?

Within the next 12 months, there is a possibility that some new regulations will be enacted that could impact the requirements for data protection and privacy obligations in Poland.

Whistleblowing

A proposed Polish act concerning whistleblower protection which aims to implement the Directive (EU) 2019/1937 (Whistleblowing Directive) into the Polish legal system is currently in the process of parliamentary works. The Whistleblowing Directive focuses on establishing robust measures for the safeguarding of individuals who report breaches of EU law. The draft Polish law on whistleblowing provides for some additional provisions regarding data protection, such as providing a specific data retention period for processing operations regarding whistleblowing. Moreover, the personal data of the whistleblower, which could reveal their identity, shall not be disclosed to unauthorized individuals unless the whistleblower provides explicit consent.

The draft Polish law on whistleblowing raises some concerns regarding the absence of provisions specifying which personal data can be used to identify whistleblowers, which could ensure a uniform catalog of data categories in various registries and be in line with the data minimization principle. Additionally, the draft fails to address the processing of special category data, despite the potential for reports to reveal the political opinions or beliefs of the alleged violator. Changes in this regard may be introduced at the stage of ongoing parliamentary works.

Most of the provisions are anticipated to take effect three months following publication of the act in the Journal of Laws.

Cybersecurity

Cybersecurity is fundamentally connected to the safeguarding of personal data. On April 24, 2024, a proposed revision of the National Cyber Security System Law was released by the Polish government, which aims to implement the NIS2 Directive. This proposal addresses the escalating necessity for enhanced cybersecurity measures within Poland and strives to align domestic policies with those of the European Union. The forthcoming changes will substantially broaden the range of organizations that fall under the regulation's purview, mandate that companies determine for themselves whether they classify as either a key or important entity according to the law (self-identification), and raise the fines for non-compliance with cybersecurity responsibilities significantly.

Electronic Communications Law

On May 7, 2024, the government adopted a draft law to replace the current Act of 16 July 2004 Telecommunication Law, which will provide a new regulatory framework for electronic communications in Poland (Electronic Communications Law). The primary purpose of the draft law is to implement the provisions of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code into the national legal order. It contains provisions comprehensively regulating the electronic communications sector, defining the rights and obligations of regulatory authorities, entrepreneurs, and end users (including consumers). The new Electronic Communications Law will comprehensively regulate, among other things, the performance of activities involving the provision of electronic communications services, the regulation of electronic communications markets, as well as the rights and obligations of users, the principles of telecommunications data processing and the protection of electronic communications secrecy. It will also set out new rules of data processing in the provision of publicly available electronic communications services.

The Electronic Communications Law will now be the subject of parliamentary works. The new laws are expected, in principle, to come into force three months after publication in the Journal of Laws. ■

TUCA ZBARCEA ASOCIATII

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

ROMANIA

Ciprian Timofte
Partner and Head of the Data Privacy
ciprian.timofte@tuca.ro
+4021 204 88 90

Daniela Manolea
Senior Associate
daniela.manolea@tuca.ro
+4021 204 88 90

CEE LEGAL MATTERS

www.ceelegalmatters.com

What are the main data protection-related pieces of legislation and other regulations in Romania?

The key regulations in the field of data protection in Romania are (a) 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 (General Data Protection Regulation/ GDPR) and (b) Law No. 190/2018 on measures to implement GDPR (Law 190/2018). Law 190/2018 mostly addresses the so-called "open matters" set forth by GDPR (i.e., the matters upon which the member states have been given the freedom to regulate at their sole discretion).

Additionally, there are a series of regulations addressing the rules for processing personal data in various fields, such as:

- Law No. 363 of 28 December 2018 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, detecting, investigating, prosecuting, and combating criminal offenses or the execution of criminal penalties, educational and security measures, and on the free movement of such data (Law 363/2018);
- Law No. 506/2004 regarding the processing of personal data and the protection of privacy in the electronic communications sector (Law 506/2004);
- Law No. 365/2002 on electronic commerce (Law 365/2002);
- Law No. 363/2022 regarding the establishment of the organizational framework for the purpose of national operationalization of the centralized system for determining the member states that hold information on the convictions of third-country nationals and stateless persons, as well as for the amendment and completion of Law no. 290/2004 regarding the criminal record (Law 363/2022).

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, etc., or equivalent)?

Law 190/2018 (Article 2)

- national identification number – the number by which a natural person is identified in certain record systems and which has general applicability, such as personal numerical code, series, and number of the identity document, passport number, driver's license number, insurance number social health;
- remedial plan – appendix to the report entailing the sanctioning of the contravention, pursuant to the conditions provided for in art. 11, by which the National Supervisory Authority for the Processing of Personal Data, hereinafter referred to as the National Supervisory Authority, establishes the remedial measures and the remedial deadline;
- remedial measure – solution ordered by the National Supervisory Authority in the remedial plan in order for the authority/public body to fulfill the obligations provided for by law;
- remediation period – the period of time of a maximum of 90 days from the date of communication of the minutes of detection and sanctioning of the contravention, during which the authority/public body has the opportunity to remedy the irregularities identified and comply with its legal obligations;
- performance of a task that serves a public interest – includes those activities of political parties or organizations of citizens pertaining to national minorities, of non-governmental organizations, which serve to achieve the objectives provided by constitutional law or public international law or the functioning of the democratic system, including encouraging the participation of citizens in the decision-making process and the preparation of public policies, respectively the promotion of the principles and values of democracy.

Law 363/2018 (Article 4)

- restriction of processing – marking stored personal data, with the aim of limiting their future processing;
- profiling – any form of automatic processing of personal data that consists in the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects of workplace performance, economic status, health, personal preferences, interests, correctness, behavior, location or movements of the respective natural person;
- data record system – any structured set of personal data accessible according to specific criteria, either centralized, decentralized, or distributed according to functional or geographical criteria;
- genetic data – personal data relating to the inherited or acquired genetic characteristics of a natural person, which provide unique information regarding the physiology or health of that natural person, as it results in particular from an analysis of a sample of biological material collected from that individual;
- biometric data – personal data resulting from specific processing techniques, related to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

- health data – personal data related to the physical or mental health of a natural person, including the provision of medical assistance services, which reveal information about their state of health;

Law 506/2004 (Article 2)

- user – any natural person who benefits from an electronic communications service intended for the public, without necessarily being a subscriber to this service;
- traffic data – any data processed for the purpose of transmitting a communication through an electronic communications network or for the purpose of invoicing the applicable amount for the operation;
- equipment identification data – technical data of the providers of communications services intended for the public and of the providers of public electronic communications networks, which allow the identification of the location of their communications equipment, processed for the purpose of transmitting a communication through an electronic communications network or for the purpose of invoicing the applicable amount for the operation;
- location data – any data processed in an electronic communications network or through an electronic communications service, which indicates the geographical position of the terminal equipment of the user of an electronic communications service intended for the public;
- communication – any information exchanged or transmitted between a determined number of participants by means of an electronic communications service intended for the public; this does not include information transmitted to the public through an electronic communications network as part of an audiovisual program service, to the extent that no link can be established between the information in question and the identifiable subscriber or user who receives it;
- value-added service – any service that requires the processing of traffic data or location data, for purposes other than the transmission of communication or the invoicing of the applicable amount for the operation;
- security breach of personal data – breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data transmitted, stored or otherwise processed in connection with the provision of electronic communications services intended for the public.

Law 365/2002 (Article 1)

- information society service – any service that is performed using electronic means and has the following characteristics:
  - is carried out in consideration of a patrimonial benefit, procured to the offeror in the usual way by the recipient;
  - it is not necessary for the offeror and the recipient to be physically present simultaneously in the same place;
  - is carried out by transmitting the information at the recipient's individual request;
- domain – an area of an IT system, owned as such by a natural or legal person or by a group of natural or legal persons for the purpose of processing, storing, or transferring data;
- commercial communication – any form of communication intended to promote, directly or indirectly, the products, services, image, name or designation, firm or emblem of a trader or member of a regulated profession; the following do not in themselves constitute commercial communications: information allowing direct access to the activity of a natural or legal person, in particular by domain name or an e-mail address, communications related to the products, services, image, name or brands of a natural person or legal, carried out by a third party independent of the person in question, especially when they are carried out free of charge;
- identification data – any information that can allow or facilitate the performance of the types of operations, such as an identification code, name or designation, domicile or headquarters, telephone number, fax number, e-mail address, registration number, or other similar means of identification, the tax registration code, the personal numerical code and the like.

Which entities fall under the data privacy regulations in Romania?

Local data privacy regulations apply to:

- individuals or legal entities (including public authorities) processing personal data as part of their activities or the activities of one of its branches established in Romania;
- individuals or legal entities established outside the EU offering goods/services in Romania or monitoring the behavior of individuals in Romania.

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

Yes, there are a series of specific sector regulations addressing special rules for processing personal data in various fields.

Hence, Law 363/2018 regulates the processing of personal data in the field of criminal law and for national security purposes.

Law 365/2022 provides for a series of rules regarding the protection of private life in relation to commercial communications and the provision of information society services, while Law 5066/2004 aims to address the special rules regarding the protection of personal data in the field of electronic communications.

What rights do data subjects have under the data protection regulations in Romania?

The data subjects benefit from the rights regulated under GDPR, namely: (a) the right of access; (b) the right to rectification; (c) the right to erasure ("the right to be forgotten"); (d) the right to restriction of processing; (e) the right to data portability; (f) the right to object; (g) the right to lodge a complaint with the supervisory authority; (h) the right to an effective judicial remedy against the supervisory authority and/or the data controller or data processor.

What is the territorial application of the data privacy regime in your jurisdiction?

Romanian data protection regulations apply to the processing of personal data:

(a) in the context of the activities of an establishment of a data controller or a data processor in Romania, regardless of whether the processing itself takes place in Romania.

(b) pertaining to data subjects who are in Romania made by a controller or processor not established in Romania, where the processing activities are related to the offering of goods or services to such data subjects in Romania (irrespective of whether a payment of the data subject is required) or the monitoring of their behavior (as far as their behavior takes place within the territory of Romania).

What are the key factors and considerations to adhere to when engaging in the processing of personal data within your jurisdiction?

Generally, organizations wishing to engage in data processing in Romania should comply with the following data processing principles:

- lawfulness and fairness: organizations should ensure that each processing has an adequate legal basis and does not lead to unfair consequences for the concerned individuals;
- transparency: organizations should ensure that the data subjects are made aware of the key aspects related to the contemplated processing unless such information is impossible or it would involve disproportionate efforts;
- purpose limitation: organizations should ensure that they are processing the personal data only for specified and compatible purposes;
- data minimization: organizations should ensure that when processing personal data they choose the less intrusive ways, to avoid excessive processing;
- data accuracy: organizations should ensure that reasonable steps are taken to ensure that personal data is accurate and updated (where the case);
- storage limitation: organizations should ensure that personal data is kept in a form that allows the identification of the concerned persons for a period that does not exceed the period necessary to fulfill the purposes for which the respective data are processed;
- integrity and confidentiality: data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures;
- accountability: organizations should be able to demonstrate due compliance with the above-mentioned principles and rules.

In addition, organizations should take into account that there are:

- sector-specific rules governing the processing of personal data in various industries (such as in the telecom, banking, and financial or e-commerce fields);
- special rules that apply when processing certain categories of personal data (such as processing of national identifiers) or for certain purposes (such as rules that apply when monitoring electronic communications means at the workplace);
- cases set out locally in which performing a data privacy impact assessment (DPIA) is mandatory.

What are the regulations and best practices concerning the retention and deletion of personal data in Romania?

Generally, when setting out the applicable retention periods organizations should consider:

- the mandatory retention periods prescribed by the applicable local regulations (for instance, 50 years for the storage of the personnel data, five years – for KYC/AML data or for financial/accounting data, etc.);
- the applicable rules regarding statute of limitations, such as for defending the rights and interests against claims in court (typically, the general three years term for time barring claims should be considered);
- the organization's business needs, subject to the particular-

ities of the carried-out activity and envisaged processing purposes.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

The regulatory authority in Romania regarding data protection is the National Supervisory Authority for the Processing of Personal Data (ANSPDCP) – https://www.dataprotection.ro

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in Romania

As per local law, appointing a Data Protection Officer is mandatory:

- where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- where the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale;
- where the core activities of the controller or the processor consist of processing on a large scale special categories of data or personal data relating to criminal convictions and offenses

It has been construed in practice that "regular and systematic" monitoring implies a continuous and recurrent monitoring activity. This might be the case, for instance, where:

- managing a telecommunication network;
- profiling and scoring for the purposes of risk assessment (for example, for credit, insurance premiums, fraud prevention, and money laundering);
- location tracking, for example through mobile applications (geo-location);
- closed-circuit television – CCTV;
- processing of patient data by a hospital;
- processing of content data, location data, and traffic data by Internet service providers;
- using behavioral advertising.
- When determining whether the processing is carried out on a large scale, the following criteria should be considered:
- the number of data subjects – a specific number or a proportion of the relevant population;
- the volume of data and/or the range of different data items being processed;
- the duration, or permanence, of the data processing activity;
- the geographical extent of the processing activity.

Where possible (including where in doubt whether appointing a DPO is mandatory), it is advisable to nevertheless designate a data protection officer, since this would show diligence and care in complying with the relevant data protection duties.

In any case, when appointing a DPO, organizations are required to:

- publish the contact details of such on their website and/ or on any other easily accessible medium;
- communicate the contact details to the local Supervisory Authority.

How should data breaches be handled in your jurisdiction?

As a rule, personal data breaches need to be reported in the cases and within the timeframe regulated by GDPR. This means that the personal data breaches should be reported to the local Supervisory Authority where they are likely to pose risks to data subjects, within 72 hours after becoming aware of them.

By exception, personal data breaches falling under Law No. 506/2004 (personal data breaches in connection with the provisions of public electronic communication services) need to be notified in all cases, irrespective if they are likely or not to pose risks to data subjects.

When assessing the risks posed to data subjects, consideration should be given to both the likelihood and severity of the breach of the rights and freedoms of data subjects. To this end, the following criteria could be inter alia taken into account: (a) the type of breach (confidentiality, data availability and/ or data integrity); (b) the nature, sensitivity, and volume of personal data; (c) the ease of identification of individuals; (d) the severity of consequences for affected individuals; (e) the special characteristics of affected individuals; (f) the special characteristics of the controller; (g) the number of affected individuals; (h) the duration of the breach.

What are the potential penalties and fines for non-compliance with data protection regulations in Romania?

Failure to comply with the relevant data protection laws might trigger the following sanctions:

- warnings or administrative fines of up to EUR 20 million or, in case of legal enterprises, of up to 4% of the total annual worldwide turnover in the preceding financial year, whichever is the higher; and/ or
- corrective measures (such as banning, temporarily or definitively, the processing of personal data, limiting the processing, orders to fulfill certain compliance actions,

including communicating a personal data breach to the affected individuals, etc.).

In certain cases, the local Supervisory Authority may decide to publish the sanction on its website, which might trigger significant reputational damages to the concerned data controller.

Are there any noticeable patterns or trends in how enforcement is carried out in Romania?

One may say that in the past most investigations were carried out by the local Supervisory Authority following received complaints. Still, a change in this paradigm may be noticed, as there is currently a trend in increasing the number of ex officio investigations.

Typically, such ex officio investigations are focused on so-called "data sensitive industries," out of which probably the most exposed ones are financial and banking, telecom, e-commerce, and retail industry. Typically, the key areas of concern during investigations were compliance with transparency rules, use of monitoring tools (new technologies included), profiling, and marketing.

On another level, there may be a trend in the increase of the volume and amounts of the applied fine, all after a past period where the local Supervisory Authority had a fairly relaxed approach to these.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in Romania?

All these emerging technologies pose significant data privacy challenges, particularly due to the high volumes of personal data involved and difficulties in addressing the key data protection principles (such as transparency, data accuracy, data minimization, etc.).

Besides such data privacy concerns, an equally important challenge is to accommodate and strike the proper balance between the need to protect private life and the achievement of the benefits entailed by such emerging technologies. This is more that at the EU level, one may notice a trend in regulating in fairly much detail these technologies which, besides the obvious advantage of increased predictability, might equally impact the appetite of using such new technologies or even hinder the implementation thereof.

These types of challenges are likely to bring incertitude to the way these emerging technologies dependent on the processing of personal data would evolve particularly on how the interference of such technologies with the data privacy requirements will be addressed and what are the expectations from the relevant stakeholders in terms of compliance. In this regard, the guidance issued by the data privacy authorities (both at the national and EU level) will play a crucial role.

Are there any expected changes in data protection on the horizon in the next 12 months in Romania?

For the next 12 months, no notable legislative evolutions are likely to appear at a local level. Rather, evolutions will most likely come from the EU level, particularly further to the adoption of the much-expected EU regulation on artificial intelligence (so-called "AI Regulation") and hopefully of EU Regulation governing the protection of personal data in the electronic communication sector (so-called "E-Privacy Regulation"), which is pending adoption from few years. ■

PR legal
PETROVIĆ - RUŽIČIĆ
ADVOKATI - ATTORNEYS AT LAW

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

SERBIA

Ivana Ruzicic
Managing Partner
ivana.ruzicic@prlegal.rs
+381 (0) 114208020

CEE
LEGAL MATTERS

www.ceelegalmatters.com

What are the main data protection-related pieces of legislation and other regulations in the Republic of Serbia?

Data protection matter in the Republic of Serbia is governed by the Law on Personal Data Protection (Official Gazette of RS no. 87/2018) (the LPDP), and several subordinate legislations passed thereunder, including Decision on the list of states, their parts of territories, or one or more sectors within those states and international organizations where it is considered that an adequate level of protection of personal data is ensured (Official Gazette of RS no. 55/2019) and Decision on the list of types of processing activities of personal data for which an assessment of the impact on the protection of personal data must be carried out and the opinion of the Commissioner for Information of Public Importance and Personal Data Protection sought (Official Gazette of RS no. 45/2019).

In addition, it is important to note that the Serbian LPDP is modeled after the GDPR, extensively mirroring the solutions outlined in the European Regulation.

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, etc., or equivalent)?

Definitions of key terms pertaining to personal data protection are stipulated by the LPDP, e.g.:

- "Personal data" refers to any information relating to an identified or identifiable natural person, directly or indirectly, particularly based on identifiers such as name, identification number, location data, electronic identifiers, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;
- "Data subject" is a natural person to whom personal data relates and is being processed;
- "Processing of personal data" encompasses any operation or set of operations performed, whether automated or not, on personal data or sets of personal data, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction;
- "Controller" is a natural or legal person, or governmental body, that independently or jointly with others determines the purpose and means of processing personal data. The law that regulates the purpose and means of processing may designate the controller or prescribe conditions for its designation;
- "Processor" is a natural or legal person, or governmental body, that processes personal data on behalf of the controller;
- "Consent" of the data subject is any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by clear affirmative action, signify agreement to the processing of personal data relating to them;
- "Personal data breach" is a breach of personal data security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data that has been transmitted, stored, or otherwise processed; etc.

Which entities fall under the data privacy regulations in the Republic of Serbia?

Pursuant to the LPDP, the subject regulation applies to the processing of personal data carried out, in whole or in part, by automated means, as well as to non-automated processing of personal data that constitutes part of a data collection or is intended for a data collection.

The LPDP, however, does not apply to the processing of personal data carried out by an individual for personal or household purposes.

In addition, the LPDP applies to the processing of personal data carried out by a controller or processor with a registered office, residence, or domicile in the territory of the Republic of Serbia, within activities conducted in the territory of the Republic of Serbia, regardless of whether the processing activity is carried out within the territory of the Republic of Serbia.

Furthermore, the LPDP applies to the processing of personal data of data subjects who have a residence or domicile in the territory of the Republic of Serbia by a controller or processor who does not have a registered office, residence, or domicile in the territory of the Republic of Serbia if the processing activities are related to:

- offering goods or services to the data subject in the territory of the Republic of Serbia, regardless of whether payment for these goods or services is requested from that data subject;
- monitoring the activities of the data subject if the activities are carried out in the territory of the Republic of Serbia.

Accordingly, data privacy regulations of the Republic of Serbia bind various types of entities, i.e., both public and private organizations and individuals (e.g., public and private companies, institutions, online retailers, healthcare providers, employers,

etc.).

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

There are specific regulatory regimes, i.e., rules applicable to:

- data processing conducted by competent authorities for specific purposes;
- processing of special categories of personal data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation); and
- data regarding criminal judgments and offenses.

Namely, the LPDP prescribes that processing carried out by competent authorities for specific purposes, involving the disclosure of racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning a person's sex life or sexual orientation (data considered sensitive, i.e., special), is permitted only if necessary, with the application of appropriate measures to protect the rights of the individuals to whom the data relates, in one of the following cases:

- the competent authority is legally authorized to process these special categories of personal data;
- processing of special categories of personal data is carried out to protect the vital interests of the data subject or another natural person;
- the processing relates to special categories of personal data that the data subject has manifestly made public.

Additionally, the LPDP provides for several exceptions to the rules that apply to data processing when carried out by competent authorities.

As for the processing of special categories of personal data, it is in general prohibited, except in cases explicitly prescribed by the LPDP (e.g., processing occurs within a registered activity, applying suitable protections by a non-profit entity like a foundation, association, or group with political, philosophical, religious, or labor union aims, provided that processing pertains to current or past members of the organization or those in regular contact concerning its goals, and that personal data remains confidential within the organization unless explicitly approved by the individuals involved).

On the subject of the processing related to criminal judgments and offenses, the LPDP prescribes that it may only be carried out under the supervision of the competent authority or, if the processing is permitted by law, with the application of appropriate measures to protect the rights and freedoms of the data subjects. A record of criminal judgments is maintained solely by and under the supervision of the competent authority.

What rights do data subjects have under the data protection regulations in the Republic of Serbia?

The LPDP prescribes the following rights of data subjects:

- Right to information: Data subjects have the right to be informed about the processing of their personal data, including the purpose of processing, types of data processed, data retention period, and other relevant information.
- Right to access: Data subjects have the right to access their personal data being processed, as well as information about the processing methods and use of their data.
- Right to rectification: If personal data is inaccurate or incomplete, data subjects have the right to request correction of such data.
- Right to erasure: Data subjects may request the deletion of their personal data if the data has been unlawfully processed or is no longer necessary for the purpose for which it was collected.
- Right to restriction of processing: Data subjects have the right to request restriction of the processing of their personal data in certain situations, such as disputing the accuracy of the data or if the processing is unlawful.
- Right to data portability: In certain cases, data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and transmit it to another controller.
- Right to object: Data subjects have the right to object to the processing of their personal data in certain situations, such as processing for marketing purposes or processing based on legitimate interests.
- Right to lodge a complaint to the Commissioner for Information of Public Importance and Personal Data Protection: Data subjects have the right to lodge a complaint if they believe that the processing of their personal data has been carried out contrary to the provisions of the LPDP.

As regards the above-mentioned right to information, the LPDP prescribes the mandatory content of the notification on personal data processing, partially depending on whether the data is collected from the data subject or a third party.

What is the territorial application of the data privacy regime in your jurisdiction?

As previously mentioned, the LPDP applies to the processing of personal data carried out by a controller or processor with a registered office, residence, or domicile in the territory of the Republic of Serbia, within activities conducted in the territory of the Republic of Serbia, regardless of whether the processing activity is carried out within the territory of the Republic of Serbia.

Additionally, the LPDP applies to the processing of personal data of data subjects who have a residence or domicile in the territory of the Republic of Serbia by a controller or processor who does not have a registered office, residence, or domicile in the territory of the Republic of Serbia if the processing activities are related to:

- offering goods or services to the data subject in the territory of the Republic of Serbia, regardless of whether payment for these goods or services is requested from that data subject;
- monitoring the activities of the data subject if the activities are carried out in the territory of the Republic of Serbia.

What are the key factors and considerations to adhere to when engaging in the processing of personal data within your jurisdiction?

When engaging in the processing of personal data within the jurisdiction of the Republic of Serbia, key factors and considerations to adhere to in particular include:

- Compliance with principles of data processing established by the LPDP: Adherence to the principles of lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality of data is of particular importance for lawful processing.
- Data security: It is necessary to implement appropriate technical, organizational, and personnel measures to ensure the security, confidentiality, integrity, and availability of personal data.
- Data subject rights: It is also important to inform data subjects of their rights pertaining to personal data protection, to respect them, and to facilitate their exercise.
- Cross-border data transfers: It is necessary to comply with legal requirements and safeguards when transferring personal data outside of the Republic of Serbia to ensure an adequate level of data protection.
- Data protection impact assessments (DPIAs): For high-risk data processing activities, i.e., which could imply a high risk to the rights and freedoms of data subjects, or which are determined as such by a decision of the Commissioner for Information of Public Importance and Personal Data Protection, it is necessary to undertake DPIA and implement necessary measures to mitigate risks to data subjects' rights and freedoms. In relation thereto, the afore-mentioned decision provides for the obligation to seek the official opinion of the Commissioner for Information of Public Importance and Personal Data Protection in the event of certain data processing activities (e.g., processing of personal data that involves tracking the location or behavior of an individual in the case of systematic processing of communication data generated using telephones, the internet, or other communication means).
- Data breach notification: It is also necessary to implement procedures for timely detection, assessment, and notification of personal data breaches to relevant authorities and affected data subjects, as required by the LPDP.

As for the above-mentioned principles of data processing established by the LPDP:

- the principle of lawfulness, fairness, and transparency means that personal must be processed lawfully, fairly, and transparently in relation to the data subject, whereby lawful processing is considered processing that complies with the LPDP or another regulation governing processing;
- the principle of purpose limitation means that personal data need to be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes;
- the principle of data minimization means that personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes of processing;
- the principle of accuracy means that personal data need to be accurate and, where necessary, kept up to date, whereby all reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay, considering the purposes of the processing;
- the principle of storage limitation means that personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes of processing; and
- the principle of integrity and confidentiality of data means that personal data need to be processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical, organizational, and personnel measures.

Regarding the aforementioned principle of lawfulness, the LPDP prescribes that processing of personal data is lawful only if one of the following conditions (i.e., legal grounds) is met:

- the data subject has consented to the processing of their personal data for one or more specific purposes;
- processing is necessary for the performance of a contract concluded with the data subject or for taking pre-contractual steps at the request of the data subject;
- processing is necessary for compliance with a legal obligation of the controller;
- processing is necessary to protect the vital interests of the data subject or another natural person;
- processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring personal data protection, especially when the data subject is a minor.

If processing is based on the consent of the data subject, the controller must be able to demonstrate that the individual has consented to the processing of their personal data. As previously mentioned, in order to be considered legally valid, the consent needs to be freely given, a specific, informed, and unambiguous indication of the data subject's will, given by a statement or a clear affirmative action.

Before giving consent, the data subject must be informed of the prescribed circumstances of processing, as well as their right to withdraw consent and the effects of withdrawal. The data subject has the right to withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Also, the withdrawal of consent must be as easy as giving consent.

In line with the practice of the Commissioner for Information of Public Importance and Personal Data Protection, consent is not considered a valid legal basis for processing personal data in employment relationships, as the hierarchical relationship between the employer and the employee does not allow for it to be considered freely given.

What are the regulations and best practices concerning the retention and deletion of personal data in the Republic of Serbia?

As mentioned above, personal data must be stored in a format that allows the identification of data subjects only for as long as necessary to fulfill the purpose of processing. In other words, once the purpose of the processing has been met, it is required to delete data.

On the subject of data deletion, the LPDP stipulates that the controller is obliged to delete the data without undue delay in the following cases:

- personal data is no longer necessary for the purposes for which they were collected or otherwise processed;
- data subject has withdrawn consent on which the processing was based (in accordance with the LPDP), and there is no other legal basis for processing;
- data subject has objected to the processing (in accordance with the LPDP);
- personal data has been processed unlawfully;
- personal data must be erased for compliance with the controller's legal obligations;
- personal data has been collected in relation to the provision of information society services (under the LPDP).

In addition, if the controller has publicly disclosed personal data, their obligation to erase the data also encompasses taking all reasonable measures, including technical measures, in line with available technologies and cost considerations, to inform other controllers processing such data that the data subject has requested the deletion of all copies of this data and references or electronic links to this data.

However, the right to erasure, i.e., data deletion is limited by the LPDP, which prescribes that it shall not be applied to the extent that processing is necessary for:

- exercising the right to freedom of expression and information;
- compliance with a legal obligation of the controller requiring processing or for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the controller;
- exercising a public interest in the field of public health (in accordance with the LPDP);
- archiving purposes in the public interest, scientific or historical research purposes, and statistical purposes (in accordance with the LPDP), where it is reasonably expected that exercising this right could render impossible or seriously impair the achievement of the purposes of such processing;
- submitting, exercising, or defending a legal claim.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

The regulatory authority in the Republic of Serbia regarding data protection is the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner).

The Commissioner is appointed by the National Assembly of the Republic of Serbia, and it is completely independent in exercising their powers and duties under the LPDP, i.e., free from any direct or indirect external influence, and cannot seek or accept instructions from anyone.

To ensure the effective exercise of the powers prescribed by the LPDP, the necessary financial resources for work, and office space, as well as the necessary technical, organizational, and personnel conditions for the work of the Commissioner, are provided from the budget.

In exercising their powers, the Commissioner acts in accordance with the law regulating general administrative procedure, as well as with the relevant provisions of the law regulating inspection supervision.

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in the Republic of Serbia, and under what conditions?

As a rule, the controller and processor may designate a data protection officer (DPO).

However, the controller and processor are required to designate a DPO if:

- the processing is carried out by a public authority, except for processing by a court in the performance of its judicial duties;
- the core activities of the controller or processor consist of processing operations which, by their nature, scope, or purposes, require regular and systematic monitoring of a large number of data subjects;
- the core activities of the controller or processor consist of processing special categories of personal data (as defined by the LPDP), or personal data relating to criminal convictions and offenses (in terms of the LPDP), on a large scale.

Appointed DPOs are subject to registration with the Commissioner, and the controller is obliged to publish their contact details.

A DPO may be an employee of the controller or processor or may perform duties based on a contract, and they are appointed based on their professional qualifications, especially their expertise and experience in the field of personal data protection, as well as their ability to fulfill the obligations prescribed under the LPDP.

How should data breaches be handled in your jurisdiction?

Pursuant to the LPDP, the controller is obliged to inform the Commissioner without undue delay of any personal data breach that may pose a risk to the rights and freedoms of individuals, or, if possible, within 72 hours from becoming aware of the breach. On the other hand, the processor is obligated to inform the controller, without undue delay, after becoming aware of a personal data breach.

The notification to the Commissioner must contain at least the following information:

- description of the nature of the personal data breach, including the types of data and the approximate number of individuals whose data of that type is affected, as well as the approximate number of personal data affected by the breach;
- name and contact details of the data protection officer or information on another way to obtain information about the breach;
- description of the potential consequences of the breach;
- description of the measures taken by the controller or proposed measures related to the breach, including measures taken to mitigate harmful consequences.

The controller is also required to document every personal data breach, including facts about the breach, its consequences, and measures taken to rectify it.

In addition, if a personal data breach may pose a high risk to the rights and freedoms of individuals, the controller must inform the data subjects without undue delay about the breach.

In the subject notification, the controller must clearly and understandably describe the nature of the data breach and provide at least the information on:

- name and contact details of the data protection officer or information on another way to obtain information about the breach;
- description of the potential consequences of the breach;
- description of the measures taken by the controller or proposed measures related to the breach, including measures taken to mitigate harmful consequences.

The LPDP also stipulates several situations in which the controller is not obligated to inform the data subject of the data breach (e.g., if notifying the data subject would involve dispro-

portionate effort in terms of time and resources, in which case the controller must provide the notification to the data subject through public notification or by other effective means).

What are the potential penalties and fines for non-compliance with data protection regulations in the Republic of Serbia?

The LPDP prescribes a misdemeanor liability for non-compliance with data protection regulations, i.e., that a fine shall be imposed, ranging:

- from RSD 50,000 to RSD 2 million (approximately from EUR 425 to EUR 16,950), if the controller or processor is a legal entity;
- from RSD 20,000 to RSD 500,000 (approximately from EUR 170 to EUR 4,240), if the controller or processor is an entrepreneur; and
- from RSD 5,000 to RSD 150,000 (approximately from EUR 43 to EUR 1,275), to an individual or a responsible person of a controller/processor (who is a legal entity).

Are there any noticeable patterns or trends in how enforcement is carried out in the Republic of Serbia?

There is indeed a noticeable trend of increasing awareness regarding personal data protection rules lately in the Republic of Serbia, meaning that businesses and individuals are paying more attention to their rights and obligations in this respect. On the other hand, the Commissioner for Information of Public Importance and Personal Data Protection has a respectable practice, following the example of EU data protection bodies, which includes not only monitoring and enforcement measures but also annual publication containing official viewpoints of the respective authority, which serve as guidelines for businesses and individuals regarding data protection issues.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in the Republic of Serbia?

Emerging technologies like AI, IoT, and blockchain have a significant impact on data protection considerations in Serbia. Some key points are given below:

- Increased data volume: These technologies lead to a massive increase in the volume of data collected, processed, and stored. This poses challenges in terms of data security, privacy, and the ability to manage and protect such vast amounts of information effectively.
- The complexity of data processing: Furthermore, the respective technologies gather and process data in real-time, often without direct human intervention. This dynamic and continuous data processing requires robust security measures and privacy safeguards to prevent unauthorized access or misuse.
- Data privacy concerns: With the extensive use of such complex algorithms, there are concerns about how personal data is collected, used, and shared. It raises questions about transparency, consent, and ensuring that individuals have control over their data.
- Cybersecurity challenges: As these technologies become more interconnected and data-driven, the risk of cybersecurity threats such as data breaches, hacking, and malware attacks also increases. As previously mentioned, robust cybersecurity measures and proactive monitoring are essential to mitigate these risks.

In summary, while emerging technologies offer numerous benefits and advancements, they also bring forth complex challenges related to data protection, privacy, cybersecurity, and ethical use of data. Adapting regulatory frameworks, implementing robust security measures, promoting transparency, and fostering awareness are crucial steps in addressing these challenges effectively.

Are there any expected changes in data protection on the horizon in the next 12 months in the Republic of Serbia?

On August 25, 2023, the Government of the Republic of Serbia adopted the Personal Data Protection Strategy for the 2023-2030 period.

The subject enactment emphasizes the need to improve the LPDP, but also to harmonize other regulations with the provisions thereof, i.e., rules regarding personal data protection, and regulating the use of equipment for audio and video surveillance, as well as the use of genetic and biometric data.

In addition to the above, it has announced a harsher penal policy for breaching obligations concerning personal data protection, emphasizing that the model used by the Commission for the Protection of Competition should be applied in this regard, according to which, in the event of a violation of regulations in the respective matter, the commission itself can impose a fine, whereby the amount thereof depends on the company's income.

It has also been announced that the institutional capacities of the Commissioner shall be strengthened, by providing additional regional offices, and by increasing the number of persons specialized for personal data protection in the bodies dealing with the subject issues, through their education.

Nevertheless, it cannot be said with certainty whether any of the above will be implemented in the next 12 months. ■


PR legal
PETROVIĆ • RUŽIČIĆ
ADVOKATI • ATTORNEYS AT LAW

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: DATA PROTECTION 2024

UKRAINE

Oleksiy Stolyarenko
Partner and Head of IT/TMT
Oleksiy.Stolyarenko@bakermckenzie.com
+380 44 590 0101

Khrystyna Oleniuk
Associate, IP Practice Group
Khrystyna.Oleniuk@bakermckenzie.com
+380 44 590 0101

CEE
LEGAL MATTERS

www.ceelegalmatters.com

What are the main data protection-related pieces of legislation and other regulations in Ukraine?

The main Ukrainian data protection law is the Law of Ukraine on Personal Data Protection (PDP) adopted in 2010. It establishes general requirements and obligations relating to the collection, processing, and use of personal data by private bodies and by the government of Ukraine.

Apart from the PDP, the main sources of personal data protection in Ukraine are:

- The Constitution of Ukraine;
- The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the additional protocol to it, ratified by Ukraine in 2010;
- The Civil Code of Ukraine;
- Respective provisions of the Code of Ukraine on Administrative Offenses and the Criminal Code establishing respective liability for personal data offenses;
- The Law of Ukraine "On Information"
- The Law of Ukraine "On Electronic Commerce"
- The Law of Ukraine "On Electronic Communications," and
- The Law of Ukraine "On Protection of Information in the Information and Telecommunication Systems"

A number of regulations approved by the Ukrainian Parliament Commissioner for Human Rights, in particular:

- Model Rules on Personal Data Processing;
- Rules on Exercising Control by the Ukrainian Parliament Commissioner for Human Rights over Compliance with the Laws on Personal Data Protection; and
- Rules for Notification of the Ukrainian Parliament Commissioner for Human Rights on the Processing of Personal Data that Constitutes a Special Risk for the Rights and Freedoms of Data Subjects, On the Structural Department or Designated Individual Responsible for Work-Related Processing of Personal Data and the Publication of Such Information.

What are the other primary definitions outlined in the legislation within your jurisdiction (among others, data processing, data processor, data controller, data subject, personal data, sensitive personal data, consent, etc., or equivalent)?

All of the primary definitions are embodied in the PDP. The PDP defines personal data as any information about an individual who is identified or can be specifically identified.

The Constitutional Court of Ukraine, in its Decision No. 2-rp/2012 dated January 20, 2012, held that "Personal Data" constitutes confidential personal information, access to which is limited by a person himself/herself. Such confidential personal information may include data about the individual's:

- nationality
- education
- marital status
- religious beliefs
- health
- current address
- date and place of birth
- property status

The list of confidential personal information is not exhaustive.

Moreover, while the PDP does not provide a specific definition for sensitive data, it prescribes that certain categories of personal data are required to be processed in a special manner. Processing of such data is allowed if unambiguous consent has been given by the personal data subject or based on specifically prescribed PDP exemptions.

According to the PDP, sensitive data includes:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical belief
- personal data revealing trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health/medical information
- data concerning a natural person's sex life or sexual orientation
- financial information
- personal data regarding an individual's criminal convictions or record
- location and or methods of transportation
- facts related to administrative liability
- criminal investigation measures related to a preliminary investigation and the measures envisaged by the Law of Ukraine "On Investigating Activity"
- instances of violence against a person

Turning to the definition of subjects, involved in personal data processing, according to the PDP, the controller/owner is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

The processor/agent is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

Personal data processing is any action or set of actions, such as collection, registration, accumulation, storage, adaptation, change, renewal, use and distribution (circulation, sale, transfer), depersonalization, and destruction of personal data, including using information (automated) systems.

Personal data processing requires consent that is defined as a voluntary expression of the individual's will to grant the permission to process his/her personal data in accordance with the stated purpose of their processing, expressed in writing or in a form that allows concluding that consent has been provided.

In the field of e-commerce, personal data subjects can provide consent by marking a checkbox, during registration. However, the system should not allow any personal data processing until the consent mark is provided.

In addition, the PDP prescribes certain cases when consent is not required, specifically:

- when it is explicitly provided for by law; and
- where the data is necessary for the purposes of maintaining national security, economic welfare, and for the protection of human rights.

Which entities fall under the data privacy regulations in Ukraine?

In general, the PDP does not limit its personal application scope. The PDP aims to protect personal data during its processing, as well as when personal data is used for purposes other than in private or certain professional circumstances.

Do specific sectors or types of data have distinct regulatory regimes within your jurisdiction? If so, which?

Yes, there is a local copy requirement applicable for banking secrecy information, which only applies to banks in Ukraine.

While the PDP does not require personal data to be stored in Ukraine or to have a local copy, there are general accounting and bookkeeping standards that require keeping electronic copies or hard copies of certain documents that might contain personal data for the purposes of tax, accounting, and other compliance, for example, payroll lists, lists of employees, etc.

What rights do data subjects have under the data protection regulations in Ukraine?

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

- the right to access the data subject's own personal data;
- the right to rectify/correct the data subject's own personal data where inaccurate or incomplete;
- the right to erasure of personal data;
- the right to restrict data processing;
- the right to data portability;
- the right to object to the processing of personal data;
- the right to withdraw consent;
- the right to know about the sources of collection, location of their personal data, purpose of their processing, location and/or place of residence (temporary residence) of the Controller or Processor of Personal Data, or to seek such information from authorized persons (unless an exception applies);
- the right to receive information about the circumstances in which personal data will be accessed, in particular information about third persons to whom their personal data are transferred;
- the right to receive a response about whether their personal data is processed and information on the content of their personal data within 30 days from the moment the relevant request was received (unless an exception applies);
- the right of protection of their personal data from illegal processing and accidental loss, destruction, damage due to deliberate concealment, failure to provide them or delay in providing such data, and protection from provision of data which are inaccurate or damaging to the honor, dignity, and business reputation of an individual;
- the right to lodge complaints about the processing of their personal data to the Commissioner or courts;
- the right to use legal remedies if there is a violation of personal data protection laws;
- the right to know about any automatic mechanism of processing of personal data;
- the right to be protected from automated decisions that have legal consequences for them.

What is the territorial application of the data privacy regime in your jurisdiction?

The PDP applies to all personal data processing (i.e., acquisition, registration, accumulation, storage, adaptation, modification, restoration, use, and distribution (dissemination, sale, transfer), depersonalization, and destruction) within the territory of Ukraine. However, enforcement of the PDP against legal entities and individuals without legal presence in Ukraine is not established at the moment.

What are the key factors and considerations to adhere to when engaging in the processing of personal data within your jurisdiction?

Most obligations outlined in the PDP directly pertain to data controllers/owners. However, data processors/agents may also share responsibility for compliance.

It is essential to follow the below requirements of PDP:

- obtain consent for data processing;
- collect and process personal data for specific purposes and avoid incompatible processing;
- process only essential data for the stated purpose; maintain a record of processing activities;
- implement appropriate measures to comply with data privacy and security;
- provide training to employees, etc.

What are the regulations and best practices concerning the retention and deletion of personal data in Ukraine?

Retention of personal data refers to maintaining the established access regime for that data. The retention period is specified either in the data subject's consent or by legal requirements. After this period expires, the personal data must be securely destroyed.

According to the PDP, personal data must be destroyed or removed in the following cases:

- when the specified storage period expires, as outlined in the data subject's consent or by legal requirements (some data storage terms cannot be shortened by consent);
- upon termination of legal relations between the data subject and the data controller/owner or data processor/agent, unless otherwise mandated by law; and/or
- when a court decision orders the removal of an individual's data from a personal database.

Who serves as the regulatory authority(s) in your jurisdiction regarding data protection?

The Ukrainian Parliament's Commissioner for Human Rights (also known as the Ombudsman) (Commissioner) oversees compliance with data protection legislation.

The PDP requires legal entities and individuals processing sensitive data to file the respective notice to the Commissioner.

Is the appointment of a Data Protection Officer mandatory for certain organizations or sectors in Ukraine, and under what conditions?

The PDP requires legal entities and individuals processing sensitive data to appoint a personal data officer (DPO) or establish a specific division responsible for personal data protection.

At the same time, the PDP does not provide any specific requirements for a DPO. However, the Commissioner suggests appointing a director of the company, their deputy, HR manager, or compliance officer to the position of DPO, because the DPO will have access to all data and premises of the company.

How should data breaches be handled in your jurisdiction?

N/A. There is no requirement to report data security breaches or losses to the appropriate state authority.

The PDP provided that personal data protection regulations are enforced by the Commissioner and by the courts of Ukraine.

What are the potential penalties and fines for non-compliance with data protection regulations in Ukraine?

The Code of Ukraine on Administrative Offenses establishes administrative liability for the following violations of the PDP:

- failure to notify or delay in providing notice to the Commissioner regarding the processing of personal data or a change to the information submitted, which is subject to notification requirements under Ukrainian legislation, or submission of incomplete or false information: may result in a fine of up to approximately USD 230, and, if repeated within a year, up to approximately USD 1,150;
- non-fulfillment of legitimate requests (orders) of the Commissioner or determined state officials of the Commissioner's secretariat regarding the elimination or prevention of violations of personal data protection legislation: may result in a fine of up to approximately USD 580, and, if repeated within a year, up to approximately USD 1,150;

- non-compliance with the personal data protection procedure established by personal data protection law, which leads to illegal access to them or violation of the rights of the data subject: may result in a fine of up to approximately USD 580, and, if repeated within a year, up to approximately USD 1,150.

The criminal penalties from regulators and law enforcement for:

- illegal processing of confidential information about a person or illegal alteration of such information is punishable by a fine of approximately USD 290-580 or correctional labor for up to two years, arrest for up to six months, or limitation of freedom for up to three years. The same actions committed repeatedly, or in cases where they have caused substantial harm to the person's rights, are punished by arrest for three to six months, restriction of liberty for three to five years, or imprisonment for the same term;
- unauthorized interference in the operation of computers, automated systems, computer networks, or telecommunication networks, which leads to leakage, loss, forgery, blocking of information, distortion of the information processing, or violation of the established order of its routing is punished by a fine of approximately USD 350-580, limitation of freedom for two to five years, or imprisonment for up to three years, with or without deprivation of the right to hold certain positions or engage in certain activities for up to two years. The same actions committed repeatedly, or by a prior conspiracy of a group of persons, or in cases where they have caused substantial harm, are punished by imprisonment for three to six years with deprivation of the right to hold certain positions or engage in certain activities for up to three years.

The PDP also prescribes for private remedies:

- recovery of monetary and/or moral damages (civil action).

Non-legal: Reputational harm and, in turn, potential loss of customer confidence and business opportunities.

Are there any noticeable patterns or trends in how enforcement is carried out in Ukraine?

New challenges in data privacy and cybersecurity are associated with the ongoing Russia-Ukraine conflict, which has strengthened the issue of the need to protect personal data. Of particular note are changes regarding cloud services, processing of personal data during the period of martial law, providing medical services, and statistical activities.

The Commissioner is not very active with its enforcement activities at the moment because of the upcoming reform in the sphere of personal data protection. But gradually, the situation may change in the course of the next several years, depending on when the data privacy reform will be adopted and the National Commission for Personal Data Protection and Access to Public Information will be established.

How do emerging technologies such as AI, IoT, and blockchain impact data protection considerations in Ukraine?

According to a recently adopted Law of Ukraine "On advertising," providers of video-sharing and information-sharing platforms, as well as audio and audiovisual services providers, are prohibited from processing personal data collected or otherwise obtained from children for commercial purposes such as direct marketing and profiling, including behavioral advertising.

Are there any expected changes in data protection on the horizon in the next 12 months in Ukraine?

Given the significant changes in international and, in particular, European standards of personal data protection, the Ukrainian parliament has developed two draft laws aimed at implementing the General Data Protection Regulation (EU) 2016/679 (GDPR) and the modernized Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 108+ in Ukraine.

On October 25, 2022, the Parliament of Ukraine registered the draft law "On Personal Data Protection" No 8153 (Draft Law on PPD), and, on October 11, 2021, the draft law "On the National Commission for Personal Data Protection and Access to Public Information" No 6177 (Draft Law on the DPA).

The Draft Law on PPD proposes, in particular, the following legislative novelties:

- unified and extended terminology (new terms defined: biometric data, data breach, genetic data, health data, overall annual turnover, pseudo-anonymization, profiling, data processing at massive scales, etc.);
- new principles on data processing (lawfulness, fairness, transparency, data minimization, purpose limitation, accuracy, storage limitation, integrity and confidentiality, accountability, etc.);
- updated grounds of processing and new ground of processing "legitimate interest";
- updated consent concept with clarified ways on how consent could be obtained, when consent cannot be considered as granted, and restrictions to use consent as a

ground for processing when other grounds apply;
- updated concept of sensitive data with an extended list of grounds for processing such data.

In addition, the Draft Law on PPD:
- determines cases when representatives of controllers and processors not established in Ukraine shall be designated in Ukraine;
- prescribes the obligation of each controller (or the controller's representative) to maintain a record of processing activities under its responsibility;
- obliges controllers to conduct regular data protection impact assessments (DPIA). Where the processing would result in a high risk, the controller shall have prior consultation with the data protection authority;
- specifies cases when the controller and processor shall appoint data protection officers (DPO) along with qualification requirements for such officers.

The Draft Law on PPD also prescribes a completely new range of different administrative fines that may be imposed on natural and legal persons violating the data protection regulations. The amount of fines differs depending on the severity of violations. For the most severe violations, the fine framework might be up to 5% of the company's annual turnover, but not less than UAH 300,000 (approximately USD 10,100) per violation.

Turning to the second legislative initiative, the Draft Law on the DPA proposes to establish an independent government agency that would be responsible for both policymaking (adopting mandatory regulations) and enforcement (prosecuting infringers) in the sphere of data privacy and access to public information.

The National Commission for Personal Data Protection and Access to Public Information would have quasi-investigative functions and would be able to investigate violations with the help of experts in technology and other spheres.

The main powers of the DPA would be the following:
- obtain information necessary for its activities, including confidential and with restricted access, from any individual company or organization;
- receive access to information and telecommunication systems, registers, and data banks, including information with limited access – the owner (administrator) of which are state bodies or local authorities – using state, including government, means of communication and communications, special communication networks and other technical means;
- receive information from databases, and registers of foreign countries, including paid information, if that is required for access to information;
- investigate possible violations of the law of Ukraine "On Personal Data Protection" and the law of Ukraine "On Access to Public Information" based on complaints but also based on its own initiative;
- collect from government and private companies, organizations, employees, and individuals written explanations on the circumstances that may indicate a violation of the corresponding laws;
- apply to the courts for enforcement of corresponding laws;
- issue fines to controllers and processors of personal data;
- have access to personal data processed by the controller and/or processor and necessary for the performance of its duties.

The Draft Law on the DPA establishes new (additional) fines. The non-compliance with decisions/requests of the DPA and/or non-provision of the access of the DPA for the purposes of investigating the activities of the company or individual would result in:
- a fine in the amount of UAH 20,000 to UAH 100,000 (approximately USD 678 to USD 3,390) for individuals, and for legal entities in the amount of 0.5% to 1% of the total annual turnover of such legal entity for the previous year, but not less than 3,000 tax-free minimum incomes (approximately USD 1,729);
- a fine of 200% of the previous fine for each next non-compliance.

The Parliament is expected to adopt both drafts and other necessary regulatory norms to launch the data privacy reform as a part of the integration into the EU Digital Single Market, implementation of the EU legislation as required by the EU-Ukraine Association Agreement, and the wider government digital agenda. However, taking into account the martial law in Ukraine, it is not yet clear when these drafts will get back to the Parliament's agenda. ■

CEE
Legal Matters

www.ceelegalmatters.com