Poland


Jakub Gładkowski


Barbara Kieltyka


Malgorzata Kieltyka

Kieltyka Gladkowski KG Legal

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The main sources developing the idea of information protection indicated in Article 51 of the Polish Constitution include Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation – GDPR) and the Personal Data Protection Act, the aim of which is to supplement and clarify the provisions of the GDPR.

The GDPR and national law apply in parallel – the GDPR regulates the fundamental principles and rights, while the national law specifies exceptions and details in specific sectors.

In addition to the GDPR, Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to data (Data Act) is also key, as it aims to regulate access to **non-personal data**. This act, for example, regulates so-called "connected products", i.e. smart devices.

1.2 Is there any other general legislation that impacts data protection?

As an extension of the above regulations, the following acts also structurally influence the condition of data circulation:

a. Polish Act on the Protection of Personal Data Processed in Connection with the Prevention and Combating of Crime.
b. Polish Electronic Communications Act.
c. Polish Act on the Protection of Databases.
d. Polish Act on the exchange of information with law enforcement authorities of EU Member States, third countries, EU agencies and international organisations.
e. Polish Act on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System.
f. Polish Act on the Processing of Criminal Information.

1.3 Is there any sector-specific legislation that impacts data protection?

A key example of the dynamic construction of the sectoral structure of regulations is the health service, which includes the Polish Act on Patients' Rights and the Patient's Rights Ombudsman, as it defines the rules for processing medical documentation and protecting sensitive health data, which is currently being covered by the latest data protection umbrella in the comprehensive initiative of Regulation (EU) 2025/327 of the European Parliament and of the Council on the European Health Data Space. The Polish Act on the Health Information System is also important, as it regulates the functioning of IT systems in healthcare, including e-prescriptions, e-referrals, and the Patient's Internet Account (IKP).

The second striking example of a comprehensive approach to data protection is the banking and finance sector. In this sector, going beyond cybersecurity issues, it is worth mentioning the Polish Banking Law, which concerns the processing of data in connection with the functioning of the banking system, and the Act on Combating Money Laundering and Terrorist Financing (implementing the AML Directive), because it imposes identification obligations and those related to transaction monitoring.

The cross-sectional approach is presented by the Polish employment law system, in which the provisions of the Polish Labor Code, which regulates employee data in the work environment, have a key place. These provisions include sources of whistleblower regulation.

Another obvious example is telecommunications and the Internet, and in this respect, the new Polish Electronic Communications Law, which implements Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and the Polish Act on the provision of services by electronic means.

The insurance sector also regulates data, including Polish Act on Insurance and Reinsurance Activities, which provides for the rules for processing personal data of insurers' customers, including health data (e.g. for life insurance policies).

Important legislation from a cross-border perspective in the EU includes the Transport and urban monitoring law, which has important sectoral provisions, including local regulations, and the Act on road transport and public transport, which containing regulations on the processing of passenger data (e.g. in ticket systems) and monitoring in public transport.

1.4 What authority(ies) are responsible for data protection?

In Polish jurisdiction, the President of the Personal Data Protection Office is a state body with the rank of a minister, responsible for supervising the compliance of personal data processing with applicable legal regulations in Poland. His competences include, among others, conducting control proceedings, considering complaints regarding violations of

data protection regulations, as well as issuing administrative decisions in this regard. Decisions may be appealed to an administrative court.

The President manages the work of the Personal Data Protection Office, which has its seat in Warsaw. The legal basis for the establishment of this body is Article 34 of the Personal Data Protection Act.

As for other supervisory authorities (in the EU), the Polish supervisory authority cooperates with the authorities of the 27 EU countries through the European Data Protection Board (EDPB) – the body coordinating the application of the GDPR at the level of the entire Union. The EDPB is an independent body of the EU responsible for the consistent application of the GDPR in all EU Member States since 25 May 2018. It was established under Article 68 of the GDPR and replaced the Article 29 Working Party. For example, the EDPB issues guidelines and recommendations on the application of the GDPR, the most recent of which are Guidelines 02/2025 on processing of personal data through blockchain technologies.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**
  Personal data is any information relating to an identified or identifiable natural person ("data subject"); the main definition includes an open catalogue of identifiers. The definition is constantly being improved by the EDPB in the context of the needs of new technologies. The latest guidelines clarify the definition for AI models and include as personal data information that contributes to the identification of a natural person in the context of the operation of technology and software (e.g. consumer profile, risk category, result of a predictive model).
- **"Processing"**
  Processing means any operation or set of operations that is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **"Controller"**
  The controller is generally a natural or legal person, public authority, entity or other entity that, alone or jointly with others, determines the purposes and means of processing personal data.
- **"Processor"**
  The processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- **"Data Subject"**
  A natural person whose personal data is processed by the controller or processor. This is a differently identified or identifiable natural person based on information as a result of data processing. An example would be a customer, employee, website visitor, prospective customer, patient, student, user, or subscriber.
- **"Sensitive Personal Data"/"Special Categories of Personal Data"**
  Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data used to uniquely identify a natural person, data concerning health, sexuality or sexual orientation of that person.
- **"Data Breach"**
  A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Other key definitions**
  The above key definitions are created using vague and undefined terms (e.g. "**automated**"). This causes complications in determining the lawfulness of data processing based on the key definitions. Therefore, there are additional definitions, referring to the lawful process of processing or working with data, which define terms such as, for example: "pseudonymization"; "directly or indirectly identifying a person"; "profiling" (the definition emphasises the automation of data processing in order to assess personal factors); or "Automated Decision-Making". The correction of basic concepts is introduced by periodic interpretative documents of the EDPB. Official documents, such as Guidelines 02/2025 on the processing of personal data through blockchain technologies, make it easier to explain whether, for example, recording data in a blockchain (e.g. signing a contract, placing an order) as a form of recording and sharing data, practically falls within the general definition of data processing under the GDPR (the full text Guidelines can be found at https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en).

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The main data protection provisions apply when an entity processes personal data and is headquartered in the EU, regardless of where the data is actually processed.

In Poland, personal data protection is regulated mainly by the EU GDPR, as well as the Personal Data Protection Act, and applies to companies outside the EU in the following two cases:

a. When they offer goods or services to individuals in the EU (even free of charge).
b. When they monitor the behaviour of individuals within the EU.

The legal basis for this approach is Article 3 of the GDPR.

An obvious practical case is an American company running an online store offering products to customers in Poland.

It should be noted that data protection regulations for both personal and non-personal data can be applied to the common practices of web scraping, i.e. working on data, collecting data using an automatic method, processing data, and parsing data, especially if the entity is headquartered in one country (even outside the EU), the software developers have a base in another country, or the data is collected globally and then sent to a server in yet another jurisdiction.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes, the GDPR provides for the exclusion of certain personal data processing activities from its scope. According to Article 2(2) of the GDPR, the provisions of the Regulation do not apply to the processing of personal data in the following situations:

- Processing of data by a natural person as part of activities of a purely personal or household nature (e.g. maintaining a private calendar with contact details).
- Processing of data as part of activities unrelated to EU law (e.g. activities within the framework of national security).
- Processing by EU institutions within the scope of their official functions (regulated in separate legal acts).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The principle of transparency is one of the fundamental principles of data processing. It is often referred to in the preamble and articles of the GDPR. The fundamental provision of Article 5(1)(A) of the GDPR focuses on the perspective of transparency **from the point of view** of the data subject ("lawfulness, fairness and transparency").
  According to the preliminary provisions of this EU regulation, *it should be transparent for individuals that personal data relating to them are being collected, used, accessed or otherwise processed and to what extent such personal data are or will be processed*. Any information related to the processing of such personal data should be easily accessible and understandable and should be presented in clear and plain language.
  Furthermore, the principle of transparency requires that any information provided to the public or to data subjects must be concise, easily accessible and understandable, using clear and plain language and, where appropriate, enhanced with visual elements.
  In the context of non-personal data, the Data Act also operates on the basis of transparency standards in the relationship between users and entrepreneurs. A key aspect of the transparency principle is the clarity and readability of contracts and trade secrets. The Data Act obliges entrepreneurs to present the conditions for data processing in a way that is understandable and transparent for users. Articles 13 and 14 of the Data Act are important, as well as the implementation of the rights of natural persons (Articles 15–22 and 34 of the Data Act).
  Transparency is an important argument in the decisions of supervisory authorities. For example, in case *ZSPR.440.1055.2019* of 5 July 2022, the lack of response from the data controller was considered by the Polish authority to be a violation of the principle of transparency and the information obligation towards the data subject.
- **Lawful basis for processing**
  The legal basis for the processing of personal data is set out in detail in Article 6(1) of the GDPR. Data processing is lawful only if at least one of the following conditions is met:
  - consent of the data subject – processing is based on the voluntary, specific, informed and unambiguous consent expressed by the data subject;
  - performance of the contract – processing is necessary for the performance of the contract;
  - legal obligation incumbent on the administrator (e.g. resulting from tax regulations, labour law);
  - protection of the vital interests of a natural person;
  - performance of a task carried out in the public interest or in the exercise of public authority; and
  - legitimate interest of the administrator or a third party.
- **Purpose limitation**
  It is expressed in Article 5(1)(B) of the GDPR. It states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered incompatible with the original purposes under Article 89(1).
  This principle means, in particular, that the purpose must be specified **before** the processing begins. The controller is not entitled to collect personal data without a clear reason. In addition, the purpose must be clear and lawful – it cannot be hidden, vague or unlawful.
  In the Data Act, the purpose limitation principle is implicitly but explicitly expressed, especially in the context of access, sharing and reuse of data. Similar to the GDPR, this principle aims to ensure that data is used only for specific, clearly defined and legitimate purposes that have been made known to the user.
- **Data minimisation**
  The principle of data minimisation is set out in Article 5(1)(C) of the GDPR. It means that personal data must be *adequate, relevant and limited to what is necessary* for the clearly defined purposes for which they are processed. Data controllers should therefore not collect or process more data than is necessary to achieve a specific purpose. The principle of data minimisation for establishing a relationship between the purpose and the scope of data processing means two requirements:
  a. limiting the collection of data to only that which is necessary to achieve the purpose; and
  b. the need to delete data when it becomes unnecessary to achieve the purpose of processing.

  The principle of data minimisation is developed in Article 25 of the GDPR, concerning data protection by design and by default. According to this provision, the controller is obliged to implement appropriate technical and organisational measures (e.g. pseudonymisation) at the planning stage of processing, which are intended to effectively implement the principles of data protection, including minimisation.
- **Proportionality**
  In practice, this principle means that the measures taken by the controller must be *appropriate, necessary and not go beyond what is necessary* to achieve the legitimate purpose of processing personal data. Data should not be collected or processed to a greater extent than is necessary to achieve that purpose.
- **Retention**
  The principle of limiting the storage of personal data, expressed in Article 5(1)(E) of the GDPR, imposes on the controller the obligation to store data only for a period no longer than necessary to achieve the purposes for which the data were collected. Personal data should be processed in a form that allows the identification of the

person to whom they relate, only for the time needed to achieve the originally specified purpose, and, after its completion, should be deleted, anonymised or properly archived. An exception to this principle would be situations in which data are stored longer exclusively for archival purposes in the public interest, scientific, historical or statistical research.

Although the Data Act does not contain a direct reference to the principle of limiting data storage, it does establish a number of regulations that, in practice, implement this principle in relation to personal and non-personal data. In particular, the Data Act provides that data may be used and shared only to the extent necessary to achieve specified and agreed purposes. This means that, after these purposes have been achieved, the data should not be further stored or processed, unless there is an express legal or contractual basis for doing so.

Due to the immutable nature of the blockchain, the EDPB in its Guidelines 02/2025 draws attention to the difficulties in implementing the principle of storage limitation, which requires that personal data be stored only for the period necessary to achieve the purposes for which they were collected. The Guidelines suggest that personal data should be stored outside the blockchain (off-chain) or at least in a form that prevents the identification of the data subjects. If it is necessary to store data on the blockchain for its entire existence, the data controller must demonstrate that this is proportionate to the purpose of the processing and document this decision accordingly.

In cases where it is technically impossible to delete data from the blockchain, the EDPB recommends using technical measures such as pseudonymisation, encryption or storing data in the form of cryptographic hashes to minimise the risk of violating the rights of data subjects.

- **Accuracy**

  The principle of accuracy is expressly anchored in Article 5(1)(D) of the GDPR. According to its wording, personal data must be accurate and, where necessary, kept up to date, and controllers should take all reasonable steps to ensure that data that are inaccurate, in light of the purposes of their processing, are promptly rectified or erased. It is also important for the controller to take all reasonable steps to erase or rectify data that are inaccurate in light of the purposes of their processing.

  Although the Data Act does not directly reference the principle of accuracy within the meaning of the GDPR, it is implied. In particular, this concerns the obligation to ensure the quality, integrity and reliability of data shared within the framework of data sharing between private entities (B2B), public entities (B2G) and users. In this context, data must be accurate because they are the basis for further analyses or decision-making models or used by AI systems.

- *Other key principles (e.g., Accountability) – please specify*

  The principles of integrity and confidentiality and accountability are key elements of the personal data protection system in the EU.

  The principle of **integrity and confidentiality** has been formulated in Article 5(1)(F) of the GDPR, according to which personal data should be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This means that the need to ensure the integrity (inviolability) of data and their confidentiality (protection against access by unauthorised persons). Controllers and processors are obliged to implement data protection measures by design and by default, in accordance with Article 25 of the GDPR.

  The principle of **accountability**, regulated in Article 5(2) of the GDPR, means that the controller must not only comply with the principles of personal data protection, but also be able to demonstrate compliance with them. In other words, accountability is the ability of the controller to document and prove that it has implemented appropriate organisational and technical measures to ensure compliance with the provisions of the GDPR.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**

  The right to access can be divided into the right to obtain information and the right to a copy of data. Based on Article 15 of the GDPR, each data subject may request the data controller to exercise the right to access. This provision entitles the entity to obtain information as to whether their personal data are actually being processed. If the data are being processed, the person requesting information may obtain, among other things, such information as:

  1. purposes of processing;
  2. the categories of personal data concerned;
  3. recipient information;
  4. where possible, the planned period for which personal data will be stored;
  5. information about the right to request that the controller rectify, delete or limit the processing of data; and
  6. information on automated decision-making, including profiling.

- **Right to rectification of errors**

  In the EU Regulation, the right to rectification of data is included in the provision of Article 16, which indicates that the data subject has the right to demand that the controller immediately rectify personal data concerning him or her that are incorrect. Taking into account the purposes of processing, the data subject has the right to demand that incomplete personal data be supplemented, including by submitting an additional declaration.

  Data rectification may also take place on the basis of proceedings conducted by the President of the Personal Data Protection Office.

- **Right to deletion/right to be forgotten**

  Information on the right to be forgotten appears in the recitals of the GDPR and directly in the provision of the Regulation. In Recital 66 of the GDPR, the emphasis is on strengthening the right to be forgotten on the Internet, and this is to be served by extending the right to erasure by obliging the controller (who has made this personal data public) to inform controllers (who process such personal data) to erase all links to this data, copies of this personal data or replications of it.

  Article 17, in turn, indicates that the data subject has the right to demand that the controller delete his or her personal data without delay, and the controller is obliged to delete personal data without undue delay if one of the following circumstances applies:

1. personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
2. the data subject has withdrawn the consent on which the processing is based;
3. the data subject files an objection;
4. personal data were processed unlawfully; and
5. personal data must be erased in order to comply with a legal obligation under Union law or the law of the Member State to which the controller is subject.

- **Right to object to processing**
  According to Article 21 of the GDPR, the data subject is entitled to file an objection. From the moment the objection is filed, the controller is not allowed to process this personal data, except in cases where the controller demonstrates that there are important legitimate grounds for processing, overriding the interests of the rights and freedoms of the data subject or grounds for establishing, pursuing or defending claims. This article also regulates the objection to the use of personal data for direct marketing purposes.
- **Right to restrict processing**
  The right to restrict the processing of personal data is included in Article 18 of the GDPR. According to this provision, the data subject may request the controller to restrict the processing of data in cases such as:
  1. questioning the accuracy of personal data – for a period enabling the administrator to check the accuracy of such data;
  2. when the processing is unlawful and the data subject opposes the deletion of personal data and requests the restriction of their use instead; and
  3. the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims.
- **Right to data portability**
  The right to data portability is regulated in Article 20 of the GDPR. According to this regulation, the data subject has the right to receive the personal data concerning him or her, which he or she has previously provided to the controller, in a commonly used format. The data subject has the right to transmit this data to another controller if:
  1. the processing is based on consent or contract; and
  2. the processing is carried out in an automated manner.
- **Right to withdraw consent**
  The data subject has the right to withdraw previously expressed consent at any time. However, withdrawing consent does not affect the lawfulness of processing that took place before the consent was withdrawn, and the person who consents to the processing of data is informed of this fact before giving consent. The process of withdrawing consent must be as easy as giving it.
- **Right to object to marketing**
  The architecture of the Regulation means that, in the context of the objection principles, marketing should be viewed as a qualified form of general objection to data processing, in this case for marketing purposes.
  This is confirmed by the position of the President of the Personal Data Protection Office, who issued guidelines that if a person's data are used for marketing purposes, i.e. to present them with an offer of goods or services, they may object to this at any time and if such an objection occurs, their data may no longer be used for such purposes.
- **Right protecting against solely automated decision-making and profiling**
  The process of automated decision-making assumes the exclusion of the human factor, and the processing of personal data is carried out using appropriate technical tools, including AI. This process may, but does not have to, involve profiling.
  The data subject (Article 22 of the GDPR) has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects the data subject in a similar manner. The application of this right does not apply where such processing: is necessary for entering into, or the performance of, a contract between the data subject and the controller; is permitted by Union or Member State law to which the controller is subject and which lays down suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject; or is based on the explicit consent of the data subject.
- **Right to complain to the relevant data protection authority(ies)**
  Legal remedies, liability and sanctions are set out in Chapter VIII of the GDPR, which defines the right to lodge a complaint with a supervisory authority. Every data subject has the right to lodge a complaint with a supervisory authority if they believe that the processing of personal data concerning them infringes the general regulation on personal data. The supervisory authority to which the complaint has been lodged is obliged to inform the complainant about the progress and results of the complaint, including the possibility of seeking a judicial remedy against a legally binding decision of the supervisory authority concerning them.
- *Other key rights (e.g., Right to compensation) – please specify*
  According to Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of a breach of the provisions of the GDPR has the right to obtain compensation for the damage suffered from the controller or processor. It should therefore be noted that in the case of compensation, it may be both material and non-material damage.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Yes. Polish procedural law, such as Article 8 of the Polish Civil Procedure Code or Article 31 of the Polish Code of Administrative Procedure, allows for the possibility of active action to protect the rights of a citizen, including initiating proceedings or admitting to participate in ongoing proceedings. It is important that this is justified by the statutory objectives of such an organisation. In Poland, Non-Governmental Organisations operate mainly in the form of associations and foundations and, in such cases, their objectives (data protection and active participation in individual cases) must be clearly and precisely indicated in their statute registered before the supervisory body.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The processing of children's personal data:

- requires special protection (Recital 38 of the GDPR);
- all information and communications should be worded in such clear and simple language that a child can easily understand them (Recital 58 of the GDPR);
- processing classified as "profiling" should not involve children (Recital 71 of the GDPR); and
- in the case of information society services, the minimum age of consent is 16 years (Article 8 of the GDPR), unless a Member State has set a lower age (at least 13 years).

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no general obligation to register personal data processing activities with the supervisory authority. Current regulations and procedures are based on the responsibility of data controllers and the principle of so-called "accountability".

GDPR

- It does not provide for a general obligation to register personal data sets with the supervisory authority.
- It introduced the obligation to keep a register of personal data processing activities. This obligation applies to:
  - All data controllers and processors employing more than 250 people.
  - Smaller entities, if the processing is not occasional, concerns sensitive data or may result in a risk to the rights and freedoms of natural persons (Article 30 of the GDPR).

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

- Article 30 of the GDPR imposes an obligation to maintain a register of processing activities by data controllers and – to the extent appropriate – also by processors. Although this is not a public register or one requiring notification to the supervisory authority, its scope is clearly defined and is of a detailed nature.
- When maintaining such a register, the data controller must include in it, among others:
  - Name and surname or name and contact details of the controller and – if any – the joint controllers, the controller's representative and the Data Protection Officer (DPO).
  - Processing purposes and other information.
- Similarly, the processor must keep a register that includes the data of the controller, the categories of processing carried out on its behalf, information on international data transfers and the security measures applied.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Although the register of processing activities is not subject to notification to the supervisory authority, their internal structure is based on a set of key categories of information. These categories determine how the register is kept and include: legal entity (controller/processor); purpose of processing; category of data; system or database; and data subjects:

- Article 30 of the GDPR introduces the obligation to keep a register of processing activities, which is a basic documentation instrument for administrators and processors.
- It is crucial that the register is kept in relation to a specific administrator or processor, which means that the organisational criterion is the legal entity that is the party responsible for the processing.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

- According to Article 30 of the GDPR, the central category of entities obliged to keep a register of processing activities is the personal data controller. This obligation also applies to the processor, i.e. the one who processes data on behalf of the controller.
- In practice, the following entities are obliged to maintain the register:
  - Local legal entities established in a given EU Member State.
  - Foreign legal entities if they process personal data of persons located in the territory of the EU and offer them goods or services or monitor their behaviour (pursuant to Article 3(2) of the GDPR).
  - Representative offices or branches of foreign entities if, as part of their activities, they process data of natural persons from the EU and are subject to the provisions of the GDPR.
- The GDPR introduces the so-called "**principle of territorial extension of application**" – controllers and processors outside the EU are covered by the obligations of the GDPR if their activities cover persons located in the Union.
- In such cases, in accordance with Article 27 of the GDPR, they are obliged to appoint a representative in the EU who becomes the formal link with the supervisory authority (in Poland, the President of the Personal Data Protection Office).
- A representative within the meaning of Article 27 of the GDPR acts on behalf of a controller or processor not established in the EU but whose activities are subject to the GDPR.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

- The basic information that must be included in the register is the identification data of the data controller or – in the case of a register kept by a processor – its data and the data of the controller on whose behalf it acts. In particular, these should be:
  - Full name of the entity.
  - Registered office address.
  - Contact details (telephone number, e-mail address, etc.).
  - If appointed, contact details of the DPO.

  - In the case of controllers or processors outside the EU, details of the representative designated in accordance with Article 27 of the GDPR.
- The register must contain a detailed description of the purposes for which personal data are processed. Examples of purposes include: recruitment; HR services; and direct marketing.
- The administrator should determine which groups of natural persons are covered by data processing.
- The administrator should also specify what type of personal data is being processed. These may include:
  - Identification data (name, surname, Personal Identification Number, Tax Number, ID card number).
  - Contact details (address, telephone number, e-mail address).
  - Location data.
  - Health data (special category of data).
- Indication of the categories of recipients to whom the data are or may be disclosed is also required.

7.6 What are the sanctions for failure to register/notify where required?

- Pursuant to Article 83(4)(A) of the GDPR, infringement of the obligations under Article 30 is subject to administrative fines of up to EUR 10,000,000 or – in the case of an undertaking – up to 2% of the total annual worldwide turnover of the previous financial year, whichever is higher.
- Lack of a register can be classified as:
  - Infringement of the administrator's obligations arising from the accountability principle (Article 5(2) of the GDPR).

In one of the decisions of the President of the Personal Data Protection Office (*DKN.5112.14.2022*), a company was fined as much as EUR 132,000 for serious violations of the provisions of the GDPR. The main violation was the failure to include profiling operations in the register of processing activities, which was a violation of Article 30(1) of the GDPR.

7.7 What is the fee per registration/notification (if applicable)?

- The GDPR does not provide for a fee for registration or reporting the processing of personal data to the supervisory authority.

Act of 10 May 2018 on the Protection of Personal Data

- The Act does not introduce any obligation to register data sets or any fees related thereto.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

- The applicable regulations impose on data controllers and processors a continuous obligation to maintain up-to-date documentation regarding data processing, which in practice fulfils the function of accountability and compliance control.
- The document for internal documentation of processing activities is not subject to formal "registration" with the office nor does it require renewal in any time cycles.
- Data administrators are obliged to keep the register up to date.
- The GDPR requires that the register of processing activities be always up to date and available to the supervisory authority (e.g. the President of the Personal Data Protection Office) upon request.

7.9 Is any prior approval required from the data protection regulator?

- As a rule, prior approval by the supervisory authority for personal data protection (in Poland, the President of the Personal Data Protection Office) is not required before data processing begins.
- However, there are exceptional situations in which prior consultation with the supervisory authority **may be mandatory**. However, these are clearly defined and are of a **supplementary nature**, rather than universal.
- The GDPR does not provide for a general obligation to obtain prior approval from a supervisory authority. Instead, the institution of prior consultation with the supervisory authority has been established (Article 36 of the GDPR), which applies only in situations of particular risk to the rights and freedoms of natural persons.
- Pursuant to Article 36 of the GDPR, where a data protection impact assessment (DPIA) pursuant to Article 35 of the GDPR indicates a high risk to the rights and freedoms of individuals, and the controller is unable to mitigate the risk by appropriate measures, the controller is required to consult the supervisory authority prior to processing.
- Examples of such cases include large-scale monitoring of public spaces (e.g. facial recognition systems), profiling that produces legal effects for individuals, or processing sensitive data (e.g. health, political opinions) in innovative or unusual contexts.

7.10 Can the registration/notification be completed online?

Currently, the personal data controller does not have to "report" anything to the data protection authority before starting to process data, apart from exceptions that concern, among others, high risk and the need for prior consultations (Article 36 of the GDPR). In the supplementary Polish law, electronic channels of contact have been created, including the Electronic Platform of Public Administration Services (EPUAP) – it is possible to submit notifications, inquiries and applications electronically.

7.11 Is there a publicly available list of completed registrations/notifications?

- There are legal regulations that provide for the possibility of sharing information on registrations or notifications regarding the processing of personal data, but the availability of this information depends on the legal context and the type of notification.
- The GDPR does not provide for a publicly available register that would contain information on all notifications or registrations made by data controllers.

7.12 How long does a typical registration/notification process take?

- There is currently no typical formal registration process that ends with confirmation by a supervisory authority.
- In some cases, we can speak of reporting activities or formal procedures.
- Pursuant to Article 30 of the GDPR, each data controller and, where necessary, the data processor, is obliged to keep a register of data processing activities.
- The time required to prepare such a document depends on the complexity of the processing processes in a given organisation, the number of processing operations, the IT systems involved, as well as the experience of the data protection team.
  - For a small organisation, preparing a complete register may take several days to several weeks.
  - In the case of large companies or public entities, where we are dealing with many departments, processing entities and a variety of data, the process may take several months.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

In accordance with Article 37 of the GDPR and Article 9 of the Act of 10 May 2018 on the Protection of Personal Data, the appointment of a DPO is mandatory in three situations:

1. When the processing is carried out by a public authority or a public body (except courts within the scope of their judicial activity).
2. Where the core activity of the controller or processor consists in the **regular and systematic** monitoring of individuals on a large scale.
3. Where the **core** activity consists of **processing special categories of data** (e.g. health data) or criminal conviction data on a large scale.

In other cases, the appointment of a DPO is optional but recommended as good practice.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO where this is mandatory constitutes a breach of the GDPR, which may result in the imposition of an administrative fine.

According to Article 83(4)(A) of the GDPR, the fine may amount to up to EUR 10 million or up to 2% of the company's annual worldwide turnover, whichever is higher.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Yes. Article 38(3) of the GDPR guarantees that the DPO cannot be dismissed or penalised for performing his or her duties.

The DPO must act independently and may not receive instructions on to how to perform his or her duties. The employer may not hold him or her liable for any negative consequences for actions taken in accordance with data protection regulations.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes. According to Article 37(2) of the GDPR, one DPO may be appointed for a group of undertakings or several public authorities/entities, provided that he or she is easily accessible from any place of business. In practice, this means, among other things, the possibility of contact in the local language and accessibility for data subjects.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The GDPR does not specify any specific education or certificates, but Article 37(5) states that the DPO should have appropriate professional knowledge of personal data protection laws and practices and the ability to fulfil the obligations arising from the GDPR.

In practice, experience, knowledge of law and IT systems count, especially in the case of large or complex organisations.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Article 39 of the GDPR specifies the main tasks of the DPO and the manner of their implementation. The GDPR provides that the DPO is to perform an advisory and supervisory function in the organisation, and its main purpose is to support the data controller and the data processor in ensuring compliance of the processing of personal data with the law.

The basic tasks of the DPO include informing and advising the controller, the processor and the persons who process data, regarding their obligations under the GDPR and other data protection regulations.

Another obligation of the DPO is to support the controller in carrying out DPIA in cases of processing that poses a high risk to the rights and freedoms of natural persons.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes. In accordance with Article 10 of the Personal Data Protection Act, the data controller is obliged to report the DPO's contact details to the President of the Personal Data Protection Office.

The notification is made electronically via a form available on the Personal Data Protection Office website.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes. Articles 13 and 14 of the GDPR require the controller to provide the DPO's contact details in information clauses and documents such as privacy policies.

The purpose of this obligation is to ensure that individuals have easy access to the DPO in the event of questions or requests regarding the processing of personal data.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

In accordance with the GDPR, if a company (data controller) entrusts the processing of personal data to an entity processing on its behalf, a personal data processing agreement is mandatory.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Article 28(3) of the GDPR sets out the essential elements of such an agreement:

- it should be specified in detail for what purpose personal data are processed and to what extent (e.g. customer or employee data);
- the processor may only process data in the manner specified by the data controller in the form of written instructions. The processor may not arbitrarily change the purpose or method of processing; and
- the processor is obliged to implement appropriate technical and organisational measures to ensure the security of the processed data (Article 32 of the GDPR). Data protection measures, such as encryption, pseudonymisation of data, protection against unauthorised access, etc., must be specified.

The agreement should also include, among other things, appropriate technical and organisational measures to protect data against unauthorised access, loss or destruction.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The prior consent of the subscriber or end user is, in accordance with the **new** Polish regulation, the basic requirement for the legality of sending commercial information, including direct marketing using automatic calling systems or telecommunications terminal equipment, particularly within the framework of using interpersonal communication services (Article 398 of the Polish Electronic Communications Law).

In the context of the GDPR, electronic marketing as the processing of personal data for marketing purposes (including sending e-mails and text messages) is only legal if the data subject has voluntarily consented to it. This means that the consent to the processing of data for marketing purposes must be given by the data subject (so-called "informed and voluntary consent").

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Yes, the new Polish regulations also apply to B2B marketing, because they refer to the end user without distinction as a private entity or a business entity. The transmission of commercial information, including direct marketing using telecommunications terminal equipment and automated calling systems, is only permissible on the basis of prior consent of the end user or subscriber. This applies to both end users who are natural persons and organisational units.

The prohibition of sending unsolicited commercial and marketing information, mainly by e-mail (spam), but also by telephone and other forms of automated calling systems, applies to messages addressed to a specific recipient: subscriber; or end user.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Direct marketing is all activities, as well as any related ancillary services , enabling the offering of products or services or the transmission of other information to a group of people – by post, telephone or other direct means – for the purpose of informing them or eliciting a response from the data subject.

The entrepreneur is not allowed to send communications for marketing purposes to the subscriber/consumer without first obtaining consent to such contact.

Automatic calling systems are automated voice communication connections that connect to the end user and transmit a previously prepared recording. Similarly, these may be other messages. Direct marketing and sending unsolicited commercial information may take place in various forms, in particular: e-mail messages; telephone calls to end users; SMS or MMS messages; and any other forms of communication. The **prior consent** of the marketing recipient **is required** for such direct marketing.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Determining whether information is being sent to a subscriber or end user requires analysis of the address information used to send the information. The marking may use any number or individual electronic address used in electronic communications.

The above restrictions on electronic, telephone and postal marketing therefore also apply to marketing sent from other jurisdictions if the recipient is located in Poland or the EU.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, the following are appropriate for enforcing violations of marketing restrictions:

1. The President of the Office of Electronic Communications, who conducts proceedings to impose a fine against an entity that uses automatic calling systems or uses telecommunications terminal equipment for the purpose of sending commercial information without prior consent of the subscriber or end user (Article 444, paragraph 1, point 81 of the Polish Electronic Communications Law).
2. The President of the Personal Data Protection Office, who conducts proceedings to impose a fine against an entity that fails to fulfil the obligation to implement technical

and organisational protection measures or the information obligation.

3. The President of the Office of Competition and Consumer Protection, because in accordance with the new provision 398, section 4 of the Polish Electronic Communications Law, illegal marketing constitutes an act of unfair competition.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Buying marketing lists from third parties is not strictly prohibited. The requirement for legality is to exercise special caution and comply with the relevant legal regulations.

a. In the case of purchasing marketing lists, the basic requirement is to ensure that the persons on such a list have consented to the processing of their personal data for marketing purposes (Article 6(1) of the GDPR).
b. It is important to have an agreement with a third party (processor) that provides such lists.
c. Before purchasing marketing lists, a risk assessment should be conducted and it should be ensured that opt-out rights are respected.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

As of December 2019, pursuant to Article 445 of the Polish Electronic Communications Law, the President of the Personal Data Protection Office may, by way of a decision, impose a fine of up to 3% of the revenue of the penalised entity achieved in the previous calendar year.

Moreover, illegal use of automatic calling systems or use of telecommunications terminal equipment for the purpose of sending commercial information without prior consent of the subscriber or end user is an act for which a fine calculated on the same basis of 3% is also imposed by the President of the Office of Electronic Communications. It also takes into account the average revenue achieved by a given entity in the three consecutive calendar years preceding the year in which the fine was imposed (Article 446 of the Polish Electronic Communications Law).

Moreover, in the case of spam, the new electronic communications law provides for the possibility of initiating a fine mechanism within the meaning of classic criminal law (Article 448).

The provisions of the GDPR regarding sanctions remain in force, and a separate issue is financial sanctions in the case of proceedings for acts of unfair competition before the Polish Office for Consumer Protection and Competition.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

In accordance with the new Article 399 of the Polish Electronic Communications Law, the use of cookies and other similar technologies that involve storing information or accessing information already stored in the telecommunications terminal equipment (such as a telephone, computer or tablet) of the subscriber or end user is permitted, **provided that**:

a. the subscriber or end user will be informed in advance in a clear, easy and understandable manner about: the purpose of storing and accessing this information; and the possibility of specifying the conditions for storing or accessing this information by means of software settings installed on the telecommunications terminal device used by him, her, or the configuration of the service;
b. the subscriber or end user, after receiving the said information, consents thereto; and
c. the stored information or accessing it does not cause any configuration changes in the end user's telecommunications terminal device and the software installed on that device.

In addition, if personal data of users are processed as part of cookies, the GDPR rules on data processing are applicable, including consent, which must be voluntary, specific, conscious and unambiguous, and expressed through active action, e.g. clicking the appropriate acceptance button.

In addition, the EDPB in its Guidelines 05/2020 indicated that the use of so-called "cookie walls" (blocking access to the website without accepting cookies) is inconsistent with the GDPR because it does not provide the user with free choice.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

It is assumed that the new provision mentioned above introducing restrictions on such direct marketing covers all information that is stored in the telecommunications terminal equipment of the subscriber or end user by entities providing telecommunications services or services by electronic means. Therefore, it is indifferent in this respect to distinguish between: essential cookies; functional cookies; analytical (statistical) cookies; and advertising (marketing) cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Looking at the Polish jurisdiction from the perspective of one of the 27 members of the EU, the greatest potential threat is due to the activity of the most high-profile cases in Europe: *Google LLC* – a fine of EUR 60 million for failing to obtain users' consent to save advertising cookies; an*d Microso*ft – a fine of EUR 60 million for failing to collect consent from users from France before placing advertising cookies.

As far as the Polish authority is concerned, one can indicate such actions as warning decisions of the Polish authority for failure to receive the relevant end-user consents (an example of an admonition judicially verified by the Polish Voivodship Administrative Court in Warsaw, reference number: II SA/WA 3993/21).

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Under Article 446 of the Polish Electronic Communications Law, the President of the Office of Electronic Communications may, by way of a decision, impose a fine of up to 3% of the revenue of the penalised entity achieved in the previous calendar year.

Moreover, the illegal use of cookies is an act in respect of which the powers of the President of the Polish Office of

Electronic Communications also apply to the President of the Office for Personal Data Protection.

The provisions of the GDPR sanctions remain in force, which is a controversial issue in light of the case law of the Polish Administrative Court (perhaps not every cookie file is personal data).

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

According to the GDPR, the transfer of personal data to third countries (outside the European Economic Area – EEA) is only permitted if:

- the European Commission (EC) has issued a decision stating the adequate level of data protection in a given country (so-called "adequacy decision"); or
- other mechanisms provided for in Chapter V of the GDPR have been used (e.g. standard contractual clauses (SCCs), binding corporate rules (BCR)).

If none of these conditions are met, the transfer of data is generally prohibited.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The most commonly used mechanisms are:

- SCCs approved by the EC.
- The consent of the data subject, given after being informed about the risks.
- Execution of a contract between the controller and the data subject (or taking steps prior to entering into a contract).
- BCR for international capital groups.
- Exceptions provided for in Article 49 of the GDPR, e.g. important reasons of public interest.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

In most cases, prior approval by a supervisory authority is not required if the transfer is based on:

- EC adequacy decision.
- SCCs or BCR (if already approved).

The consent of the supervisory authority may be required if:

- the administrator relies on so-called "*ad hoc* contractual clauses" that have not been approved; or
- wants to rely on so-called "one-off exceptions" (e.g. occasional transfers in the legitimate interest of the controller).

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Transfer impact assessment (TIA) is mandatory:

- when transferring personal data to a country without an adequacy decision from the EC;
- when using SCCs or other mechanisms; and
- when the recipient country's laws may undermine GDPR's protections.

A TIA includes an assessment of whether the law of the recipient country does not effectively limit the enforcement of natural persons' rights and whether additional protection measures are needed (e.g. encryption, pseudonymisation, end-to-end encryption).

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C 311/18)?

The Personal Data Protection Office, following the EDPB, indicated:

- controllers must independently assess the level of protection in a third country;
- even when using SCCs, it is necessary to apply additional technical and organisational measures if the recipient's law does not provide equivalent protection; and
- the need to conduct a TIA and document the risk assessment.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The Personal Data Protection Office supports the use of new SCCs published by the EC on 4 June 2021.

Recommendations:

- conducting a TIA before implementing SCCs;
- adapting clauses to a specific transfer case (selecting appropriate SCC modules);
- assessment of the adequacy of technical measures (e.g. encryption); and
- maintaining documentation of transfer decisions (accountability principle).

Following the *Schrems II* decision, data protection authorities have published guidelines on the use of SCCs as a data transfer mechanism. The key guidelines are:

- Compliance assessment – companies must conduct a thorough assessment of whether the use of SCCs ensures an adequate level of data protection in the third country.
- Additional protective measures – if standard clauses do not provide sufficient protection, additional protective measures should be taken.
- Documentation and reporting – companies must document their risk assessment and any data protection actions taken.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

In Poland, the new Act of 14 June 2024 on the Protection of Whistleblowers is in force in this respect. The permissible scope of operation of company helplines, also known as ethical or corporate helplines, includes primarily anonymous, confidential and free receipt of reports from employees.

An oral report made via a recorded telephone line or other recorded voice communication system is documented with the whistleblower's consent in the form of:

1. a recording of the conversation, enabling its retrieval; or
2. a complete and accurate transcript of the conversation prepared by the unit or a designated person.

An oral report made via an unrecorded telephone line or other unrecorded voice communication system is documented in the form of a conversation record.

Reports may be made to various people within the organisation, including superiors, co-workers and other people associated with the company if there is a suspicion of abuse or irregularities.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting of irregularities in companies is generally permitted, but it is not the employer's obligation to accept such reports. The Whistleblower Protection Act does not oblige employers to allow anonymous reports, leaving them free in this matter. However, the employer must clearly state in the procedures whether it accepts anonymous reports and how it will verify them.

Anonymous reports are associated with the risk of abuse, such as false accusations, and difficulties in obtaining additional clarification, which can limit the effectiveness of the investigation. Therefore, companies that decide to accept anonymous reports often implement procedures to minimise these risks, such as an initial assessment of the credibility of the report before a full investigation, and also encourage reporting through open channels that guarantee confidentiality.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Currently, in accordance with the GDPR and national regulations (e.g. the Labor Code, Civil Code), the data controller (e.g. a company or a property owner) does not have to register the CCTV system separately with the data protection authority if the monitoring is carried out in accordance with the principles of minimisation and purposefulness of data processing.

The law imposes an obligation to openly inform people staying in the monitored area about the monitoring being conducted. This means that visible signs or information boards about the monitoring must be placed in the place covered by the image recording.

14.2 Are there limits on the purposes for which CCTV data may be used?

- cameras may not record people without their knowledge or consent, especially in private places;
- monitoring should have a legitimate purpose, such as protecting property or ensuring safety, and not be a means of unjustified surveillance;
- in the case of cameras in public places, camera recordings can only be stored for a certain period of time and must be protected from unauthorised access; and
- the people being recorded have the right to access these recordings.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

In Poland, employee monitoring is permitted, but subject to strict limitations resulting from the Labor Code and personal data protection regulations: the purpose of monitoring must be to ensure safety and work organisation; the monitoring must be proportionate to the purpose it is to achieve; employees must be informed about the scope and purpose of monitoring; and the employer must comply with the principle of data minimisation and have a legal basis for processing personal data.

Permitted types of monitoring and circumstances

- Video monitoring – this can be used to ensure employee safety, property protection, production control and protection of confidential information. Monitoring cannot cover places such as toilets, changing rooms or social rooms. It functions to increase safety, property protection or production control.
- Monitoring activity on a company computer – the employer can monitor the history of Internet browsing, application use, company email, as well as record keyboard and mouse activity or take screenshots. This monitoring applies only to company devices and is intended, among other things, to increase work efficiency.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The employer does not have to obtain employees' consent to introduce video monitoring in the workplace if the monitoring is used in accordance with Article 222 of the Labor Code, i.e. for purposes such as ensuring employee safety, protecting property, controlling production or protecting confidential information.

However, the employer is obliged to inform employees about the introduction of monitoring at least two weeks before its launch. This notification should include information about:

- the scope of data processing (e.g. which areas are monitored);
- monitoring purposes;
- the method and period of data storage; and
- employee rights related to monitoring;

Typically, notification is provided in written or electronic form (e.g. email, regulations, privacy policy), and may also be announced during a meeting or posted on a notice board.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The employer is obliged to notify employees about the introduction of monitoring in the manner adopted by a given employer, no later than two weeks before its launch.

In workplaces where employee representatives operate (e.g. works council), the employer should inform them about the planned monitoring and the arrangements for its scope and purpose.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Employers have the right to process information regarding an employee's presence in the office, but the scope and method of such monitoring must comply with the provisions of labour law and personal data protection.

Legal bases and limitations

The employer has the right to keep records of the working time and attendance of employees, which is their obligation under the Labor Code. They can do this, for example, through attendance lists, entry registration systems (e.g. access cards) that register the actual time an employee enters and leaves.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

In the case of personal data, there is a general obligation in Poland and the EU to ensure the security of personal data, which results from the GDPR. It results from Article 5(1)(F) of the GDPR, which states that personal data must be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures. Article 32 of the GDPR specifies in detail the obligations in the scope of security of processing, including risk assessment, pseudonymisation, encryption, business continuity, etc. The following are responsible for the security of personal data: the data controller; the entity processing (processor); or the joint controllers.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is a legal requirement under Polish and EU law to report personal data breaches to the relevant supervisory authorities.

Article 33 of the GDPR requires the controller to notify the supervisory authority of a personal data breach without undue delay, and no later than 72 hours after the breach has been discovered, unless it is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. if the data has been encrypted and an unauthorised person could not read it). The notification must include at least:

- the nature of the personal data breach (where possible, the categories and approximate number of data subjects and the types and approximate number of data records);
- the name and contact details of the DPO (or other contact person);
- a description of the possible consequences of a violation; and
- a description of the measures taken or proposed by the controller to address the breach, including actions intended to minimise its possible negative effects.

In Poland, personal data breaches may be reported to the President of the Personal Data Protection Office.

In situations where a breach does not meet the criteria for mandatory reporting, but the controller has doubts about the risk assessment, a voluntary report is possible.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Both Polish and EU law require that personal data breaches are reported to data subjects, but only in specific cases. According to Article 34 of the GDPR, the controller is required to notify the data subject immediately of a personal data breach if it is likely to result in a high risk of violating their rights or freedoms. Such a notification must be clear and understandable and should include at least:

- a description of the nature of the breach (e.g. data leakage, loss, access by an unauthorised person);
- the name and contact details of the DPO (if appointed) or other contact point;
- the possible consequences of a breach (e.g. identity theft, financial losses, damage to reputation);
- the measures taken or proposed by the controller to remedy the breach; and
- the recommended actions a person can take to reduce the risk (e.g. changing password, monitoring account activity, contacting their bank, etc.).

The GDPR does not give a specific time period for notifying an individual, but requires this to be done "without undue delay" after the breach has been identified.

Notification to the relevant person is not necessary if the controller has implemented appropriate technical and organisational protection measures that make the data unreadable to unauthorised persons (e.g. encryption).

16.4 What are the maximum penalties for personal data security breaches?

The GDPR provides for two main thresholds for financial penalties:

- up to EUR 10 million or up to 2% of the company's annual worldwide turnover (whichever is higher), for violations such as:
  - failure to keep a record of processing activities;
  - failure to report a data breach to the supervisory authority;
  - failure to appoint a DPO when required; and
- up to EUR 20 million or up to 4% of the company's annual worldwide turnover – for the most serious infringements, such as:

- data processing without a legal basis;
- a lack of consent or its improper obtaining;
- the violation of the rights of data subjects (e.g. the right to delete data); and
- the transfer of data to third countries without adequate safeguards.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) Investigative powers
Investigative powers of the enforcement body in Poland include:
- conducting explanatory proceedings (investigations) regarding the application of the GDPR;
- requesting information from the controller or processor and their representatives;
- conducting data protection control, including access to personal data and information necessary to perform tasks;
- obtaining access to premises and technical infrastructure (after appropriate procedures);
- requesting explanations, documents and data related to the processing of personal data; and
- securing evidence, including copies of databases.

(b) Corrective powers
The remedial powers of supervisory authorities are referred to in Article 58(2) of the GDPR and include:
- admonishing the administrator or processor in the event of a breach of the provisions of the GDPR;
- ordering compliance with the data subject's request, e.g. rectification of data, access to data, etc.;
- ordering the adaptation of processing operations to the provisions of the GDPR in a specified manner and within a specified time;
- ordering the controller to notify the data subject of a personal data breach;
- temporarily or definitively restricting processing, including prohibiting it; and
- ordering the rectification or deletion of personal data or restriction of processing (the right to be forgotten).

(c) Authorisation and advisory powers
In the context of EU law, the EDPB and national supervisory authorities have various supervisory authorisations and powers. The most important here are Articles 57 and 58 of the GDPR, which define the tasks and powers of supervisory authorities, as follows:
- advice to controllers and processors (Article 57(1)(C) of the GDPR) – the supervisory authority may advise data controllers and processors, including on DPIAs, and promote good data protection practices; and
- giving opinions on draft legal acts.
- The Personal Data Protection Act contains a number of advisory powers of the President of the Personal Data Protection Office, including:
- issuing opinions on draft legal acts – in accordance with Article 60 of the Act, the President of the Personal Data Protection Office may issue opinions on draft normative acts that affect the processing of personal data; and
- supporting public and private entities in the interpretation of regulations – in practice, the President of the Personal Data Protection Office issues guidelines, recommendations, positions and guides regarding the interpretation of GDPR and national regulations.

(d) Imposition of administrative fines for infringements of specified legal provisions
The Personal Data Protection Office imposes fines for violations of GDPR provisions.

(e) Non-compliance with a data protection authority
The Personal Data Protection Office may, for example, use one of the measures provided for in Article 58 of the GDPR (ordering the controller or processor to comply with the GDPR; ordering access to data; issuing a warning or admonition; or ordering compliance with the data subject's requests, etc.). The authority may also impose an administrative fine on a specific entity in the amounts specified in question 16.4. Furthermore, pursuant to Article 82 of the GDPR, the data subject may claim compensation from the controller or processor for damage caused by a breach of the GDPR, including as a result of failure to comply with the authority's instructions.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Personal Data Protection Office – both under Polish law and EU law – has the right to issue a ban on a specific personal data processing activity. This does not require obtaining a prior court order. Article 58(2)(F) of the GDPR states that the supervisory authority has the right to order the controller or processor to adapt the processing operation to the provisions of the GDPR, order the restriction of the processing of personal data, and order the suspension of the flow of data to a recipient in a third country. These powers are of an administrative nature and may be exercised independently by the supervisory authority. The President of the Personal Data Protection Office may, among other things: prohibit the processing of data; order their deletion; or limit the processing, without the need to obtain a court order. Such decisions may be appealed to an administrative court, but issuing a processing ban does not require prior court consent.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

According to the latest report, the Personal Data Protection Office issued around 2,000 administrative decisions in one year, of which over 90% were cases based on a complaint and not *ex officio*. In half of these cases, it applied remedial measures (Article 58 of the GDPR) and in 300 cases, an injunction. Only 30 cases had penalties.

For 2025, the Personal Data Protection Office has planned sectoral inspections, focusing on areas with a growing risk of personal data breaches and those that are particularly important from a social perspective, i.e. bodies processing personal data in the EU's Large-Scale Systems (including the Schengen Information System and the Visa Information System), as well as entities processing health data.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes, the Personal Data Protection Office exercises its powers towards companies based in other jurisdictions, especially when these companies process the personal data of persons

located in the territory of Poland or the EU and are subject to the provisions of the GDPR.

The Personal Data Protection Office cooperates with other data protection authorities in the EU within the so-called "cooperation and coherence mechanism" (one-stop-shop), which allows for the coordination of actions towards entrepreneurs based in other EU Member States. In the case of entrepreneurs from outside the EU, cooperation may take place on the basis of international agreements or other cooperation mechanisms.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Companies check whether the request comes from a legitimate authority and whether it has a legal basis in accordance with local and international data protection and privacy regulations. This often requires analysing whether the request complies with the GDPR or the relevant regulations in the company's jurisdiction.

Businesses also seek legal advice to assess the scope and validity of the request and to ensure compliance with data protection regulations and to avoid violating the rights of data subjects.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

Data transfers must be carried out in accordance with national legislation as well as with the provisions of the GDPR (especially Chapter 5), which aims to ensure the continued protection of personal data after their transfer to a third country or an international organisation.

Disclosure of data to law enforcement or government authorities abroad should be based on a legal basis, such as international agreements, mutual understandings or relevant national and EU laws. This must take into account the rulings of the ECJ and the recommendations of supervisory authorities.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Under Article 21 of the GDPR, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her in a similar manner.

Examples of restrictions under Regulation (EU) 224/1689 (the AI Act) when using AI systems are:

- the obligation to leave the final decision to the human being (Recital 61);
- the obligation to inform an individual that a high-risk AI system is being used against him or her (Article 26 of the AI Act);
- the obligation to implement monitoring of such decision-making after the introduction of such an AI device to the market; and
- the right of a natural person to be provided with clear and substantive information about the role and the main elements of the decision taken by an entity using an automated decision-making system (Article 86 of the AI Act).

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The Personal Data Protection Office follows the guidelines of the EDPB (Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models as of 17 December 2024).

Particularly, regarding anonymisation, the above Opinion states that whether an AI model is anonymous should be assessed on a case-by-case basis by data protection authorities. For a model to be anonymous, it should be very unlikely that (1) the individuals whose data was used to create the model can be directly or indirectly identified, and (2) such personal data can be extracted from the model through queries.

With respect to legitimate interest, the Opinion provides general considerations that data protection authorities should take into account when assessing whether legitimate interest is an appropriate legal basis for the processing of personal data to develop and implement AI models.

If an AI model has been developed on the basis of personal data processed unlawfully, this may affect the lawfulness of its implementation, unless the model has been properly anonymised.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The following trends can be observed in the enforcement of data protection regulations:

- a significant part of the fines is imposed in connection with the intentional action or omission on the part of the controller, i.e. failure to notify the supervisory authority of a breach of personal data protection or failure to respond to requests from the President of the Personal Data Protection Office;
- the amount of a fine increases with the scale of the incident, i.e. the number of people affected by the violation;
- some of the penalties concern unintentional violations – for example, using IT resources without ongoing support from their manufacturers – resulting from negligence or failure to comply with the obligation to apply appropriate security measures; and
- more severe financial penalties are imposed in cases of data breaches, such as those concerning Personal Identification Numbers or ID cards' series and numbers.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

Poland is working on the final text of the Act on Artificial Intelligence Systems. The main objective of the draft act is to implement the provisions of the AI Act into Polish law. The aim is for supervision of AI systems in Poland to take into account

the special position of the supervisory authority for personal data protection, resulting from both the provisions of the AI Act and the GDPR.

The hot topics for the data protection authority are:

- protection of financial data, especially in the shadow banking sector;
- protection of sensitive data, including medical data;
- verification of biased algorithms that form the basis of data processing;
- data protection by design; and
- evaluation of machine data processing in e-commerce.

Jakub Gładkowski is a managing partner and attorney, having qualified in 2013, with full rights of representation before all courts in Poland. He advises clients from a wide variety of sectors, including the: technology; fintech & blockchain; cybersecurity; media & telecommunications; healthcare and life sciences; financial institutions; real estate, construction & infrastructure; transport & logistics; manufacturing; retail & distribution; and energy sectors. He negotiates and drafts contracts in international sales and construction, represents clients in investments processes, mergers and acquisitions, and advises on commodity supply contracts, franchise agreements and joint-venture agreements. He has assisted a number of clients in technology transactions, crowdfunding and virtual currencies. In this respect he has gained experience in a number of legal issues covering compliance, IP and licensing proceedings. He was involved in robotic process automation contracts and technology licensing structures. He has additional qualifications, including a private detective licence, which facilitates debtors' assets tracing. He has 15 years of experience in commercial and corporate legal matters. He specialises in cross-border transactions and litigation.

Kieltyka Gladkowski KG Legal
Twarda 18, 00-105 Warsaw
Poland

Tel: +48 530 920 011
Email: jg@kg-legal.pl
LinkedIn: www.linkedin.com/in/k-jakub-g%C5%82adkowski-26907277

Barbara Kieltyka was admitted to the Bar in 1982, after entering into the State Commercial Arbitration Register (a central organisational unit of the government from 1949–1989, established to resolve disputes over property rights, establish legal relations, ensure discipline in the implementation of national economic plans and ensure the implementation of contracts concluded between economic entities). She is a licensed receiver and a veteran of corporate, banking and energy law, with 45 years of legal experience. She has more than 20 years' experience in-house at the Thermal Power and Energy Enterprise, where she litigated numerous court cases – civil, criminal, administrative and employment – in all instances, including at the Supreme Court and the Supreme Administrative Court. She acted as an in-house lawyer for the biggest Polish bank for almost 20 years, where she worked with international clients, assisted in difficult negotiations, litigated cases and assisted in restructuring and debt collection of difficult loans. She rendered assistance to the State Archives, dealing with complex documents and public procurement cases.

Kieltyka Gladkowski KG Legal
Sw. Anny 9, 31-008, Krakow
Poland

Tel: +48 12 263 46 74
Email: bk@kg-legal.pl
URL: www.kg-legal.eu

Malgorzata Kieltyka is a partner and attorney, with full rights of audience in all courts in Poland. She has been a practising lawyer since 2008 and is ranked among the leading individuals in healthcare & life sciences sector by *The Legal 500 EMEA* 2020 (https://www.legal500.com/firms/232083-kieltyka-gladkowski-kg-legal/c-poland/lawyers/4391814-magorzata-kietyka). She represents mostly international clients operating in various sectors, such as pharmaceuticals, new technologies, IT, media, healthcare and life sciences, transport & logistics, telecommunications, financial institutions, including fintech and start-ups. She deals with commercial law, formation of companies, handles M&A transactions, corporate restructuring, corporate governance and provides ongoing advice to corporate clients. She extensively advises on life science and technology transactions and litigation. In that respect, she has extensive experience in regulatory and commercial issues involving pharmaceuticals, medical devices, cosmetics, foods, including novel foods and borderline products. She handles entry procedures, labelling, advertising matters (including competition aspects) and advises on sales models.

Kieltyka Gladkowski KG Legal
Sw. Anny 9, 31-008, Krakow
Poland

Tel: +48 501 648 500
Email: mk@kg-legal.pl
LinkedIn: www.linkedin.com/in/małgorzata-kiełtyka-021425156/

Kieltyka Gladkowski KG Legal is a full-service Polish law firm, with offices in Warsaw, Krakow and with an address office in New York in the One World Trade Center (https://www.istart1.com). We also have a unit branch in the city near the border with Ukraine. The team comprises more than 30 lawyers. Our law firm is made up of Polish lawyers with an international background, including still active veteran banking and energy attorneys, practising law since 1982.

Kieltyka Gladkowski KG Legal handles mainly cross-border cases. It has a dedicated corporate and private client desk. We advise international and domestic clients on the basis of Polish law, in litigation and in non-contentious matters.

Our particular focus is on cross-border and multi-jurisdictional matters, primarily within the international trade; technology; technology transfers, IP/IT, TMT, fintech and blockchain; cybersecurity; AI data centres, media and telecom; healthcare and life sciences; digital health; financial institutions; DeFi; defence; real estate, construction and infrastructure; transport and logistics; e-commerce; manufacturing; and retail and distribution sectors, apart from standard areas of expertise like corporate, commercial, antitrust and competition, bankruptcy, commercial litigation, energy and employment.

www.kg-legal.eu