Legal 500
Country Comparative Guides 2025

Poland

Data Protection & Cybersecurity

Contributor

Kieltyka Gladkowski
KG Legal

K. Jakub Gładkowski

Attorney, Managing Partner | jg@kg-legal.pl

Barbara Kiełtyka

Attorney, Counsel | bk@kg-legal.pl

Małgorzata Kiełtyka

Attorney, Partner | mk@kg-legal.pl

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Poland.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Poland: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

Achieving and maintaining a satisfactory level of data protection and security of the virtual ecosystem – this is probably the basic common denominator of the very complex and fastest growing catalogue of legislative efforts of the European Union of three pillars: 1) data processing; 2) privacy; 3) cybersecurity. Due to the assumption of the Polish presidency of the EU Council in 2025, it is Polish jurisdiction that will play a key role this year in this aspect.

The most famous Salt Typhoon and the widely described critical problem of maintaining infrastructure in the first days of the Ukrainian crisis reveal the key role of a legal environment friendly to investment and development in protecting critical infrastructure of the functioning of state institutions and the defense sector. In turn, the phenomenon of ransom attacks and threats to access by unauthorized persons in the process of data processing in the course of processes in the IT system and database provoke the need to create a legal environment for the protection of data processing. Therefore, the legal framework of cybersecurity, privacy and data protection applies to all sectors and spheres of life of the economy and information circulation.

Hence, the review of key legal acts should be organized based on the "triangle" of the addressee of the regulation:

A) Legal acts relating to the functioning, supervision and responsibilities of national authorities and the European Union;

In this respect, the regulations focus on cyber threats, incident response and cyber crisis management in the EU, market issues, product security and certification; risk management; EU cybersecurity status processes and mechanisms for disclosing vulnerabilities and the legal implications related to them.

B) Regulations addressed to business or to protect the environment of all economic sectors;

The addressee in the form of non-public sector actors is equipped in Polish jurisdiction with regulations that primarily focus on artificial intelligence and next-generation technology, as it is hoped that AI techniques will improve security operations and help mitigate adversary attacks. In addition, it is necessary to indicate the related issues of post-quantum cryptography, including cryptographic algorithms that are to be resistant to breaking using a quantum computer. It is also necessary to indicate such regulatory objectives as awareness and "cyber hygiene" and regulations related to liability; certification procedures and standards for data processing and data leakage and protection of access to data; cyber threats, cybersecurity of critical sectors; digital identity and data protection; incident and risk management and the issue of disclosing security gaps.

C) Regulations aimed at protecting personal data.

Key legal acts relating to data collection, processing and protection reveal the core of the following sources of law:

- There can be invoked the main function of 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, and repealing Directive 95/46/EC (**GDPR**).
- Currently, the latest act supplementing the data protection space is the currently implemented **Regulation** (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 **on the European health data space** and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ EU L 2025, item 327) and in this respect it is an example of a comprehensive sectoral approach of the European Union to the processing of personal data and particularly sensitive data (as a supplement to the GDPR).
- As a key complement to the GDPR, it is necessary to indicate the Directive, which is the main engine of the functioning of the key agency in the European Union, created to provide guidelines and interpretation of the provisions of the GDPR, i.e. The European Data Protection Board (EDPB). Namely, it is Directive 2016/680 of 27 April 2016, known as **the Data Protection Law Enforcement Directive**.
- EU statutory law is continuously supplemented with interpretative documents and white papers on specific

provisions created by European Union bodies, for example the latest EDPB guidelines concern the procedure for the approval of Binding Corporate Rules for controllers and processors (adopted on March 13, 2025).
- European Union legislation is supplemented by the law of individual EU countries and in Poland the key act in this respect is the act implementing the Data Protection Law Enforcement Directive, i.e. **the Polish Act of 10 May 2018 on the protection of personal data** (Journal of Laws of 2019, item 1781). This is a key document in Polish jurisdiction and the main source of data protection law, because the body supervising the enforcement of GDPR provisions in Poland, namely the Personal Data Protection Office (PDRO), operates on the basis of this act.
- An additional important act is the Polish act that intensifies the implementation of the GDPR, namely the Act of 21 February 2019 on amending certain acts in connection with ensuring the application of the GDPR.
- An important legal act, especially crucial from the perspective of web scraping and data parsing issues, is **the Act of 27 July 2001 on the protection of databases** (Journal of Laws of 2024, item 1769).
- A key pillar is also **the Polish Act of 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime** (Journal of Laws of 2023, item 1206).
- An example of a sectoral approach to data protection regulation in Poland is **the Act of 14 June 2024 on the protection of whistleblowers** (Journal of Laws, item 928), which complements the symbiosis of the data processing protection environment, focusing in this case on the instruments of circulation of reporting irregularities, not only in the work environment but also in organizations such as business corporations.
- The above system is supplemented by administrative decisions of the President of the Polish Personal Data Protection Office, who enforces data protection in Poland, for example, the most recent two decisions concern the infringement of personal data by a public postal institution and Decision number DKN.5112.10.2024 of March 6, 2025 imposing a fine on the company for, among other things, the lack of encryption of media containing personal data used outside the processing area.

The architecture of legal sources in cybersecurity is as follows:

- The core source for the cybersecurity sector is focused on **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA** (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ EU L 151, 2019, No. 151, p. 15, as amended).

In addition, the following list of sources of rules, which are created jointly by the European Parliament and the Council of the European Union in the form of the following regulations, needs to be indicated:

- Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 on establishing measures to enhance solidarity and capacity in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (**EU Cyber Solidarity Act**).
- Regulation (EU) 2023/2841 of the European Parliament and of the Council of 13 December 2023 on establishing measures for a high common level of cybersecurity in the Union institutions, bodies, offices and agencies.
- Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technological and Research Centre and the Network of National Coordination Centres.
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 **on the digital operational resilience of the financial sector.**
- Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 **establishing the Digital Europe programme.**

And also:

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (**NIS 2 Directive**).

The above sources are supplemented by regulations issued by the Council of the European Union in the form of regulations, i.e. acts directly applicable in the European Union countries, of which the following is the most recent example:

- Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures **to combat cyberattacks threatening the Union** or its Member States.

The EU cybersecurity system is also being created through so-called implementing regulations of the European Commission, which structurally streamline the administrative work of the European Union. For example:

- Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 establishing the circumstances, formats and procedures for notification pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and information and communication technology cybersecurity certification.
- Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council with regard to the adoption of a European cybersecurity certification scheme based on common criteria (EUCC).
- Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 with regard to technical and methodological requirements for cybersecurity risk management measures and clarifying the cases in which an incident is considered to be serious in relation to DNS service providers, TLD name registries, cloud service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, online marketplace providers, online search engines and social networking platforms, and trust service providers.

Sources of cybersecurity law also include the so-called COMMISSION (EU) DELEGATED REGULATIONS, EU DECISIONS and COMMISSION (EU) RECOMMENDATIONS.

The EU cybersecurity system is complemented by Polish legislation, which includes the following basic legal acts:

- **Act on the National Cybersecurity System** (of 5 July 2018), which specifies the principles of organisation and functioning of the national cybersecurity system, the obligations of regulated entities and the principles of cyber incident management.
- The Act on the Internal Security Agency and the Intelligence Agency, which contains regulations regarding the activities of special services in the field of cybersecurity.
- The Crisis Management Act, which relates to the protection of critical infrastructure, including ICT systems.

The above legal sources also include regulations of individual Polish government units and agencies, such as:

- Regulation of the Minister of Digitization of 4 December 2019 – specifying the organizational and technical conditions for entities providing cybersecurity services.
- Regulation of the Council of Ministers of 31 October 2018 – regarding the thresholds for recognizing an incident as serious.
- Regulations of the Minister of National Defense of June 13, 2022, May 5, 2022, October 12, 2018 – regulating cybersecurity activities in the armed forces.

Cybersecurity enforcement agencies:

- Minister of Digital Affairs – responsible for coordinating cybersecurity policy.
- Cybersecurity Board – advisory body on strategic decisions regarding cybersecurity.
- Internal Security Agency (ABW) – deals with the protection of key infrastructure and responding to cyber threats.
- CERT Polska – computer incident response center.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

- In 2025 in Poland, an amendment to the Act on the National Cybersecurity System should be passed, which is to implement the NIS 2 directive. The time to implement this regulation into the national legal order of the Member States has already passed, but the Polish legislator has not yet managed to introduce the appropriate regulations. The website of the Government Legislation Centre (RCL) most likely published the final draft of the amendment to the Act on the National Cybersecurity System of 7 February 2025. The Act implements the NIS 2 directive, introducing a number of significant changes to the national cybersecurity system. The new provisions cover a wider range of entities, introduce more stringent requirements for risk management and incident reporting, and provide for more severe sanctions for violations.

Based on the previous Article 5 of the Act on the National Cybersecurity System, the status of the operator of essential services was granted administratively, and its

scope was specified in the annex to the Act. The amendment introduces a completely new wording of Article 5, **defining a key entity and an important entity**. In the new approach, a key entity is not only an organization providing key services, but also a provider of managed services in the field of cybersecurity, top-level domain registries (TLDs) or qualified trust service providers.

- At the beginning of 2025, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (**AI Act**) entered into partial application. The provisions currently in force indicate the scope of the Regulation and prohibited practices. The *vacatio legis* for the rest of the act will end on 2 August 2026, when the Regulation will, in principle, apply in its entirety.
- At the beginning of 2025, **Regulation** (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 **on establishing measures to enhance solidarity and capacity in the Union to detect, prepare for and respond to cyber threats and incidents** entered into force. The Regulation is intended to achieving the general objectives of strengthening the competitive position of industry and services in the Union across the digital economy, including micro, small and medium-sized enterprises and start-ups, and contributing to the Union's technological sovereignty and open strategic autonomy in the field of cybersecurity, including by boosting innovation in the Digital Single Market.
- Also at the beginning of 2025, **Regulation** (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 **on the digital operational resilience of the financial sector** entered into force. The aim of the Regulation is to achieve a high common level of digital operational resilience, which is to be achieved by the uniform requirements for the security of networks and information systems regulated by the Regulation.

As for the legal environment of data, not only personal data but all data, including financial data, the year 2025 is primarily about the implementation of European Union law, which aims to harmonize the provisions on fair access to and use of data (Regulation (EU) No 2023/2854 of the European Parliament and of the Council of 13 December 2023, the so-called **Data Act**).

The European Union, including the Polish jurisdiction, aims to unify the data market in Europe through the Data Act. However, this requires interference in current legislation, which is why the Data Act not only supplements the legal system with its own provisions, but also introduces changes to the current law, including Regulation (EU) 2017/2394 and Directive (EU) 2020/1828. The provisions are to increase competition in the data market and expand access to data for market participants, with non-personal data also being regulated. Hence, in 2025, new requirements for the design and manufacture of Internet of Things (IoT) devices are key for data market participants, which will apply to products introduced to the market in 2026. The regulation is cross-sectional and creates obligations for service providers in this sector.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) does not provide for a licensing or registration obligation for entities covered by these regulations. Certification under the Regulation remains voluntary. Such obligations have also not been introduced in Poland under national laws on personal data protection.

However, despite the lack of registration/licensing obligations, it should be remembered that some entities are obliged to appoint a Data Protection Officer. The appointment of this body is required in situations where:

a. processing is carried out by a public authority or body, with the exception of courts when exercising their judicial powers;
b. the core activities of the controller or processor consist of processing operations which, by their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale; or
c. the core activities of the controller or processor consist in the processing on a large scale of special categories of personal data or personal data relating to criminal convictions and offences.

It is possible for one Inspector to be appointed by several entrepreneurs.

CYBERSECURITY – certification issues:

Entities required to apply a legal layer of data protection are very often also subject to regulations on cybersecurity, which is a branch of European Union law subject to greater security verification formalities than data protection. An example of certification operating in

Polish jurisdiction is the so-called trust service provider notification procedure, which, pursuant to Article 3, point 16 of eIDAS Regulation concerns the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps or website authentication. In Poland, the National Bank of Poland is the notifying body for providers of such services and as part of the supervision in the eIDAS Regulation , this is an example of a certain certification that the services meet the conditions of cybersecurity.

The current period 2025-2026 shows that EU cybersecurity certification is evolving within the broader EU regulatory context, and ENISA is developing a number of programmes and projects to support this certification.

Currently, there are a number of different cybersecurity certification schemes in the EU for information and communications technology (ICT) products, such as technology components (chips, smart cards), hardware and software.

The first system under the Cybersecurity Act certification is based on the renowned international standard Common Criteria. The core of this certification is Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council with regard to the adoption of a European cybersecurity certification scheme based on common criteria (**EUCC**). The program is based on established international standards, for example ISO/IEC 15408 and ISO/IEC 18045. Certification under this program (certification scheme) applies to such ICT products as:

- Biometric systems;
- Firewalls (both hardware and software);
- Detection and response platforms;
- Routers;
- Switches;
- Specialized software (such as SIEM and IDS / IDP systems);
- Data diodes;
- Operating systems (including for mobile devices);
- Encrypted mass storage and, above all,
- Databases and Smart Cards and secure elements contained in various types of products, e.g. passports, which are used by all citizens on a daily basis.

Currently, final work is underway on the Draft Act on the National Cybersecurity Certification System, which will be the Polish national implementing act of Regulation (EU) 2019/881 of the European Parliament and of the Council. The Draft Act specifies the obligations of the national government administration body responsible for security certification – i.e. the minister responsible for computerization. According to the Draft Act, in order to conduct research on ICT products, services and processes, interested entities will have to obtain accreditation from the Polish Accreditation Center. The Draft Act also provides for the possibility of imposing an administrative penalty on an entity that conducts conformity assessment without the required accreditation.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

The year 2025 shows a clear trend of introducing European Union regulations applied directly in the jurisdictions of the Member States, including Poland, which, for the purposes of comprehensive regulation of a specific sector, for example health, introduce separate legal definitions of key terms of information flow. Despite this, the source core of the data flow nomenclature remains GDPR.

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

In the initial part of the GDPR, the creators of the regulation indicated that: Personal data which, by their nature, are particularly sensitive in the light of fundamental rights and freedoms, require special protection, because the context of their processing may pose a serious risk to fundamental rights and freedoms. Such personal data should include personal data revealing racial or ethnic origin.

In addition, a principle has been introduced according to which it is prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or

philosophical beliefs, trade union membership, and to process genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning the health, sex life or sexual orientation of that person.

There is also a **definition of Data Controller**, which should be understood as a natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of processing personal data; where the purposes and means of such processing are determined by Union law or the law of a Member State.

Processor, on the other hand, means a natural or legal person, public authority, agency or another body that processes personal data on behalf of the controller.

The definitions contain, as can be seen, vague terms, because Polish jurisdiction is not based on precedent. Consulting practice shows that the term "personal data" causes problems in precisely defining the legality of IT data processing activities. An example is the general nickname in social media and depending on the approach and economic justification for operations on such data, it will depend on whether a given activity, for example web scraping, will concern personal data.

Based on the guidelines of the authorities for the protection of personal data and court judgments, it can be indicated that personal data is an identification number, location data, internet identifier. There are guidelines, although they are contradictory, as to whether license plates can constitute data identifying a driver. According to the Polish Personal Data Protection Office guidelines, although a telephone number does not directly determine the identity of a natural person, it is information that allows direct contact with a specific person, and determining the identity itself does not require excessive costs, time or actions. Therefore, the mere possibility of contacting this person may lead to determining their identity, and therefore the telephone number constitutes personal data within the meaning of the provisions of Regulation 2016/679 679. Additionally, according to the President of the Polish Personal Data Protection Office, the IP number constitutes information about an already identified (in the digital environment) person, i.e. a specific user. Therefore, in the light of art. 4 point 1 of Regulation 2016/679, both the IP number (regardless of whether it is variable or not) and the ID number are considered personal data.

In the context of the latest changes to EU data law, the fundamental source of the GDPR is supplemented by acts currently coming into force, which regulate sectoral data processing issues. An example is **Regulation (EU)** 2023/2854 of the European Parliament and of the Council of 13 December 2023 **on harmonised rules on fair access to and use of data** and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (**Data Act**), which contains a particularly interesting approach to the definition of "data" in general and the concept of "metadata", respectively:

1. "data" means any digital representation of actions, facts or information as well as any compilation of such actions, facts or information, including in the form of an audio, visual or audio-visual recording;
2. "metadata" means a structured description of the contents of data or of how data are used, which facilitates the discovery or use of the data.

Another example is Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024, which is the legal basis for the system called "**Eurodac**", supporting the asylum system. Asylum proceedings in migration policy generate the problem of processing biometric data, hence this act has particularly interesting definitions in the area of personal data, namely such as:

- "fingerprint data" means data relating to the prints, in the form of flat and rolled impressions, of all ten fingers, if the person concerned has them, or to invisible latent fingerprints;
- "facial image data" means digital images of the face that are of sufficient resolution and quality to be used for automated biometric matching;
- "biometric data" means fingerprint data or facial image data.

However, the crowning example of the official definition of key legal terms protecting the interest in information flow is the example of introducing comprehensive regulation of the flow of health sector data by means of Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European health data space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847.

This document introduces separate definitions such as:

a. "electronic personal data relating to health" means data relating to health and genetic data processed in electronic form;
b. "non-personal electronic health data" means electronic health data other than electronic personal health data, including both data that have been anonymised so that they no longer relate to an identified or identifiable natural person ("data subject") and data that have never related to an identified individual.

c. "electronic health data" means electronic personal data or electronic non-personal health data.

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

The principles of personal data processing are specified in detail in the GDPR. According to this legal act, personal data must be processed lawfully, fairly and in a transparent manner for the data subject; collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; adequate, relevant and limited to what is necessary for the purposes for which they are processed; accurate and, where necessary, updated.

All reasonable steps must be taken to ensure that personal data that are incorrect in light of the purposes for which they are processed are immediately deleted or rectified; stored in a form which allows the identification of the data subject for no longer than is necessary for the purposes for which the data is processed.

Data must be processed in a way that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures.

The principles contained in Article 5 of the GDPR:

- Principle of legality, reliability and transparency;
- Purpose limitation principle – data may only be collected for specified, explicit and legally justified purposes, and may not be processed in a manner incompatible with these purposes;
- Data minimization principle – data must be adequate, relevant and limited to the minimum necessary;
- Principle of correctness – the administrator's obligation to ensure that data is up-to-date and correct and to correct or delete erroneous information;
- The principle of storage limitation – data is stored only for the period necessary to achieve the purpose, after which they are deleted or anonymized;
- Principle of integrity and confidentiality – the obligation to protect data against unauthorized access, loss, destruction or damage;
- Principle of accountability – the data controller must be able to demonstrate compliance of data processing with the regulations and appropriately document its processes.

Legal basis for processing personal data (Article 6 GDPR):

- consent of the data subject – unambiguous and voluntary;
- performance of the contract – for example, processing customer data in order to complete the order;
- legal obligation – for example, storing personnel documentation in accordance with labor law provisions;
- protection of a person's vital interests – e.g. emergency medical intervention;
- performance of a task carried out in the public interest – activities of state administration bodies;
- the legitimate interest of the administrator or a third party – for example, transferring employees' personal data to a contractor (it cannot violate the rights of the data subjects).

To sum up, the principles indicated by the GDPR in the field of personal data protection are: legality, reliability, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality.

From the perspective of practice in 2025, other sources of EU law are also important, which create legal foundations in the chain of regulations regarding the circulation and access to data. For example, taking **Regulation 2023/2854 on harmonised rules on fair access to and use of data**, this regulation supplements the core in the form of GDPR with rules for sharing data by entrepreneurs with consumers as well as in B2B relations and regulates other issues of access to data within the framework of interoperability, or changing the data provider's service provider. For the purposes of this document, for example Article 2 contains definitions of terms such as processing and data processing service. This is therefore one of the examples of sectoral supplementation of the principles of GDPR and the principles indicated above.

6. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or

bundled with other matters (such as consents for multiple processing operations)?

Consent to the processing of personal data is one of the legal bases for data processing in accordance with Article 6 paragraph 1 letter a) of the GDPR, which means that if there is no other basis legalizing the processing, it is required. Additionally, in the case of special categories of data, the definition of which is given above, this consent must be explicit.

According to the GDPR, **consent should be given by means of an unambiguous, affirmative act** which expresses the voluntary, informed and unambiguous consent of the data subject, in a specific situation, to the processing of personal data concerning him or her, and which takes the form, for example, of a written (including electronic) or oral statement.

This may consist of ticking a box when browsing a website, selecting technical settings for the use of information society services or any other statement or conduct which clearly indicates in a given context that the data subject has accepted the proposed processing of his or her personal data. Silence, pre-ticked boxes or the absence of action should therefore not constitute consent.

Consent should apply to all processing activities carried out for the same purpose or purposes. Where the processing serves different purposes, consent is required for all of these purposes. Where the data subject is to give consent in response to an electronic request, such a request must be clear, concise and not unnecessarily disruptive to the use of the service to which it relates.

Bullet points:

Form, content and manner of administering consent.

The requirements for consent are set out in the GDPR. They are:

- voluntariness – the person giving consent must have a real opportunity to choose and withdraw consent as easily as he or she gave it (Article 7(3) of the GDPR);
- awareness – according to the definition of consent in Article 4, consent is a voluntary, specific, conscious and unambiguous expression of will, the person should know what he or she agrees to (Article 4, point 11 of the GDPR)
- specific purpose – consent cannot be general, it should refer to a specific purpose of data processing.

Can consent be?:

- implied – NO, consent must constitute the voluntary, informed and unambiguous consent of the data subject; silence, pre-ticked boxes or failure to take action should not imply consent (recital 32 of the GDPR);
- incorporated into a broader document (e.g. regulations) – the principle of transparency requires that all information and communications related to the processing of personal data be easily accessible, understandable and formulated in clear and plain language (especially if addressed to a child); consent should be clearly separated from the rest of the text and highlighted along with the purposes for which it will be used;
- combined with other issues (such as consent to various processing operations) – NO, if the data processing is for various purposes, consent for all of these purposes is necessary (recital 32 of the GDPR).

A separate issue is the operation on data as a result of performing public services by offices and bodies. An example worth emphasizing is the legality of data processing by public health entities within the framework of the institution of so-called access services to electronic health data introduced by Regulation 2025/327. This act complements the general right to rectify data indicated in Article 16 of the GDPR for the purposes of procedures of health sector entities. In other words, it is an example of the latest regulation that changes both Directive 2011/24/EU and regulates the space of health data as a whole and regulates, for example, supplementing the core of the GDPR, creating a legal basis for at least one service of access to electronic patient health data and creating an obligation for Member States to create such information obligations regarding data processing.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

In Polish jurisdiction, as well as in the entire European Union, the basic act that substantively regulates the processing of personal data introduces a general principle of prohibition of processing special categories of personal data. This is therefore a reversal of the rule by introducing the principle of an implied prohibition, unless the administrator finds specific reasons, i.e. exceptions, for performing operations on these data under the law. In

order to introduce this prohibition, a provision of the main legal act, the GDPR, was created, which begins its editorial text in the prohibition by listing the features of data that are a special category of personal data.

According to the GDPR: **It is prohibited** to process personal data revealing racial or ethnic origin, political opinions, religious or ideological beliefs, trade union membership, and to process genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning the health, sex life or sexual orientation of that person.

However, **there are numerous exceptions** to this principle listed in Article 9 of the GDPR. According to this regulation, the processing of sensitive data is permissible in a situation where, among other things, it is necessary for health reasons; the person concerned expressly consents; processing is necessary, for example, for public interest.

On the other hand, where personal data relating to criminal convictions and offences or related security measures are processed, such processing may only be carried out under the supervision of official authorities or if the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

In the case of information society services, it is permissible to accept the consent and process the personal data of a child who has reached the age of 16. If the child is under 16, the processing of data is only possible if the consent has been given by the person exercising parental authority.

Bullet points:

Specific requirements for the processing of certain categories of personal data:

1. Processing of special categories of personal data – Article 9, paragraph 1 of the GDPR: is prohibited unless:

- the data subject has given his/her explicit consent;
- it is necessary for the fulfilment of obligations and the exercise of specific rights by the controller or the data subject in the field of labour law, social security and special protection;
- it is necessary to protect vital interests;
- it is necessary for the establishment, pursuit or defence of legal claims or in the course of the administration of justice by courts;
- it is necessary for reasons of important public interest;
- it is necessary for the purposes of preventive healthcare or occupational medicine, for assessing the employee's fitness for work, for medical diagnosis, for the provision of healthcare or social security care, treatment or for the management of healthcare or social security systems and services;
- it is necessary for reasons of public interest in the area of public health;
- it is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

2. 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);
- 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).

3. The processing of data relating to convictions and prohibited acts may only be carried out by specific entities under the supervision of public authorities.

From the perspective of the latest regulations generated by European Union legislation, the most interesting status of particularly sensitive data is the problem of so-called **health data**. It should be pointed out that the interest in proper management of health information is opposed to the needs of medical procedures for which patient data is processed, which, in turn, requires freedom of processing for the purposes of treating the patient. This is important not only from the perspective of the new supplementary provisions of Regulation 2025/327, which comprehensively regulates the primary use of personal health data by entities participating in the health service, but data processing is the result of regulatory complex medical procedures, including not only therapeutic methods but also diagnostic procedures. Therefore, the problem of the legal basis for data processing in Polish jurisdiction is related to **the concept and term of the general right of the patient to information about their health** as indicated in art. 9 sec. 1 of the Act of 6 November 2008 on patient rights and the Patient Rights Ombudsman.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already

described? If so, please describe the relevant provisions.

One example of interference in the principles of standard circulation of personal data protection is a special act established in Poland in connection with the change in the geopolitical situation of Polish jurisdiction, for example due to the Ukrainian crisis. Namely, it concerns a special procedure, introduced by art. 10, of the new act amended in 2024 on the defense of the homeland. It concerns a special right of access by Polish military authorities to the processing of information from data sets maintained not only by other Polish military services but also state institutions and public authorities. This is therefore a special legal basis for the Polish army to obtain information, including personal data, with the reservation, however, that the processing of this data will take place within the scope of the competence of a given military authority, however, the processing of such information may be secret or even take place without the consent and knowledge of the data subject.

Another example is the criminal law sphere and penalizing art. 267 of the Penal Code of cybercrime aimed at illegally obtaining protected information, including personal information. However, the criminal law sphere and consequences go beyond the scope of this guide.

In Poland, additional exclusions and limitations apply to the protection of personal data.

GDPR does not apply to:

- processing of data for personal and domestic purposes – unrelated to professional or commercial activities, e.g. storing correspondence or addresses (recital 18 of the GDPR);
- national security and the activities of state services (recital 16 of the GDPR).

Restrictions on data processing for archiving, research and statistical purposes (Article 89 of the GDPR).

The EU legislator assumed that the nature of personal data processing for specific purposes requires modification of the general rules on personal data protection. The abovementioned provision distinguishes the following specific purposes of processing:

1. archival in the public interest,
2. scientific research,
3. historical research and
4. statistical.

The implementation of all the above-mentioned purposes, due to their specificity, requires a modified approach to the issue of personal data protection, because the general approach may prove to be too restrictive and prevent the implementation of the processing purposes. At the same time, the EU legislator draws attention to the need to guarantee appropriate safeguards, indicates the principle of data minimization, pseudonymization and refers to further data processing (i.e. processing for purposes other than those for which the data were originally collected).

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

In accordance with Article 35 of the GDPR, **where a type of processing, in particular using new technologies**, is likely to result in a high risk to the rights and freedoms of natural persons due to its nature, scope, context and purposes, the controller shall assess the impact of the planned processing operations on the protection of personal data before starting the processing. A single assessment may be carried out for similar processing operations involving a similar high risk.

The assessment shall include at least:

a. a systematic description of the planned processing operations and the purposes of processing, including, where applicable, the legitimate interests pursued by the controller;
b. assessing whether processing operations are necessary and proportionate to the purposes;
c. an assessment of the risk of infringement of the rights and freedoms of data subjects; and
d. the measures planned to address the risk, including safeguards and security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

For example, **when assessing technical knowledge, it is necessary to take into account, among other things, standards and norms (e.g. from the ISO/IEC 27001 series)**, which are subject to continuous reviews and changes conditioned by technological progress. These norms are based on the basic values of information, i.e. confidentiality, integrity and availability. For example, according to the guidelines of the Polish Personal Data Protection Office, it is currently assumed in cryptography

that for many years DES encryption (in its basic form) has not provided a high level of security due to the length of the key and the much greater computing power of today's computers.

As regards the scope of processing, when assessing the risk, all quantitative aspects of the processing should be taken into account, such as the scope of the data categories, the amount of data processed, the number of entities affected by the data processing.

In the context of processing, the intensity of the interference in the privacy of a given data processing process, e.g. related to monitoring, the adopted technical solutions, the circumstances and manner of using the assumed solution and the relationship to other evaluation elements, including the purpose of processing, as well as legalization premises, should be assessed. The processing time may also be important.

When assessing the risk of processing, it should be borne in mind that the reference point for this assessment is to be the rights and freedoms of data subjects, which the GDPR does not limit exclusively to the sphere of personal data or even privacy. Recital 75 of the GDPR notes that risks to the rights and freedoms of individuals, of varying likelihood and severity, may result from the processing of personal data that may lead to physical harm, property damage or non-property damage. This applies in particular where the processing may result in discrimination, identity theft or identity fraud, financial loss, damage to reputation, breach of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social harm.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

In Poland, there are specific codes of conduct that are approved by the President of the Personal Data Protection Office, as the competent authority in accordance with Article 40 of the GDPR. Among key sectors such as the military, defense, education, finance, cybersecurity, there are mainly known cases of approved codes of the medical services sector, because this sector needs to unify the principles of data processing for the purposes of patient relations, which by its nature does not concern the issue of competition and favors the association of similar entities in order to achieve appropriate methods of regulation.

The Polish Personal Data Protection Office is currently conducting procedures to approve codes of conduct for data processing at various stages of the proceedings:

- Code of Conduct for the Photography Industry;
- Data Protection Code of Conduct for the Sports Industry;
- Code of conduct with personal data in local government units;
- Code of procedure in common courts [covering activities outside the scope of the justice system];
- Code of Conduct for the Medical Research Industry;
- Code of Conduct for the Protection of Personal Data in the Non-Governmental Organisation Sector – authors: a group of non-governmental organisations led by the ALIVIA Oncology Foundation;
- Code of conduct on personal data protection National Chamber of Tax Advisers;
- Code of conduct on the protection of personal data of the Employers' Association, Organisation of Opinion and Market Research Companies;
- Code of Conduct on Personal Data Protection for the Polish Hotel Industry Chamber of Commerce;
- Code of conduct on personal data protection for the Internet Industry Employers' Association IAB Polska.

11. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Each controller of personal data, in accordance with the requirements of the General Data Protection Regulation (GDPR), **must maintain a register of personal data processing activities for which they are responsible**. This register is a key element of the personal data protection management system and is intended to enable monitoring, control and documentation of data processing activities in the organization.

This register shall include all of the following information:

1. name and contact details of the controller and any joint controllers and, where applicable, of the controller's representative and the data protection officer; purposes of processing;
2. a description of the categories of data subjects and the categories of personal data;
3. the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international

organisations; where applicable, transfers of personal data to a third country or an international organisation, including the name of that third country or international organisation;
4. if possible, planned dates for deletion of individual categories of data; if possible, a general description of the technical and organisational security measures.

An exception to the principle of keeping a register of activities related to the processing of personal data is introduced by Article 30, paragraph 5 of the GDPR, which states that **this obligation does not apply to organizations employing fewer than 250 people**, **unless** the processing they perform may pose a risk to the rights or freedoms of data subjects, is not of an occasional nature or involves special categories of personal data. In order to meet their obligations, organizations create data processing registers (in paper/electronic form), train employees in the field of the GDPR, implement company data protection policies and then monitor the compliance of the resulting policy with the regulations resulting from the GDPR.

In practice, the register of data processing activities reflects the work and division of responsibilities of the life of the organization.

If we take the most representative example, then an interesting one is the register concerning the technology transfer center of a technical university. Such a register is then divided into the entire life of the organization. For example, if such an institution employs employees, then we have at least several dozen data processing activities, which are recorded in sample separate segments of such a register.

- First, we have the problem of recruitment, so such a register contains personal data of those who conduct the recruitment, as well as those who are subject to this recruitment.
- We have a specified operating system and access to this system, with a description of the name of the system, for example HIT Kadry or Web soop admin and we have people applying for employment.
- In the case of personnel, information is divided in the same way, for example on the periodic assessment of employees, or work time records, or in payroll.

In practice, then a specific activity of processing such data is indicated, for example calculation of salaries, or in matters of occupational health and safety or occupational medicine. In the same way, it is indicated how data processing activities take place, for example medical examinations of candidates for studies. Technical and organizational security measures are also indicated, such as disk encryption, antivirus software, cyclical password changes, and data anonymization.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

The principle of **time-limited data storage** states that personal data should only be stored for as long as is necessary to achieve the purposes for which it was collected.

This means that organizations should set specific retention periods, and after these have passed, the data should be deleted or anonymized, unless there is another legal basis justifying its continued storage.

GDPR requires organizations to have clear policies and procedures that specify how long different categories of personal data should be stored. According to the GDPR, data subjects have the right to request the deletion of their personal data. This is the so-called right to be forgotten.

The data subject may request the deletion of their data if:

1. The data is no longer necessary for the purpose for which it was collected – if the purpose of data processing has been achieved or the data is no longer necessary to achieve that purpose.
2. The person has withdrawn consent to data processing – if data processing was based on the consent of the person who later withdrew it, the organization must stop processing the data and delete it, unless there is another legal basis for processing it.
3. The data was processed unlawfully – if the data was processed in a way that violates the provisions of the GDPR.
4. The obligation to delete data results from European Union law or national law – when legal provisions impose the obligation to delete data in certain situations (e.g. tax or data protection regulations).

After the period for which the data was processed has elapsed, it should be deleted, unless there is another legal basis for retaining the data, e.g. archiving or statistical data.

To comply with data retention and deletion rules, organizations must develop and implement appropriate data retention policies and data deletion procedures. These policies should specify:

1. The storage period for different categories of data;
2. Procedures for deleting data securely once the data is no longer needed or the retention period has expired;
3. Identifying those responsible for overseeing the data storage process, monitoring data deletion deadlines and ensuring compliance with regulations;
4. Monitoring and auditing mechanisms for compliance with data retention and deletion policies to ensure that data is not retained longer than necessary.

Failure to comply with data retention and deletion regulations can lead to serious consequences, both legal and financial. In summary, data protection regulations require organizations to establish clear data retention and deletion policies. It requires that personal data is retained only for the period necessary for the purposes of its processing, and after that period effectively deleted or anonymized.

The latest court decisions show that the legality of data storage and the lack of its deletion depends on the proper justification for storing data after the end of processing. There is case law concerning financial institutions, which shows the divergence of the court's assessment of whether, for example, storing the data of financial institution customers is legal after the end of the processing period. Thus, the entity in Poland that undertakes the legal assessment of whether the data processed, for example by a financial institution such as a bank, is stored correctly is the President of the Personal Data Protection Office. However, the decision of such an authority is only a stage of the entire case, which, especially in the financial sector, goes to the administrative court, where the parallel parties are the Office that issued such a decision and, for example, the bank to which the negative decision applies.

An example is the latest judgment of the Supreme Administrative Court in Poland of February 13, 2025 (reference number III OSK 6563/21), where the bank used customer data for the purpose of examining creditworthiness and transferred it further. This is one of the latest and very detailed interpretations of the GDPR regulations, which indicates that data storage in the light of the GDPR is the effect of banking and financial procedures also provided for in banking law. This shows that sectoral law creates provisions for the data controller on the basis of which data can be stored.

In another decision, the President of the Personal Data Protection Office indicated that the data controller **cannot** rely on the lack of technological possibilities to delete a natural person's data and this does not constitute a basis for refusing to delete their data from the database. Since the data controller obtained the data (for example, in the form of a telephone number) and entered it into the database, he should therefore have the tools to delete the data (Decision of the President of the Personal Data Protection Office number: ZSPR.440.963.2019).

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

According to Article 36 of the GDPR, consultation with the supervisory authority is mandatory in situations where a data protection impact assessment (DPIA) shows that a particular processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects. In such a case, the controller must consult the supervisory authority before starting processing, unless the risk assessment has been adequately mitigated by the application of data protection measures.

In accordance with the guidelines of the Polish Office for Personal Data Protection, it should be noted that prior consultations are a tool for cooperation between the supervisory authority and the controller, and the purpose of prior consultations is to best secure the processing of personal data by the controller in cooperation with the supervisory authority.

Although consultation with the supervisory authority is mandatory only in certain situations, there are also cases where such consultation is recommended, especially when the controller has doubts about the compliance of its activities with the provisions of the GDPR or in the case of more complex data processing operations. Such situations may include:

- uncertainty about compliance,
- complex processing activities,
- transfers of data to third countries or
- changes in processing processes.

In the Polish jurisdiction, one of the interesting recent examples of consultations with a data protection authority is a case involving a **controller who offers a sports achievement monitoring system using cloud computing, cooperating with smart wristbands recording heart rate data, i.e. processing of special categories of personal data and location data**.

Thus, the data protection authority in Poland has created case-by-case guidelines on which groups of data processing actors and in what cases would be welcome to consult the authority, for example:

- social media and platforms for user profiling,

- machine-to-machine communication systems, in which the car informs the surroundings about its behaviour (movement) and in the event of an emerging threat receives warning messages from the surroundings (road infrastructure, other cars),
- workplaces (monitoring of IT systems, e-mail, software used, access cards, etc.) – using systems for monitoring employee working time and the flow of information in the tools they use (e-mail, Internet),
- online stores offering promotional prices for specific customer groups.
- companies operating loyalty programs (shopping communities) – using customer profiling systems to identify shopping preferences, automatically setting promotional prices based on the profile.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

The most important information for the private sector is that GDPR and the Personal Data Protection Act of 2018 impose in some situations the obligation to appoint a Personal Data Inspector.

The appointment of a Personal Data Inspector is required in situations where:

a. processing is carried out by a public authority or body, with the exception of courts when exercising their judicial powers;
b. the core activities of the controller or processor consist of processing operations which, by their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or processor consist in the processing on a large scale of special categories of personal data or personal data relating to criminal convictions and offences.

In accordance with the provisions of the GDPR, it is possible for one Data Protection Officer to be appointed by several data controllers, especially in cases where the organisations are linked (e.g. groups of enterprises, networks of organisations) but process data in a similar way.

The tasks of the Personal Data Protection Officer include, among others:

- informing the controller, the processor and employees who process personal data of their obligations under the GDPR and other data protection provisions of the Union or Member States and advising them on this matter;
- monitoring compliance with the Regulation, other data protection provisions of the Union or Member States and the controller's or processor's policies in the field of personal data protection, including the allocation of responsibilities, awareness-raising activities;
- training of staff involved in processing operations and related audits;
- providing recommendations on request for the data protection impact assessment and monitoring its implementation;
- cooperating with the supervisory authority;
- acting as the contact point for the supervisory authority on issues relating to processing, including prior consultation and, where appropriate, conducting consultations on any other matters.

The selection of the Personal Data Inspector is subject to notification. Within 14 days of the date of appointment, the President of the Personal Data Protection Office must be notified of this appointment, indicating the data required by law.

The GDPR requires the appointment of a Data Protection Officer in certain situations, but does not impose an obligation to appoint other specialists, such as a Chief Information Security Officer. In practice, organizations may, but are not required to, appoint other persons responsible for information security or data protection. Such persons may perform supporting functions in the implementation of data protection policies and information security management, but their tasks and responsibilities are usually less formal than those assigned to the Data Protection Officer.

For public sector entities, the GDPR provisions are overlapped with other regulations being created. The protection of personal data processed by public entities is based on the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC as implemented by ESMA in implementing rules adopted by its Management Board. Under this act, each Union institution or body appoints a data protection officer (Article 43). The data protection officer thus appointed has the main task of informing the controller, the processor and the employees who process personal data of the obligations incumbent on them

under the Regulation and other Union data protection provisions and advising them on this matter.

Therefore, in the case of an entity such as the European Securities and Market Authority, such an entity will operate on the basis of a combination of the above-mentioned sources of law.

15. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

Employee training related to personal data protection is based not only on data protection regulations but primarily on the Polish Labor Code, which regulates the employer's obligations in the broadly understood scope of occupational health and safety, which also includes obligations in the scope of data protection, data processing and cybersecurity. Thus, even if a given training obligation in this scope does not result directly from data protection regulations (for example, there is only such a recommendation), **the provisions of labor law directly impose on the employer the obligation to train the employee in a given sector if they deal with data**. It should also be borne in mind that this may apply not only to the employee in the strict sense (working under an employment contract) but also to the broadly understood staff (contracts of mandate, contracts for specific work, remote work, body leasing, interns, trainees).

Staff training is an issue that regulatory provisions link to the obligations of the unit established in the organization for data protection. The main emphasis on raising awareness of data processing and protection in the form of training concerns such employees who have contact with data. For example, in the light of Article 39 of the GDPR, this is staff (and not only employees) who participate in each data processing operation. Additionally, such training is also subject to people who also conduct audits of data operations.

The data controller has an obligation to raise awareness of personal data protection within the organization. In this context, it can be considered that the controller has an obligation to provide employees with appropriate educational resources so that they understand their obligations in the field of personal data processing.

Essentially, this means that training should cover at least the following topics:

1. Principles of personal data processing – employees should be familiar with the principles of safe processing of personal data;
2. Scope of responsibility in the processing process – employees should know the scope of their responsibility related to data processing;
3. Procedures related to personal data breaches – employees should have information on when and how to report incidents related to personal data breaches;
4. Data retention policies – employees should know how long they can store data and how to ensure its security;
5. Data subject rights – training should explain how to respond to requests from data subjects, such as requests for access, rectification, deletion, and the right to data portability.

16. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

The data protection regulations applicable in Polish jurisdiction (particularly Article 13 of the GDPR) impose on the Data Controller the obligation to provide a range of information to the person whose data is being processed. The Controller must provide information on:

1. identity and contact details and, where applicable, the identity and contact details of the representative;
2. where applicable, the contact details of the data protection officer;
3. the purposes of processing personal data, and the legal basis for processing;
4. legitimate interests pursued by the controller or by a third party; information on the recipients of the personal data or categories of recipients;
5. where applicable, information on the intention to transfer personal data to a third country or an international organisation and on the Commission's finding or failure to find an adequate level of protection.

The administrator is also required to provide information on the period of time for which the data will be processed or to indicate the source of the obligation to provide information (under law or under contract) and the consequences of failure to provide data. These obligations are described in detail in Articles 13 and 14 of the GDPR, which require data administrators to provide this information to data subjects in a clear, understandable and easily accessible manner. Typically, such an information obligation is implemented by placing

a privacy notice on the organization's website, in documents containing a privacy policy or during the conclusion of an agreement with the data subject.

In the current practice, the President of the Polish Office for Personal Data Protection points to the most common errors in information clauses, in particular, incorrect designation of the administrator, lack of obligatory elements, use of overly specialized formulations, lack of information about the recipient, imprecise indication of the data storage period.

It is worth noting that in the case law verifying the information obligations of obliged entities, there has been a detailed explanation of the conflict between the information clause of data processing and the so-called press clause related to information activities and the problems of the conflict between the application of data protection regulations and the exclusions of the application of specific data protection regulations in relation to journalistic activities (Judgment of the Supreme Administrative Court III OSK 2883/21). It follows that press activities are subject to Polish press law and the rights of persons whose data are processed are regulated therein.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

The data controller is the main person responsible for the compliance of personal data processing with the law. It is he who decides on the purposes and methods of data processing. In practice, this means that the controller has full control over how data is collected, processed, stored and deleted. The controller is responsible for ensuring that all data processing activities are in accordance with the principles of the GDPR, such as data minimization, purpose of processing, compliance with the law and ensuring appropriate security measures.

If the processing of data by the controller violates the provisions of the GDPR, the controller shall be liable for any damage that has occurred as a result of such violation. According to Article 82 of the GDPR, any person who has suffered damage (material or non-material) as a result of a violation of the provisions of the Regulation has the right to seek compensation for the damage suffered from the controller or the entity processing the data.

The distinction between the liability of the controller and the data processor is that the controller is liable for damages caused by data processing in breach of the provisions of the Regulation, while the data processor is liable for damages resulting from its improper performance of its obligations related to data processing. This liability arises when the processor has failed to fulfil its obligations, e.g. has not applied appropriate data security measures, has not conducted the required audits, or has not cooperated with the controller in the event of a data breach. It may also be liable if it has acted outside the scope of the instructions issued to it by the controller, e.g. by processing data in a manner inconsistent with the contract or without the prior consent of the controller.

18. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

Generally speaking, the use of monitoring has limitations under the data protection law in force in Polish jurisdiction. **First**, the law focuses on regulating the freedom to monitor in public places. **Second**, the law focuses on limiting the time of storing monitoring recordings. **Third**, the law in Polish jurisdiction emphasizes securing monitoring recordings against unauthorized access. **Fourth**, people who are being recorded have the right to access these recordings, which should also be considered a limitation of the freedom to monitor.

Article 22 of the GDPR regulates the right of the data subject not to be subject to a "decision based solely on automated processing, including profiling, which produces legal effects for that person or significantly affects him or her in a similar manner". The right not to be subject to a decision based solely on automated processing is a manifestation of the broadly understood right to the protection of personal data and constitutes an important element thereof.

There is also a general prohibition on making decisions based solely on automated processing of special categories of data, i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and processing genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning the health, sexuality or sexual orientation of that person. Such a prohibition is a consequence of the general prohibition on processing special categories of data.

In the context of personal data protection, automated decision-making, including profiling, is an enigmatic and controversial issue. Interestingly, the interpretation of this issue is revealed in the assessment of the application of data protection regulations in Poland to non-automated disclosure of personal data in the case law of the Supreme Administrative Court (Supreme Administrative Court judgment of 23 February 2024, reference number III OSK 3838/21). Data protection regulations apply not only to the processing of personal data in an automated manner, but also to the processing of data in a non-automated manner, provided that they are part of a data set or are intended to be part of it. Disclosure of personal data in a public place (e.g. a parliamentary office) may constitute a violation of the GDPR if this data is linked to other information characteristic of the data set (e.g. an employee's personal file).

According to the GDPR, individuals may be assigned online identifiers such as **cookie identifiers**. The creation of identifiers may result, among other things, in leaving traces that, in combination with a unique identifier and other information, may be used to create profiles and identify these individuals. The possibility of creating profiles entails the responsibility of website owners to obtain users' consent to save online identifiers such as cookies on their devices. The website owner is also obliged to inform what exactly the consent concerns.

In accordance with the **Polish Electronic Communications Act** of 12 July 2024 (Journal of Laws, item 1221), storing information or accessing information already stored in the telecommunications terminal equipment of the subscriber or end user is permitted, provided that the subscriber or end user is previously informed 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 using software settings installed in the telecommunications terminal equipment used by them or the service configuration.

The subscriber or end user must consent to the storage of information and, in addition, the information stored or accessed does not cause configuration changes in the telecommunications terminal equipment of the end user and the software installed in this device.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

Targeted advertising and behavioral advertising are often used in the context of personalizing advertising content based on user data. Personalizing ads involves tailoring marketing messages to a specific person, based on their previous online activities, preferences, and interests. Tools such as cookies, web beacons (tracking pixels), and other tracking technologies allow to collect information that can be used to create user profiles.

Behavioral advertising, based on the analysis of users' online behavior, collects data on their interests, which are then saved in cookies. In this context, an important obligation for website owners is to provide users with the possibility of expressing their consent to the storage of cookies. They should provide a form that allows the user to accept or reject cookies. In addition, information on the processing of user data, including how data on their interests is used, must be included in the privacy policy of the website.

Restrictions on targeted/behavioral advertising are introduced by Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the Single Market for Digital Services (DSA). The DSA introduces **two new restrictions on advertising haggling**. In order to ensure the proper protection of minors on the Internet, Internet platform providers cannot use personal data to profile minors in order to present them with tailored advertisements on this basis. Additionally, the **DSA prohibits Internet platform providers from displaying advertisements based on user profiling that are based on special categories of data** specified in the GDPR, such as sexual orientation, ethnic origin, religious beliefs, or health.

The AI Act, which entered into force on August 1, 2024, is the first legal regulation for artificial intelligence systems and models, and it can also serve as a guideline for direct references to the use of AI solutions to create and direct personalized advertising to consumers. From the perspective of the new AI Act regulations, each service provider should assess whether its use of an AI system for targeted advertising purposes is permissible under the regulations, as well as classify the system based on the degree of risk it poses. This is also associated with a catalog of obligations that such a provider will have to meet when using targeted and behavioral advertising.

It is assumed that the underlying AI systems used for behavioral advertising purposes, e.g. product recommendations on a website based on content viewed, will generally be low-risk AI systems. However, **it is important to consider the underlying algorithms used to create the AI training to create such ads and the potential liability for biases in such algorithms**.

A very interesting parallel problem is the case law of the European Court of Justice of the European Union dealing with the model of tracking and combining data about people as an aspect of behavioral advertising. In an important judgment (C-604/22), of 7 March 2024, the European court clarified the role of the joint controller of data in the situation of a pop- up requesting "consent" to tracking and transferring data, because the user's "consent" goes to hundreds of intermediary companies participating in the so-called Real Time Bidding (RTB) – advertising exchanges on which these companies combine data about users to display them appropriately tailored advertising. The judgment of the national court in this case may assess whether the entity may be liable for violations of personal data that may occur under the TCF [Transparency and Consent Framework] system provided by them, allowing the exchange of information about users' preferences regarding advertising profiling on the network. In particular, the Court's judgment states that TC Strings (digital signals containing user preferences) constitute personal data when they can be linked in a clear manner to an identifier, such as the IP address of the user's device, and the controller can have access to such data.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

The sale of personal data has no legal definition.

Although the term "data sale" has no legal definition, in practice it means the transfer or sharing of personal data between different entities, including the sale of databases, which involves the need to comply with numerous information obligations.

In the context of selling personal data, the right to information takes on special importance. Therefore, the seller is obliged to inform the person whose personal data is being processed about the purpose of processing and that their personal data may be sold or transferred to another entity. At the same time, the seller must obtain the consent of the person whose personal data is being processed about possible sale of data. Obtaining consent should be done in a clear and unambiguous manner, as well as voluntarily. In this case, the data controller is obliged to inform the data subjects about the processing of this data, even if it was obtained from another entity and not directly from the data subject. According to Art. 14 of the GDPR, if the personal data was not obtained from the data subject (only from the seller of the database), the controller provides the data subject with information such as: their identity and contact details; the purpose of processing; information about the recipients of the data; the period for which the data will be processed; the source of the data, etc. In principle, this information should be provided by the controller within a reasonable period of time, but **no later than within one month**.

The level of protection of personal data is revealed in data trading from the perspective of purchasing a database, where the legality of data trading depends on meeting the following conditions:

- the database seller should have the right to make the database available;
- the database vendor should have appropriate consent or other legal basis for processing and transferring personal data.

In addition, the persons whose data is in the database should be informed that their data has been purchased, for what purpose and on what basis it will be processed, and about the possibility of objecting or withdrawing consent.

In addition, data security and protection must be ensured by applying appropriate technical and organisational measures to prevent unauthorised access, loss, damage or misuse of data.

In addition, the rights of persons whose data is in the database must be respected, such as the right to information, access, rectification, deletion, restriction, transfer, objection, not being subject to automated decision-making, etc.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

Direct marketing involves contact via email, telephone, or instant messaging. Contact is initiated by a representative of a person offering specific services. Contact is directed to an entity that may be interested in a given product or service.

In order to use direct marketing in the form of text, telephone or email communication, it is necessary to **obtain consent from the person** who is to be included in the scope of marketing activities. This consent must be voluntary, conscious and unambiguous.

In accordance with the e-Privacy Directive, consent may be given in any way that allows the user to freely and knowingly express their wishes, including by ticking a box when browsing a website (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (**Directive on privacy and electronic communications**) (OJ EU L 201, 2002, No. 201, p. 37, as amended)).

The Directive on the processing of personal data and the protection of privacy in the electronic communications sector prohibits the use of false identity data or false return addresses or numbers when sending unsolicited communications for direct marketing purposes.

The **Polish Electronic Communications Law Act** (Act of 12 July 2024 – Electronic Communications Law (Journal of Laws item 1221)) establishes the following restrictions:

1/ the use of automatic calling systems is prohibited,

2/ the use of telecommunications terminal equipment is prohibited, in particular when using interpersonal communication services.

Automatic calling systems are understood to mean machines making calls without human intervention. Telecommunications terminal equipment is understood to mean mobile phones, tablets or computers. This prohibition applies to unsolicited commercial information. Marketing consent makes the above prohibition cease to apply.

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

According to Article 4, point 14 of the GDPR,

- "biometric data means personal data resulting from special technical processing, relating to the physical, physiological or behavioural characteristics of a natural person and enabling or confirming the unique identification of that person, such as facial images or fingerprint data".

The provisions of the GDPR introduce a general prohibition on the processing of biometric data, as this type of data is considered to be extremely sensitive. The point is that biometric data can lead to the unique identification of a person and are considered to be very private. However, there are exceptions to this prohibition.

Biometric data can be processed in situations where:

1. the data subject gives his/her explicit consent,
2. the processing of this data is necessary for health reasons,
3. processing is necessary for important public interest reasons.

An independent problem of the legal approach to biometrics from the perspective of protecting the privacy of the person whose biometric data is concerned is a particularly interesting example of the regulation of **the Polish Labor Code**. The provision of Article 22(1b) of the Polish Labor Code states **that the processing of an employee's biometric data is also permissible when the provision of such data is necessary for the purpose of controlling access to particularly important information**, the disclosure of which may expose the employer to damage, or access to premises requiring special protection.

This provision constitutes the legal basis for the employer to use employee biometrics in the work environment. However, this is an approach from the perspective of cybersecurity rather than the protection of sensitive data, because biometrics is a particularly important medium for securing the IT environment and supervising the safety of the work environment.

In connection with the processing of biometric data, the controller must remember not only to comply with the basic principles of personal data processing under Article 5 of the GDPR, including the principles of lawfulness of processing, data minimisation and the integrity and confidentiality of processing, or to notify the data subject about the processing of biometric data and what rights they have in this respect, **but also** to conduct a risk analysis and, if necessary, a data protection impact assessment (DPIA).

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

Artificial intelligence uses personal data. It processes, analyzes, or learns from it. The Polish Office for Data Protection analyzes artificial intelligence and machine learning technology and their impact on the privacy of individuals and the protection of their data. Given the importance of personal data for the development and functioning of artificial intelligence algorithms, the issue of personal data protection has been regulated in the **EU Artificial Intelligence Act** (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June

2024 laying down harmonised rules on artificial intelligence). The entire act will enter into force on 2 August 2026, with the exception of some provisions that will only apply from 2 August 2027. However, the provisions of Sections I and II of this regulation are already applicable. The Regulation defines an AI system as a machine system that is designed to operate with varying levels of autonomy after its deployment, that may exhibit adaptive capabilities after its deployment, and that, for explicit or implicit purposes, infers how to generate outputs from the input it receives, such as predictions, content, recommendations or decisions that may impact the physical or virtual environment.

Transparency of algorithms is important from this perspective. According to GDPR, users have the right to information about the processing of their data and this raises questions about the transparency of AI algorithms that affect decisions about individuals.

It is worth pointing out that **the European Data Protection Board (EDPB) on 17 December 2024 adopted an opinion on the use of personal data to develop and implement artificial intelligence models ("Opinion")**. The guidelines are applicable also in the Polish jurisdiction.

According to this Opinion, as regards **anonymisation**, it is stated 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. that such personal data can be extracted from the model by means of queries.

The Opinion provides a non-exhaustive and non-binding list of methods to demonstrate anonymity.

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 artificial intelligence models.

A three-step test helps assess the use of legitimate interest as a legal basis. The EDPB provides examples of a consultant talking to users and using AI to improve cybersecurity. These services can be beneficial to individuals and can be based **on legitimate interest** as a legal basis, but only if the processing is deemed strictly necessary and the balance of rights is maintained.

The Opinion also includes a number of criteria to help data protection authorities assess whether individuals can reasonably expect a specific use of their personal data. These criteria include whether the personal data was publicly available, the nature of the relationship between the individual and the controller, the nature of the service, the context in which the personal data was collected, the source from which the data was collected, the potential further uses of the model, and whether individuals are actually aware that their personal data is available online.

If the balancing test shows that processing should not take place due to the negative impact on individuals, mitigating measures may limit that negative impact. The Opinion provides a non-exhaustive list of examples of such **mitigating measures**, which may be of a technical nature or may facilitate the exercise of individuals' rights or increase transparency.

Finally, 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 duly anonymised.

It should be remembered that in the light of the GDPR, **the processing of personal data refers to all operations that are performed on these data, such as collection, analysis, transfer, storage**. It therefore refers to both manual and automated activities (because the regulations do not limit the method of working with data). Therefore, even with the use of new technologies and automation systems, the provisions of the GDPR will apply to activities on data, at every stage.

In the context of automated data processing, the AI Act also introduces a **requirement for human supervision of an AI system** if it is deemed to be high-risk.

New regulations on the assessment of the risk of using artificial intelligence and machine learning to process data will be of particular importance from the perspective of **processing mass data** by financial institutions. In conducting such tests, the criterion of "explainability" of AI will be important, i.e. whether it is possible to precisely explain why there is a specific result of AI's operation. Just as in the GDPR we are dealing with the principle of privacy by design, in the AI Act the legislator generally introduces the requirement of transparency by design.

The full menu of provisions is presented in the latest **Artificial Intelligence of Things**, or the combination of two legal layers for two technologies: the Internet of Things (IoT) and Artificial Intelligence (AI), where AI, including machine learning, analyzes this data, detects patterns, predicts events and makes decisions, e.g. optimizing

energy consumption, predicting machine failures or personalizing services, analyzing data generated by IoT, enabling intelligent decisions and process automation.

The source of legal protection for technologically processed data will be:

1/ in the layer of legality of data processing, these will be, for example, the provisions of the Polish Electronic Communications Law of July 2024, including Article 399 regarding the privacy of subscriber or user data in the end device and the provisions of the GDPR Regulation and related opinions of the European Data Protection Board (EDPB), for example applications related to mobility and regarding awareness of consent to the processing of end-user data;

2/ in turn, from the perspective of data control, for example in the scope of cybersecurity certification of products, services and processes – there is the crucial role of the Regulation (EU) 2019/881 of the European Parliament and of the Council on Cybersecurity, and additionally the provisions of the Polish Act of 5 July 2018 on the national cybersecurity system for cloud computing services.

24. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

The transfer of personal data is a complex and particularly critical issue in terms of legality. The GDPR has unified the standards of personal data protection regulations throughout the European Union. An important postulate of the EU legislator is the principle of the free transfer of personal data between EU Member States.

This means that **the transfer of data within the territory of the European Economic Area is generally safe**. However, the issue of data transfer and the protection of personal data in the event of their transfer outside the EEA remains.

The GDPR indicates the conditions that must be met if data is to be transferred outside the EEA (Chapter V of the Regulation). In order for data to be transferred to countries outside the EEA, it is necessary for the controller and the processor to meet the conditions specified in the Regulation. Ensuring an adequate level of protection by a specific third country or international organization is a necessary condition for data transfer.

In accordance with the Personal Data Protection Regulation, there are **three basic modes of transferring personal data to countries outside the EEA**:

1. Decision on the adequacy of protection (Article 45 of the GDPR),
2. Transferring data subject to appropriate safeguards (Article 46 GDPR),
3. Binding Corporate Rules (Article 47 GDPR),

Transfer is also possible based on a court order or an administrative body of a country outside the EEA. Data transfer is also possible when the person has given their consent, despite the lack of appropriate safeguards.

Article 49 of the GDPR states that in the absence of an adequacy decision pursuant to Article 45(3) of the GDPR or appropriate safeguards pursuant to Article 46 of the GDPR, the transfer of personal data to a third country or an international organisation may only take place provided that:

a. the data subject, having been informed of the possible risks to which the proposed transfer may relate due to the absence of an adequacy decision and appropriate safeguards, has expressly consented to it;
b. the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the data subject;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary to establish, pursue or defend legal claims;
f. the transfer is necessary to protect the vital interests of the data subject or of other persons where the data subject is physically or legally incapable of giving consent;
g. the transfer is made from a register which, in accordance with Union or Member State law, is intended to provide information to the public and which is accessible to the public in general or to any person who can demonstrate a legitimate interest, but only to the extent that the conditions for such access laid down in Union or Member State law are met in the specific case.

On July 10, 2023, the **European Commission issued an**

implementing decision establishing an adequate level of protection for personal data under the Data Privacy Framework, related to the protection of personal data within the European Economic Area. This decision, issued under Article 45(3) of the GDPR, means that (currently) the transfer of personal data to the United States is legal, within the framework and on the principles resulting from this decision.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

The obligations of administrators and data processors have been implemented into the Polish legal system based on Regulation (EU) 2016/679 of the European Parliament and of the Council in the Act of 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime. In accordance with Article 22 of the aforementioned Act, the administrator is subject to information obligations.

This means that the administrator is obliged to, among other things, provide information about the entity that will use the data, indicate the purpose of data processing or provide information on the right to lodge a complaint with the President of the Data Protection Office or another supervisory authority based on separate provisions in the event of a violation of a person's rights as a result of the processing of their personal data and the contact details of the President of the Data Protection Office or another supervisory authority.

Under the Personal Data Protection Act, the basic tasks of the administrator include ensuring that personal data are:

1. processed lawfully and fairly and using the necessary technical and organisational measures, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights and freedoms of natural persons of varying likelihood and severity;
2. processed for specific and legitimate purposes;
3. adequate, relevant and not excessive in relation to the purposes for which they are processed;
4. correct and updated as necessary;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of processing;
6. processed in a way that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using technical and organisational measures appropriate to the threats and categories of data being protected, and in particular protected against making them available to unauthorised persons or coming into possession of an unauthorised person.

In addition, the General Data Protection Regulation (GDPR) requires controllers and processors to **implement technical and organizational measures**. This requirement aims to ensure an appropriate level of security in relation to the risk.

These measures include, among others: **data encryption**, **regular testing** and evaluation of the effectiveness of security measures, **control of access to data** and processing only necessary data. Furthermore, the controller is also required to conduct an impact assessment, e.g. mass monitoring, in order to reduce the risk to the rights and freedoms of natural persons.

In the event of a breach of personal data protection, the administrator must report the incident to the President of the Personal Data Protection Office within 72 hours. In addition, the administrator is obliged to notify the data subject if there is a high risk of their rights being breached.

Administrators and processors are also required to keep a register of data processing activities. The register documents the purposes of processing, the categories of data subjects, the entities to which the data is made available and a description of the security measures used to protect the data.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

A personal data breach is understood to mean a **breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data** transmitted, stored, or otherwise processed.

An example would be a breach of:

- confidentiality,
- availability, or

- integrity of data.

According to Article 33 of the GDPR, the controller is required to report a breach to the supervisory authority (the President of the Personal Data Protection Office), unless it is unlikely that the breach will result in a risk of violating the rights or freedoms of natural persons. The controller shall report the breach without undue delay – if possible, **no later than 72 hours after the breach is discovered**. An explanation of the reasons for the delay shall be attached to the report submitted to the supervisory authority after 72 hours.

The structure of Article 33 of the GDPR means for data controllers that not every breach of personal data protection will qualify for reporting to the supervisory authority – there may be a situation in which a given breach will involve a "low" risk of violating the rights or freedoms of natural persons.

The second obligation that may arise in the event of a breach is the **obligation to notify individuals whose data has been breached**. Article 34 of the GDPR refers to this and indicates that the obligation to notify individuals arises in a situation where a breach of personal data protection may result in a high risk of violating the rights or freedoms of natural persons.

The purpose of notifying a data subject of a breach of their personal data is to provide them with appropriate information regarding the breach affecting their personal data. A description of the nature of the breach is an essential element of the information provided to the data subject.

According to Article 34 of the GDPR, the information provided to the data subject must be provided in clear and plain language so that the data subject can understand what has happened to their personal data, why and what it may mean for them.

In addition, it is worth paying attention to the second version of **the guidelines on reporting a personal data breach under the GDPR** – Version 2.0 of 28 March 2023. Guidelines EO 9/2022 is an interpretative document developed by **the European Data Protection Board (EDPB)**. It is an umbrella organization associating national data protection authorities (national supervisory authorities) of the European Economic Area countries, as well as the European Data Protection Supervisor (EDPS).

Here is the link to the full text of the guidelines: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

The document is a collection of practical information **because it shows model examples** when a data process breach is not subject to the obligation to report. Where the situation is particularly interesting is when the data has been encrypted using the most modern algorithm, data backups have been created, the unique key has not been broken, and the data can be restored in due time – then it may happen that this breach is not subject to reporting. However, if the key is broken at a later time, this situation will require reporting.

These guidelines complement the legal environment also with a focus **on cross-border infringements** and infringements in non-EU establishments.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

The information obligations of the administrator include indicating that the entity has the right to request access to personal data, rectification or deletion of personal data, or restriction of the processing of personal data relating to that person.

The right of access means that the data subject has the right to access their personal data at their request. To obtain access to the data, an application must be submitted to the controller, who, taking into account the request, provides or transfers a copy or an extract from the data prepared in an accessible form. In the event of refusal or restriction of access, the interested entity must be informed of the possibility of filing a complaint with the President of the Personal Data Protection Office. In accordance with the EU Regulation, the basis for refusing access may be justified by an adverse effect on the rights and freedoms of others.

A person whose data is processed in violation may submit a **request to delete their data**. It is not possible to order the deletion of personal data collected during operational and reconnaissance activities conducted on the basis of legal regulations.

Under the GDPR, the data subject also has the right **to request the correction of their personal data** if it is incomplete, incorrect or outdated. The data controller is obliged to correct such data without undue delay. In addition, one can request **the restriction of the processing** of one's data if one contests its accuracy, objects to the

processing, or if the controller no longer needs the data for the purposes of processing, but the person wants to retain it for the purposes of establishing, pursuing or defending claims.

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

In the field of private right of action, the personal data protection law in force in Poland mainly focuses on compensation.

In this respect, the main circumstance materialising the private claim is **the fact of suffering damage resulting from a breach of substantive data protection law**, which in the case of personal data is EU law, namely the GDPR Regulation.

A breach of data protection law involves an interest protected by sectoral law, which, in the case of personal data, finds support in the institution of **protection of personal interests** and the related claims mechanism.

In the structure of Polish civil law, private claims can be divided into:

1/ demand that the action violating the protected data be discontinued, unless it is not illegal;

2/ in addition, in the event of an infringement – a demand that the person who committed the infringement takes the actions necessary to eliminate its effects, in particular submits a declaration of appropriate content and form;

3/ under the principles provided for in Polish civil law, it is also possible to demand monetary compensation or payment of an appropriate sum of money for a specified social purpose. If, as a result of the violation of data as a personal right, property damage has been caused, the injured party may demand its redress under general principles.

From the perspective of the private claims mechanism under sectoral law, it is important that personal data protection law provides for **liability for damages not only for property damage** (e.g. financial losses) but also for **non-property damage** (e.g. mental health damage, stress).

A person entitled to private claims has the right to obtain compensation for the damage suffered from the controller or processor.

Each controller involved in the processing is liable for damage caused by processing that violates the legal protection of personal data. The processor is liable for damage caused by processing only if it has failed to comply with the obligations that the law directly imposes on processors or if it has acted outside the controller's lawful instructions or contrary to those instructions.

It is also important that the controller or processor is exempted from liability for damages if they prove that they are not in any way responsible for the event giving rise to the damage.

Where more than one controller or processor is involved in the same processing, or both a controller and a processor are involved, and are responsible for the damage caused by the processing, **they shall be jointly and severally liable** for the entire damage in order to ensure effective compensation for the data subject.

In addition to the sectoral arsenal of claims under the GDPR regulations, another issue is **the pool of claims for damages from the perspective of the data breach system** within the legal system of database protection. In this respect, Polish data protection law is affected by the fact that the European Union, in its Directive 96/9/EC on the protection of databases, has left it to the Member States (including the Polish legislator) to establish sanctions for infringement of database rights, i.e. copyright and *sui generis* rights. In the latter case, the arsenal of claims includes:

- a claim for cessation of infringement;
- a claim for removal of the effects of infringement,
- a claim for redress of the damage caused, including: a claim for the issuance of the obtained benefits; publication claims or a claim for compensation (including in the variant of redressing the damage on the principles: 1) of general compensation (under the Polish Civil Code) or 2) as a lump sum claim (sometimes referred to as "preferential"), by paying twice or three times the appropriate remuneration.

However, the basis for protection of databases *sui generis* provided for in Article 11 of the Polish Act of 27 July 2001 on the Protection of Databases, indicating the database producer as the holder of the above-mentioned claims, does not combine the value of the private status of the database producer with the disposal of such claims.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require

actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

According to Article 82 of the GDPR Regulation, any person who has suffered material or non-material damage as a result of an infringement of the regulation 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. The CJEU in its case law indicates that damage should be understood broadly.

To claim compensation, the following conditions must be met:

- the fact of the damage and its amount;
- a culpable damage event, taking into account the presumption of fault of the responsible entity;
- the existence of a connection between the damaging event and the damage.

The list of breaches that may lead to damage is included in Article 4, point 12 of the GDPR. It provides for security breaches leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to personal data transmitted, stored or otherwise processed.

Damage is understood in this respect broadly, also as non-pecuniary damage, for example related to the fear of data leakage. However, there will be evidentiary obligations associated with this.

Polish courts examining data leak cases are of the opinion that the mere existence of a sense of threat, uncertainty, fear of the effects of a data leak, lack of control over the use of personal data constitutes a violation of personal rights and gives rise to the obligation to redress the harm suffered as a result. For example: judgment of the Regional Court of Warsaw-Praga in Warsaw of 17 December 2021 (reference number III C 1169/19).

30. How are data protection laws in your jurisdiction typically enforced?

Enforcement of data protection regulations involves activities such as **supervision**, **control**, **imposition of penalties**, and international cooperation.

In Poland, a body called **the President of the Personal Data Protection Office** has been established. The President of the Personal Data Protection Office has supervisory powers and is responsible for conducting proceedings in cases of personal data infringement. The President of the Personal Data Protection Office **is authorized to impose administrative fines**, and is also the body conducting control over compliance with regulations on personal data protection.

The President of the Personal Data Protection Office has the **right to conduct inspections** of the processing of personal data by various entities, both public and private. Inspections may concern, among others, compliance with the principles of data processing, implementation of appropriate data protection measures, realization of the rights of data subjects, or compliance with obligations related to documenting data processing processes.

The President of the Personal Data Protection Office is also the authority competent to conduct explanatory proceedings in cases where there is a suspicion of a breach of personal data protection regulations. Such proceedings may be initiated at the initiative of the supervisory authority, as a result of a complaint from the data subject, or on the basis of other signals of potential breaches. If breaches are revealed during the proceedings, the President of the Personal Data Protection Office is the authority competent to impose an administrative penalty.

The President of the Personal Data Protection Office is also responsible for imposing obligations on data controllers, such as changing data processing practices, deleting data or ensuring appropriate security measures.

These decisions may also include issuing an order to stop processing data in an unlawful manner.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

Penalties for non-compliance, breach or infringement of GDPR provisions are imposed in Poland by the President of the Personal Data Protection Office, **by way of an administrative decision**. When considering each case, the President of the Personal Data Protection Office takes into account all the circumstances of the act committed, approaching the case individually. The funds from the administrative fine constitute income for the state budget (Article 104 of the GDPR).

The GDPR regulations provide for two categories of financial penalties (depending on the type of

misconduct). The penalties contained in the GDPR are not limited to financial penalties, as the President of the Personal Data Protection Office may decide that the penalty will not be financial.

Financial penalties may amount to:

- up to EUR 10 million or 2% of the company's total annual turnover in the previous year – "minor" violations
- up to EUR 20 million or 4% of the company's total annual turnover in the previous year – other infringements.

Fines may also be imposed on organisations processing personal data if a breach of personal data protection occurs. In the event of a breach of the key principles of data processing set out in Article 5 of the GDPR – such as legality, fairness, transparency and data minimisation – or the lack of a legal basis for processing in accordance with Article 6 or Article 9 of the GDPR, the controller may be charged with an administrative fine of up to EUR 20 million. In the case of a company, this fine may amount to up to 4% of its total annual global turnover. A lower fine – up to EUR 10 million (or up to 2% of the company's annual global turnover) – is provided for breach of obligations related to, among others, the implementation of appropriate organisational and technical measures (Article 32 of the GDPR) or failure to carry out a data protection impact assessment (Article 35 of the GDPR).

Under the provisions of the Polish Act on the National Cybersecurity System, the operator of essential services and the provider of digital services are subject to penalties. A financial penalty is imposed, by way of a decision, by the authority competent for cybersecurity. The proceeds from these penalties constitute the income of the Cybersecurity Fund. Due to the limited regulatory regime specified for digital service providers in the NIS Directive, the penalties apply only to issues related to reporting and handling significant incidents, removing vulnerabilities that have led or could have led to a significant incident or acting to the detriment of defense, state security, public safety and order or human life and health. In the light of the provisions of the Directive, it is permissible to impose sanctions in the form of financial penalties on a digital service provider only in the event of violations of national provisions implementing the Directive. However, it is not permissible to introduce penalties for provisions established by the European legislator, i.e. provisions on the security of information systems used to provide digital services specified in Implementing Regulation 2018/151.

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

In Poland there is no tariff for calculating penalties, the penalty is always calculated individually. GDPR states that the penalties imposed should be effective, proportionate and dissuasive, and when determining their amount in each individual case, attention should be paid to the individual criteria for the violation.

The process of arriving at a specific amount is therefore very complicated, so **the Guidelines 04/2022 on the calculation of administrative fines under the GDPR** can provide important guidance (issued by The European Data Protection Board).

When determining the amount of the fine for violating the GDPR, the President of the Polish Personal Data Protection Office pays attention primarily to:

- the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing in question, the number of data subjects affected and the extent of the damage suffered by them;
- intentional or unintentional infringement;
- actions taken to minimize the damage;
- the degree of responsibility of the controller or processor (taking into account the technical and organisational measures implemented);
- previous violations (or lack thereof) by the controller or processor;
- degree of cooperation with the supervisory authority;
- the categories of personal data affected by the breach;
- other aggravating or mitigating factors relevant to the case.

The European Data Protection Board (EDPB) has developed Guidelines 04/2022 on the calculation of administrative pecuniary penalties under the GDPR, adopted on 24 May 2023. The Guidelines include the following methodology for calculating administrative pecuniary penalties:

Step 1	Identification of the processing operation in a given case and assessment of the application of Article 83(3) of the GDPR
Step 2	Establishing a starting point for further calculations based on the assessment of: • Classification as specified in Article 83, sections 4-6 of the GDPR; • The seriousness of the infringement pursuant to Article 83(2)(a), (b) and (g) of the GDPR; • The turnover of the company is one of the essential elements to be taken into account in order to impose an effective, dissuasive and proportionate fine in accordance with Article 83(1) of the GDPR.
Step 3	Assessment of aggravating and mitigating circumstances related to the past or current conduct of the controller/processor and increase or reduce the fine accordingly.
Step 4	Determination of appropriate legal maximum amounts for individual processing operations. Increases applied in previous or subsequent steps may not exceed this amount.
Step 5	Analyse whether the final amount of the calculated fine meets the requirements of effectiveness, dissuasiveness and proportionality, pursuant to Article 83(1) GDPR, and increase or reduce the fine accordingly.

President of the Polish Personal Data Protection Office in

its decisions when calculating and justifying the amounts of fines imposed on data controllers and processors, takes into account the above Guidelines (for example in the decision number: DKN.5112.35.2021 which imposed a penalty on the company for the lack of appropriate technical and organizational measures to ensure the security of data processing in IT systems, resulting in a breach of the principle of integrity and confidentiality and the principle of accountability).

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Sectoral data protection is an exception to the two-instance order in administrative proceedings in Poland. That is, the standard is that before the applicant (entrepreneur or complainant punished by a fine) and the Office move to the level of a dispute in an administrative court, there is a possibility of appeal to a higher body. In the event of a breach of data protection in Polish jurisdiction, there is no higher body than the President of the Personal Data Protection Office, and therefore there is no possibility of appeal to a higher body. Art. 7 of the Act of 10 May 2018 on the protection of personal data states that the proceedings before the President of the Personal Data Protection Office are single-instance.

However, in accordance with Article 78 of the GDPR Regulation, every natural or legal person has the right to an effective remedy before a court against a legally binding decision of a supervisory authority concerning them, therefore **a complaint against the decision of the President of the Personal Data Protection Office may be lodged with the Polish Provincial Administrative Court**. The deadline for filing a complaint is 30 days from the date of delivery of the decision. The complaint should be filed through the President of the Personal Data Protection Office, taking into account the formal requirements and possible allegations regarding the violation of procedural or substantive law.

The Polish Code of Administrative Court Procedure also provides for the possibility of filing a cassation appeal against a judgment or a decision ending the proceedings issued by the Provincial Administrative Court if, during the proceedings, there was a violation of substantive law due to its incorrect interpretation or incorrect application or a violation of procedural provisions, if such an irregularity could have a significant impact on the outcome of the case.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

In 2025, the enforcement priorities of the Office for Personal Data Protection in Poland focus on the protection of privacy in monitoring, compliance with data processing consents, the legality of direct marketing and the security of personal data transfer.

The Office for Personal Data Protection in Poland is applying an increasingly rigorous approach to data protection, is increasing the number of inspections and explanatory proceedings and, in the event of revealing irregularities, is imposing high administrative fines.

The Polish jurisdiction is no exception in identifying threats to the application of data protection mechanisms. This is evidenced by the most recent recommendations of the President of the Personal Data Protection Office, **signaling the ongoing analysis of the service model of Chinese origin and the use of applications and other services offered as part of AI technology combined with IoT technology**. This concerns one of the technologies in the form of a chatbot based on generative artificial intelligence technology, which was introduced to the global market in January 2025, among others as a free application. The main element of this technology is software designed to understand and process human conversations.

In particular, the Polish Personal Data Protection Office analyses and warns about whether the said application operates in accordance with the principles of data processing, whether suppliers ensure the scope and purposes of processing and whether they fulfil the information obligation towards users.

Taking into account the initial findings related to the information provided by the provider in its privacy policy, the President of the Polish Personal Data Protection Office recommends extreme caution in using the application and other services offered as part of the new chatbot. The information contained therein indicates, among other things, that user data may be stored on servers located in a jurisdiction for which the European Commission has not issued a decision stating an adequate level of protection.

The Polish Office for Personal Data Protection also reminds that technologies based on generative artificial intelligence are in principle based on the processing of huge amounts of data that can be used for purposes inconsistent with the user's original wishes, e.g. for further model training or for marketing purposes.

The Polish Office for Personal Data Protection is in contact with other supervisory authorities, which are members of the European Data Protection Board, in order to examine the activities of the chatbot in the EU and their impact on the protection of natural persons in connection with the processing of their data. The Polish Office for Personal Data Protection exchanges information on national actions taken with the supervisory authorities.

It should also be noted that after seven years of transformation of Polish law, the main administrative body for data protection focuses on data processing processes in connection with sectoral solutions under **Digital Markets Act and Digital Services Act**.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

Poland is currently obliged to implement the NIS 2 Directive (2022/2555). The Directive has not yet been implemented into the Polish legal system, although the implementation deadline passed in October 2024.

The NIS 2 Directive currently being implemented applies to key entities such as utility providers, banks, communication companies, and essential entities such as shipping companies, social media platforms, data center providers. The new regulations and requirements will also apply to postal and courier services, waste management, production, processing and distribution of chemicals, production, processing and distribution of food, digital services, scientific research, and trust service providers (including legal services).

Currently, the Act of 5 July 2018 on the National Cybersecurity System implementing the NIS Directive is in force in Poland. Under the current legal status, entities are required to implement a security management system in the information system used to provide a key service. A key service should be understood as a service that is crucial to maintaining critical social or economic activity, listed in the list of key services. Other obligations apply to key service operators, and others to key service providers. The implementation of the NIS 2 Directive is planned for Poland in mid-2025.

The NIS 2 Directive introduces broader and more specific requirements for cybersecurity risk management measures. The obligations on key and important entities will be the same. Under this Directive, **key and important entities will be required to implement appropriate and proportionate technical, operational and organisational measures to**:

- manage the risks to the security of the networks and information systems used by them and
- prevent incidents from affecting the recipients of their services or other services.

According to Article 21(2) of the NIS 2 Directive, cybersecurity risk management measures should take into account all risks and aim to protect network and information systems from incidents.

They should include at least following elements:

a. risk analysis and IT systems security policy;
b. servicing the incidents;
c. business continuity, e.g. backup management, disaster recovery, and crisis management;
d. supply chain security, including security aspects of the relationship between each entity and its direct suppliers or service providers;
e. security in the process of acquiring, developing and maintaining networks and IT systems, including handling and disclosing vulnerabilities;
f. policies and procedures for assessing the effectiveness of cybersecurity risk management measures;
g. cyber hygiene practices and cybersecurity training;
h. policies and procedures for the use of cryptography and, where appropriate, encryption;
i. human resources security, access control policy and asset management;
j. where appropriate, use of multi-factor or continuous authentication, secure voice, text and video calls, and secure intra-entity communications systems in emergency situations.

The above regulations should also be viewed from the perspective of the European Union's legislative initiative in a sectoral approach.

In Poland, legal documents directly applicable in all European Union countries and adopted by the European Union have direct application in cybersecurity.

An example of such a legislative action is the so-called **DORA Regulation**, which is the legal source of such definitions as operational digital resilience, networks and information systems, operational incident of an ICT resource, or cyberattack. This is an example of **an act that is applicable**, for example, to investment firms, payment institutions, managers of alternative investment funds,

electronic money institutions.

The DORA Regulation requires, for example, that financial entities, as part of their comprehensive ICT risk management:

a. at least once a year and after significant changes to ICT systems supporting critical or important functions, test the ICT business continuity plans and the ICT response and recovery plans for ICT systems supporting all functions;
b. test information action plans in the event of a crisis.

This act also imposes the obligation to create procedures and make backup copies as well as to develop methods and procedures for restoring and recovering data.

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

The Act of 5 July 2018 on the National Cybersecurity System regulates the organization and functioning of the national cybersecurity system in Poland. In its current wording, however, it does not contain detailed provisions imposing direct obligations in the field of supply chain management in the context of cybersecurity.

However, attention should be paid to the ongoing process of implementing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, known as NIS 2, which introduces new requirements in this area. The NIS2 Directive expands the scope of entities covered by the regulations and imposes on them obligations related to risk management, **including those related to supply chain security**. In accordance with Article 21 paragraph 2 letter d) of the NIS 2 Directive, key and important entities are required to implement appropriate technical, operational and organizational measures to manage risks to the security of network and information systems, which also include supply chain security.

The implementation of the NIS 2 Directive into the Polish legal order requires an amendment to the Act on the National Cybersecurity System. The draft amendment provides, among others, for an obligation for key and important entities to conduct risk analysis in the supply chain and exclude high-risk suppliers from it.

The amendment to the Act on the National Cybersecurity System, which implements the NIS 2 Directive, extends the obligations in the field of protection of networks and information systems in key sectors, such as energy, transport and digital infrastructure. In particular, critical entities must adapt to the requirements for information security management systems that are compliant with the PN-EN ISO/IEC 27001 and ISO 22301 standards.

In the context of **supply chain security, we can summarise three key obligations** that companies will have to comply with under the new regulations:

a/ Risk assessment: Businesses will need to assess cybersecurity risks not only for their own internal systems, but also for the critical systems of suppliers within their supply chain. This also applies to external partners and suppliers who process sensitive data or provide key services for the operation of the business.

b/ Supplier screening: regulations will require the implementation of strict criteria for selecting suppliers, and contracts must include appropriate cybersecurity measures.

c/ Monitoring: traders will be required to ensure greater transparency of information flows so that each element of the chain is monitored and traceable, thereby preventing fraud, disruptions or cyberattacks in the supply chain.

Essential elements of such supply chain cybersecurity obligations include: risk assessment, business continuity plans, and employee training.

A good example of the sectoral approach to supply chain management obligations is one of the provisions of the DORA Regulation described above, i.e. an act oriented mainly at the financial sector. Namely, Article 29, which, in the obligations to assess the risk of ICT (Information and Communication Technologies) resource concentration, draws attention to the obligation to assess the financial entities' impact of the supply chain **on** the ability to monitor cybersecurity.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

In accordance with the Act of 2 July 2018 on the national cybersecurity system, key entities (operators of key services, digital service providers, public administration units) are obliged to **cooperate and exchange information** on cyber threats with state authorities and other entities within the National Security System and to report incidents (events that have or may have an adverse impact on cybersecurity) to the appropriate CSIRT

(Computer Security Incident Response Team).

In Poland there are 3 of these entities:

- CSIRT GOV – Computer Security Incident Response Team operating at the national level, led by the Head of the Internal Security Agency;
- CSIRT MON – Computer Security Incident Response Team operating at the national level, led by the Minister of National Defence;
- CSIRT NASK – Computer Security Incident Response Team operating at the national level, run by the Scientific and Academic Computer Network – National Research Institute.

Article 48 of the Act on the National Cybersecurity System clearly indicates that key and important organizations must share information on cyber threats and incidents with the appropriate state authorities, especially the CSIRT. In addition, individual CSIRTs are obliged to exchange information with each other in order to ensure the most effective system for responding to cyber threats.

Article 7, section 8 of the Polish Act on the national cybersecurity system states that data from the list of key service operators, to the extent necessary to perform their statutory tasks, shall be made available by the minister responsible for computerization, upon request, to the following entities:

1) authorities competent for cybersecurity; 2) the Police; 3) the Military Gendarmerie; 4) the Border Guard; 5) the Central Anticorruption Bureau; 6) the Internal Security Agency and the Intelligence Agency; 7) the Military Counterintelligence Service and the Military Intelligence Service; 8) courts; 9) the prosecutor's office; 10) authorities of the National Revenue Administration; 11) the director of the Government Security Centre; 12) the State Protection Service.

It should also be noted that CSIRT MON, CSIRT NASK and sectoral cybersecurity teams, when processing personal data specified in Article 9 paragraph 1 of Regulation 2016/679, conduct risk analysis, apply anti-malware protection measures and access control mechanisms, and develop procedures for the secure exchange of information.

However, there are **certain limitations**, namely Article 38 of the Polish Act on the National Cybersecurity System provides for a ban on disclosing information processed under the Act if its disclosure would undermine the protection of the public interest in relation to security or public order, and would also negatively affect the conduct of preparatory proceedings in cases of crimes, their detection and prosecution.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

The Polish Act on the National Cybersecurity System imposes on key service operators and designated public entities the obligation to designate a person responsible for maintaining contacts with entities of the national cybersecurity system. Public administration bodies and local government units may designate such a person.

In addition, the minister responsible for computerization in Poland runs the Single Point of Contact, whose tasks include, among others:

1) receiving reports of a serious incident or a significant incident affecting two or more Member States of the European Union from single points of contact in other Member States of the European Union, as well as forwarding these reports to CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams;

2) forwarding, at the request of the relevant CSIRT MON, CSIRT NASK or CSIRT GOV, reports of a serious incident or a significant incident concerning two or more Member States of the European Union to the single points of contact in other Member States of the European Union.

Additionally, if an organization processes personal data, it may be required to appoint a Personal Data Protection Officer.

The current Personal Data Protection Act specifies that **the appointment of information security administrator is a privilege of the data administrator**. This means that they have the possibility, not the obligation, to appoint information security administrator. The information security administrator has been "replaced" in the Personal Data Act by the data protection officer (DPO). GDPR has changed not only the name of this function, but also the requirements for the person who would perform it in the organization and has expanded the scope of their duties.

Accordingly, in Poland there is an obligation to appoint a person responsible for cybersecurity, but it **mainly applies to key service operators**, public administration units and companies processing personal data.

Moreover, a good example of a micro-scale cyber regulation, i.e. one that interferes with the organisational structure of an enterprise, is Article 5 of the DORA Regulation, i.e. applicable to all financial institutions.

In accordance with this provision, financial entities other than micro-enterprises shall establish a function to monitor arrangements with external ICT service providers regarding the use of ICT services or designate a senior manager as responsible for overseeing related risk exposure and relevant documentation.

In addition, DORA introduces enterprise-level reporting channels, whereby for the purposes of the DORA regulations, it is the financial entity's management body that determines, approves and oversees the implementation of all ICT risk management framework arrangements.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

EU regulations on cybersecurity of operators of key and critical services **in the financial sector** are based on two main pillars: the NIS2 and CER (Critical Entities Resilience) Directives. Both legal acts apply to the same group of entities, but the CER Directive goes beyond purely cybersecurity issues, covering a broader range of issues.

DORA Regulation (Digital Operational Resilience Act) is a more detailed, sectoral legal act that applies exclusively to financial entities. Its main purpose is to supplement regulations such as the NIS2 directives and the GDPR regulations. DORA introduces requirements for the operational resilience of financial institutions to cyber incidents, including the need to implement appropriate risk management and data protection mechanisms.

The NIS2 Directive, which is part of the EU cybersecurity system, is the foundation for the adoption of the Polish Act on the National Cybersecurity System, which covers all providers of key services whose activities are critical to the functioning of the state, such as energy, transport or digital infrastructure.

In Poland, matters concerning cybersecurity of financial institutions have so far been regulated mainly by the PSD2 directive and Recommendation D issued by the Polish Financial Supervision Authority. However, the changes related to the introduction of DORA are aimed at tightening the system, especially in the area of risk management, which is particularly important in the context of the growing number of cyber threats and the need to increase the operational resilience of financial institutions.

In the context of **the healthcare sector**, GDPR plays a key role, as medical institutions process sensitive patient data. According to this regulation, medical institutions must implement appropriate technical and organizational measures to ensure data security, such as data encryption, access control, regular audits and employee training. Additionally, it is necessary to appoint a Data Protection Officer (DPO) in each institution that processes patient personal data.

The National Cybersecurity System Act also has an impact on the healthcare sector. As in other industries, medical facilities that are considered critical entities (e.g. hospitals, clinics) **are required** to comply with information security management requirements, report cybersecurity incidents, and participate in the national information exchange system. It is also required to implement cyberattack protection systems, such as firewalls, monitoring systems, and appropriate incident response procedures.

In the medical sector, the implementation of international standards for information security management (ISO/IEC 27001) and business continuity management (ISO 22301) is particularly important. These standards help medical facilities create comprehensive systems for protecting against cyber threats and ensuring continuity of operation in the event of incidents related to IT security.

In the healthcare sector, in addition to general regulations, there are also specific recommendations and guidelines on cybersecurity. The e-Health Centre, acting on behalf of the Polish Minister of Health, has developed an **Action Plan on Cybersecurity in Healthcare**, which focuses on four key areas:

- protection of medical data;
- email protection;
- network edge protection;
- protection of workstations.

Although these recommendations are not mandatory, they constitute important guidelines for medical facilities in improving their level of IT security.

One of the initiatives from 2024 is the FERC, the Digital Development Fund, which includes improving cybersecurity in healthcare facilities in Poland. The main assumptions are:

a/ Increased financing – Allocating funds for employee

training, implementing patient data protection tools and improving IT infrastructure.

b/ International cooperation – Poland cooperates with institutions such as the European Cybersecurity Agency to create a common framework for protecting health from cyber threats.

c/ Raising data protection standards – Medical facilities must implement procedures compliant with the GDPR to protect patient data.

d/ Cooperation with the private sector – Medical facilities use the services of IT companies providing cybersecurity solutions.

Government administration, including ministries, central offices and local government units, are subject to obligations in the area of information security management and critical infrastructure protection. According to the Polish Act on the National Cybersecurity System, these entities must report cybersecurity incidents to the national system, conduct audits and implement appropriate risk management procedures. Cooperation with the national cybersecurity authority and participation in threat information exchange programs are also important elements.

Public administration processes large amounts of personal data of citizens and is therefore also subject to data protection regulations. According to the GDPR, public entities must apply appropriate data protection measures, conduct data protection impact assessments (DPIAs) and implement privacy policies.

The Polish Act on the Protection of Classified Information concerns the protection of classified information stored in public administration IT systems. It specifies requirements for the security of this information, including requirements related to data encryption, access control, audits and monitoring systems.

On February 28, 2025, the **Digital Poland Project Center** began recruiting for a program that will enable government administration units to modernize their cybersecurity systems. The assistance is directed to entities of the national cybersecurity system, referred to in art. 4 item 7 of the Act of July 5, 2018 on the national cybersecurity system, i.e. the supreme and central government administration bodies and voivodes.

40. What impact do international cybersecurity standards have on local laws and regulations?

International cybersecurity standards have a **significant impact** on shaping local laws and regulations for protecting networks and information systems. These standards provide global guidelines that can be implemented in national legal frameworks, thus enabling harmonization of regulations and increasing digital security on a global scale. The basis for this impact is both international commitments of states and national regulations that adapt to best practices in cybersecurity.

The NIS2 Directive (EU Directive 2022/2555) introduces cybersecurity requirements for key service operators in the European Union. It was adopted as a response to growing threats in cyberspace, and its aim is to raise the level of cybersecurity in the Member States. The NIS2 Directive indicates the need to implement international norms and standards, such as **ISO/IEC 27001**, in order to ensure appropriate information security management.

In Poland, the NIS2 Directive is implemented through the Act on the National Cybersecurity System, which specifies cybersecurity obligations for companies operating in key sectors. Compliance with international standards, such as PN-EN ISO/IEC 27001, is the basis for creating information security management systems, which helps protect against cyber threats and meet legal requirements.

The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council) governs the protection of personal data in the European Union. In the context of cybersecurity, the regulation requires organizations to implement appropriate technical and organizational measures to protect personal data from breaches.

International cybersecurity standards such as ISO/IEC 27001 provide frameworks and tools that enable organizations to comply with GDPR requirements. Implementing these standards in local regulations, such as the Polish Personal Data Protection Act, increases the level of protection of personal data in the context of cyber threats. International standards also support audit processes, which are key to monitoring compliance with GDPR regulations.

In Poland, the basic legal act regulating cybersecurity issues is the Act of 5 July 2018 on the National Cybersecurity System. This Act aims to ensure the protection of critical national infrastructure against cyber threats. It requires public sector entities and companies operating in key sectors such as energy, transport, healthcare or finance to comply with information security management requirements.

The National Cybersecurity System Act refers directly to

international standards such as ISO/IEC 27001, 27032, or 22301. Implementation of these standards helps companies create effective information security management systems that are compliant with national and European requirements. By complying with these standards, national entities can more easily achieve the required level of security, as well as fulfill the obligations resulting from national and international legislation.

International organizations such as ENISA (the EU Cybersecurity Agency) and ISO are developing global standards that facilitate cooperation between countries in countering cyber threats. International cybersecurity standards promote cooperation between countries and organizations to protect against cross-border threats. An example is the cooperation within the so-called Cybersecurity Act in the European Union, which places emphasis on building certification systems compliant with international standards.

ENISA participates in the implementation of the EU's cybersecurity policy. It builds trust in digital products, services and processes by designing cybersecurity certification schemes. It cooperates with EU countries and bodies and helps prepare for cyber challenges.

The Agency works with organisations and businesses to increase trust in the digital economy and the resilience of EU infrastructure, and therefore ensure digital security for EU citizens. It does this by raising awareness, training staff, building structures and raising awareness. The EU Cybersecurity Act has extended the Agency's remit.

International standards such as:

- **ISO/IEC 27001 (for information security management systems)**,
- **ISO/IEC 27032 (for cybersecurity)** and
- **TISAX (for the automotive industry)**

are widely used for security assessment, certification and auditing in various sectors.

In Poland, both the public and private sectors can use certificates of compliance with these standards as proof of compliance with national requirements for information security management. In the financial sector in particular, compliance with these standards makes it easier for organizations to meet the requirements of national laws and regulations, such as statutory requirements for the protection of financial data.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Polish regulations impose obligations to report cybersecurity incidents, especially on key service operators, digital service providers and public administration units.

Regardless of the definitions created by European Union legal acts, such as the DORA regulation, which, for the needs of the financial sector, contains specific definitions of an incident, an ICT-related incident, an operational incident, a cyber threat or a cyberattack and contains the tasks of the leading supervisory authority, which in Poland, in the light of Art. 33 of DORA, is the Polish Financial Supervision Authority, **the Polish Act on the national cybersecurity system defines an incident as an event that has or may have an adverse effect on cybersecurity**.

The Polish Act on the national cybersecurity system also provides for a further division of incidents, classifying them as:

- critical incident – an incident resulting in significant damage to security or public order, international interests, economic interests, the operation of public institutions, civil rights and freedoms or human life and health, classified by the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV;
- serious incident – an incident that causes or may cause a serious reduction in quality or interruption in the continuity of the provision of a key service;
- significant incident – an incident that has a significant impact on the provision of a digital service within the meaning of Article 4 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council with regard to further specifying the elements to be taken into account by digital service providers in managing existing risks to the security of network and information systems and the parameters for determining whether an incident has a significant impact (OJ EU L 26, 31.01.2018, p. 48);
- incident in a public entity – an incident that causes or may cause a reduction in the quality or interruption of the implementation of a public task carried out by a public entity.

Article 11 section 1 point 4 of the Polish Act on the National Cybersecurity System imposes on the operator of the essential service **the obligation to report a serious incident immediately, no later than within 24 hours** from the moment of its detection, to the appropriate CSIRT in electronic form, or, if this is not possible, using other available means of communication. This report must contain:

1. details of the reporting entity, including the entrepreneur's name, number in the relevant register, registered office and address;
2. name, surname, telephone number and e-mail address of the person submitting the report;
3. name, surname, telephone number and e-mail address of the person authorized to provide explanations regarding the reported information;
4. a description of the impact of the serious incident on the provision of the key service, including:
   a. the reporting party's key services affected by the serious incident,
   b. the number of users of the key service affected by the serious incident,
   c. the time of occurrence and detection of the serious incident and its duration,
   d. the geographic scope of the area affected by the serious incident,
   e. the impact of the serious incident on the provision of the key service by other operators of key services and digital service providers,
   f. the cause of the serious incident and the manner in which it took place, as well as the effects of its impact on information systems or key services provided;
5. information enabling the relevant CSIRT MON, CSIRT NASK or CSIRT GOV to determine whether the incident concerns two or more Member States of the European Union;
6. in the event of an incident that could have an impact on the provision of a key service, a description of the causes of the incident, how it occurred and the probable effects of the impact on information systems;
7. information about preventive actions taken;
8. information about corrective actions taken;
9. other important information.

The Polish Act on the National Cybersecurity System also imposes on the digital service provider the obligation to report a significant incident immediately, no later than within 24 hours of detection, to the appropriate CSIRT in electronic form, and in the event that it is not possible to transfer it in electronic form – using other available means of communication. The catalogue of information that this report should contain is similar to that mentioned above.

Article 22 of the Polish Act on the National Cybersecurity System regulates issues related to an **incident in a public entity**. In order to speak of an incident in a public entity, several elements must occur – the occurrence of an event that has or may have an adverse effect on cybersecurity; this event must cause or be able to cause a decrease in quality or interruption of the performance of a public task.

The Act obliges public entities to report incidents in a public entity to the appropriate CSIRT. The legislator specified that the report should be made immediately, no later than 24 hours from the moment of detecting the incident in the public entity. The maximum 24-hour period therefore does not run from the occurrence of the incident, but from its detection, i.e. from the actual receipt of information about the occurrence of the incident. The deadline for reporting is extremely short – immediately, no longer than 24 hours. The rule is therefore to make reports immediately.

In addition, if the incident concerns a breach of personal data protection, the organization is required to report it to the Polish Personal Data Protection Office within 72 hours. And if it poses a high risk to the rights and freedoms of natural persons, the organization must also inform the data subjects thereof.

42. How are cybersecurity laws in your jurisdiction typically enforced?

All EU acts regulating cybersecurity issues delegate the obligation of supervision to a national unit and thus oblige a given country to designate such an authority or contact point. For example, in the situation of operational resilience of the financial sector under the DORA Regulation, in practice the authority responsible for enforcing the regulations is **the Polish Financial Supervision Authority** and it is this financial authority supervising banks, the stock exchange, financial platforms that will perform the tasks as the leading authority indicated in Article 35 of this Regulation.

In turn, when it comes to the Regulation on the European Health Data Space (EHDS), which comprehensively regulates the electronic circulation of health data, this act also delegates the enforcement of the law from this regulation to the authority to be designated by a given country, for example the Ministry of Health or a health insurance fund, and it is this authority that will enforce the cybersecurity regulations, including monitoring,

imposing penalties, enforcing obligations, and control proceedings.

The main responsibility for the implementation and functioning of the National Cybersecurity System is borne by the Council of Ministers, as the supreme body of government administration. It is the Council that, through appropriate legal acts and decisions, shapes the organizational and competence framework of the system. The key role here is played by the Prime Minister, who appoints the Government Plenipotentiary for Cybersecurity.

The Polish Ministry of Digital Affairs plays a key role in the implementation of the National Cybersecurity System, as the authority responsible for civil cybersecurity, and coordinates the implementation of the provisions of the National Cybersecurity System Act and EU directives in this area.

The main tasks of the Ministry include identifying operators of essential services and issuing decisions on recognizing a given entity as an operator. The Ministry of Digital Affairs also maintains a register of operators and supervises their fulfillment of statutory obligations, such as implementing security management systems or reporting incidents.

The Ministry of Digital Affairs is also responsible for cooperation with **digital service providers**, although in their case, due to the cross-border nature of the services, a harmonized regulatory regime at the EU level applies. The Ministry monitors the compliance of providers with security requirements and incident handling.

Government Security Centre (RCB) – performs a coordinating and supervisory function in the field of critical infrastructure protection and response to cybersecurity incidents. The tasks of the Government Security Centre include, among others, supporting the work of the Critical Incident Team, which aims to monitor and manage serious cyber threats in the country. The Government Security Centre cooperates with other state bodies, institutions and international organizations, and also takes action in the event of incidents that may affect national security.

The minister responsible for computerization also carries out his tasks in cooperation with subordinate units (Digital Poland Projects Centre), supervised units (Central Information Technology Centre, Institute of Telecommunications – National Research Institute, Institute of Mathematical Machines, Institute of Innovative Technologies EMAG, Scientific and Academic Computer Network – NASK National Research Institute – NASK PIB) and supervised bodies (President of the Office of Electronic Communications).

In addition, the following solutions operate at the operational level: CSIRT NASK, operating in NASK PIB, is the first Polish team responding to cybersecurity incidents, whose task is to register and handle events that violate network security, and to detect and analyze threats directed against Polish Internet users or threatening the ".pl " domain. CSIRT NASK also cooperates with similar entities around the world, both within the framework of operational activities and research and implementation.

Single Point of Contact (SPOC) – run by the Minister responsible for IT, plays a key role in coordinating cooperation between EU Member States in cybersecurity matters. SPOC deals with receiving reports of serious or significant incidents that affect two or more EU countries. Additionally, SPOC cooperates with law enforcement agencies and the body responsible for personal data protection, especially in the context of cross-border cybersecurity incidents.

Personal Data Protection Office – is responsible for monitoring compliance with the provisions on the processing of personal data, including protection against leakage and unauthorized access to data in the digital environment. In the event of detection of violations of the provisions related to the protection of personal data, Personal Data Protection Office has the power to impose administrative penalties. This body operates in the context of the GDPR, but also in relation to national regulations related to cybersecurity, such as the Act on the National Cybersecurity System.

Head of the Internal Security Agency (ABW) – plays a supervisory role in the protection of state security, including protection against threats in cyberspace. The Head of ABW manages CSIRT GOV (Government Computer Incident Response Team), which monitors and responds to cybersecurity incidents in public institutions. If necessary, the Head of ABW may order an audit of the security of the information system of key service operators. ABW also cooperates with other special services and law enforcement agencies to prevent cyber threats at the national level.

Certification organizations and procedures – Poland also has bodies responsible for certifying cybersecurity products and services, which aim to ensure compliance with applicable standards, such as PN-EN ISO/IEC 27001. Entities operating in the area of critical infrastructure are required to conduct security audits of their systems and to obtain appropriate certificates confirming compliance

with cybersecurity standards.

All these bodies cooperate with each other to ensure effective enforcement of cybersecurity regulations in Poland. In case of violations of the regulations, these bodies have the power to impose administrative, financial sanctions or even conduct criminal proceedings, depending on the severity and nature of the violation.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

It should be pointed out that cybersecurity law provides a very large menu of measures at all stages of the process of detecting threats and the effects of their actual occurrence.

When it comes to cybersecurity in the financial services sector, which is also important for fintechs and ICT providers operating in the EU and in Poland, the performance of all obligations, for example under the DORA Regulation, is enforced through such measures as active acquisition of information from market participants, conducting so-called general investigations, and conducting inspections, including entering into facilities and real estate, exercising ongoing supervision and participating in the harmonization process within the EU agenda, as well as conducting follow-up activities.

In the case of the financial market, a very interesting regulation is the very precise diversification and specification of the competent authority in the European Union to perform and comply with the DORA Regulation in the Polish jurisdiction, where this provision contains as many as 17 references to the competences of authorities in many European Union acts and delegates, in cascade manner, executive and supervisory powers to these acts.

For sectors not covered by comprehensive regulations, reference should be made to the Polish national act implementing the NIS Directive.

Supervision under the Polish act

Pursuant to Article 53 of the Act on the National Cybersecurity System, the entities authorized to apply supervision are:

1. minister responsible for computerization;
2. authorities responsible for cybersecurity in the scope of:
   a. performance by key service operators of their obligations under the Act regarding counteracting cybersecurity threats and reporting serious incidents,
   b. compliance by digital service providers with the security requirements for the digital services they provide, as specified in Implementing Regulation 2018/151, and performance of the obligations arising from the Act regarding the reporting of significant incidents.

As part of their supervision, the above-mentioned bodies have the authority to conduct inspections of the performance of essential services, report serious incidents or verify the compliance of security requirements. In addition, the bodies responsible for cybersecurity have the authority to impose fines on operators of essential services and digital service providers.

Control under the Polish act

The scope of control activities is specified in Article 55 of the Polish Act on the National Cybersecurity System. According to this regulation, the person conducting control activities towards entities that are entrepreneurs has various rights. Such an entity has the right to freely enter and move around the premises of the controlled entity without the obligation to obtain a pass and is entitled to inspect documents concerning the activities of the controlled entity, collect and secure documents related to the scope of the control, in compliance with the provisions on legally protected secrecy. The person conducting the control activities may also prepare copies and extracts from documents necessary for the control. Moreover, to the extent necessary to achieve the purpose of the control, they are authorized to process personal data. The controlling entity has the right to request oral or written explanations in matters concerning the scope of the control, as well as to conduct inspections of devices, media and information systems.

Audit under the Polish act

Pursuant to the Polish Act on the National Cybersecurity System, the operator of a key service is obliged to ensure that a security audit of the information system used to provide the key service is carried out at least once every 2 years.

The audit may be conducted by:

1. a conformity assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on conformity assessment and market surveillance systems (Journal of Laws of 2022, item 1854), to the extent appropriate for undertaking

information system security assessments;
2. at least two auditors with the qualifications specified in the Act on the National Cybersecurity System;
3. sector cybersecurity team.

In accordance with the Polish Act on the National Cybersecurity System, the auditor, based on the collected documents and evidence, prepares a written report on the conducted audit and forwards it to the key service operator together with the documentation from the conducted audit.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

Pursuant to the provisions of the Polish Act on the National Cybersecurity System, entities obliged to ensure an appropriate level of IT security may be subject to **financial sanctions for failure to fulfil the obligations arising from the Act**.

Financial penalties may be imposed on key service operators, i.e. entities operating in strategic sectors of the economy. Their obligations include, among others, systematic risk assessment, effective management of the risk of an incident or implementation of appropriate technical and organizational measures. Failure to perform their obligations may result in the imposition of a financial penalty. **The amount of the penalty depends on the nature and seriousness of the violation**.

Penalties for key service operators range from PLN 15,000 to PLN 200,000. The most severe penalties are provided for:

- Failure to conduct a security audit;
- Failure to implement post-inspection recommendations within the specified time limit.

The Polish Act on the National Cybersecurity System also regulates **digital service providers**. Their obligations mainly include ensuring an appropriate level of security of IT systems, reporting incidents and implementing measures to reduce the risk of cyberattacks. Failure to comply with these obligations may result in a financial penalty of up to PLN 20,000.

Fines are imposed by a decision of the cybersecurity authority. This authority assesses the degree of the breach and the potential threat resulting from non-compliance.

It precisely answers the question of probably the most important postulate of the NIS 2 directive currently implemented in the Polish cybersecurity legal system, that **the means of enforcing cyber regulations**, including administrative **fines**, should be **proportionate** to the violations.

The NIS2 Directive provides for financial penalties, organisational sanctions and management liability for non-compliance.

One of the penalties is a fine of **up to EUR 10 million or 2% of the annual turnover for key entities**.

Then, a maximum of **EUR 7 million or 1.4% of annual turnover is the fine for important entities**.

Additional penalties include management bans and withdrawal of permits or certifications.

It is also necessary to mention the postulated liability of management, where managers can be fined up to 300% of their monthly salary.

A separate group consists of **legal sanctions**, i.e. the consequences of violations, which will be determined as part of the implementation of NIS2 into Polish law.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Penalties and fines for violating cybersecurity rules are calculated **depending on the type of entity and the type of violation**. This is a type of administrative penalty and **there is no** specific binding **calculator** in this matter under Polish law.

For the rules on calculating such fines, the EDPB guidelines 04/2022 can be used.

On 24 May 2023, the European Data Protection Board (EDPB) issued Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

While these guidelines are intended for the purpose of data breaches, they can be used to predict hypothetical breach valuation values in the cybersecurity space as well.

The methodology developed by the EDPB for calculating these fines consists of five steps. First, the processing operations in question must be identified and the application of Article 83(3) of the GDPR must be assessed. Then, the starting point for further calculations of the fine is determined. To this end, the following is

carried out:

- classification of the violation,
- assessing the seriousness of the violation in the context of the circumstances of the case,
- analysis of company turnover.

In the next step, aggravating and mitigating circumstances are assessed, taking into account the past and current conduct of the processor, and the penalty is increased or reduced accordingly. The fourth step consists in identifying the maximum amounts of the penalty provided for by law for the infringement in question. Finally, it is necessary to analyse whether the final amount meets the requirements of **effectiveness**, **dissuasiveness** and **proportionality**.

The presented methodology takes into account, among other things, the nature, gravity and duration of the infringement, as well as the category and turnover of the undertaking.

The regulation of more severe penalties for non-compliance with cybersecurity provisions can also be found in the NIS2 Directive. The NIS2 Directive also assumes that the penalties provided for must be effective, proportionate and dissuasive. This legal act introduces three main types of penalties:

- non-monetary measures,
- administrative penalties,
- financial penalties.

Key aspects include, among others, the gravity and nature of the infringement, its duration, as well as the scope and scale of the damage suffered by individuals or legal entities. An important element is the analysis of the financial benefits obtained by a given entity as a result of the infringement, as well as any previous cases of non-compliance by the same entity.

The aforementioned document introduces the distinction between entities that are key and important for the functioning of the economy and society. Article 34 of the NIS2 Directive regulates the general principles of the requirements for imposing administrative fines on such entities. According to this provision, key entities are subject to fines of a maximum of at least EUR 10,000,000 or at least 2% of the total global turnover in the previous financial year of the company. Important entities are subject to fines of a maximum of at least EUR 7,000,000 or 1.4% of the total annual global turnover in the previous financial year of the company.

The NIS2 Directive introduces the possibility of applying administrative penalties, which can be imposed independently of financial sanctions. The administrative measures available include, among others, temporary suspension of certification or withdrawal of the authorisation to operate in the case of serious infringements.

In addition, supervisory authorities gain the authority to issue binding orders, which may include, among others, the obligation to immediately remove detected violations, implement corrective measures or adapt procedures to applicable cybersecurity standards. As part of their controlling activities, they may also order additional security audits to assess the entity's compliance with regulations and identify potential threats.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

In the light of Polish domestic law, regardless of EU regulations, decisions on imposing financial penalties for violating cybersecurity regulations are issued by the Polish supervisory authority, including the Minister for Computerization. The procedure is carried out under the general principles of administrative procedure. The implementation of the NIS 2 Directive in this respect is left to the Polish authorities for consideration by the European Union, and work in this regard is ongoing. It is important that the decision is subject to judicial review, where the authority is only a party to the case and must present arguments so that the court can examine whether the decision was issued correctly by the administrative authority.

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

Currently, the cybersecurity regulatory landscape in Poland is a legislative initiative catching up with the personal data protection legislation, the creation of which was a priority.

The current legal status in Poland shows a preventive tendency in relation to compulsory instruments for eliminating the effects of violations. There is also a certain mirror image of legal structures created primarily for data protection and not in the origin for cyber protection of computer system space.

The preventive nature of instruments penalizing cybersecurity violations is a common denominator to the technological trend in Poland of distinguishing between

two types of threats. Ransom attacks are different from cyber threats related to espionage activity. Therefore, there is a clear trend to address cyber threats in order to discipline actors in the cyber sector to eliminate threats to systems.

The act implementing the NIS2 directive into the Polish legal system provides for high fines for violating cybersecurity rules. As a result, supervisory authorities, such as the Polish Minister for Information Technology and national cybersecurity institutions, will have greater enforcement powers, including the ability to impose higher financial and administrative fines. The amount of fines provided for in the legal act is significant and is intended to motivate organizations to prioritize security.

In addition, a trend in Poland is the intensification of state cooperation with EU bodies, such as ENISA – the European Cybersecurity Agency. The agency works with organizations and companies to increase trust in the digital economy and the resilience of the EU infrastructure, and thus ensure digital security for EU citizens.

Therefore, it can be said that trends in enforcement activity in Poland focus on increasing the responsibility of entities for cybersecurity. Until the NIS2 directive is implemented, it should be assumed that the authorities will use their powers to impose penalties in a manner similar to the current enforcement of obligations arising from the GDPR.

Contributors

K. Jakub Gładkowski
Attorney, Managing Partner
jg@kg-legal.pl

Barbara Kiełtyka
Attorney, Counsel
bk@kg-legal.pl

Małgorzata Kiełtyka
Attorney, Partner
mk@kg-legal.pl