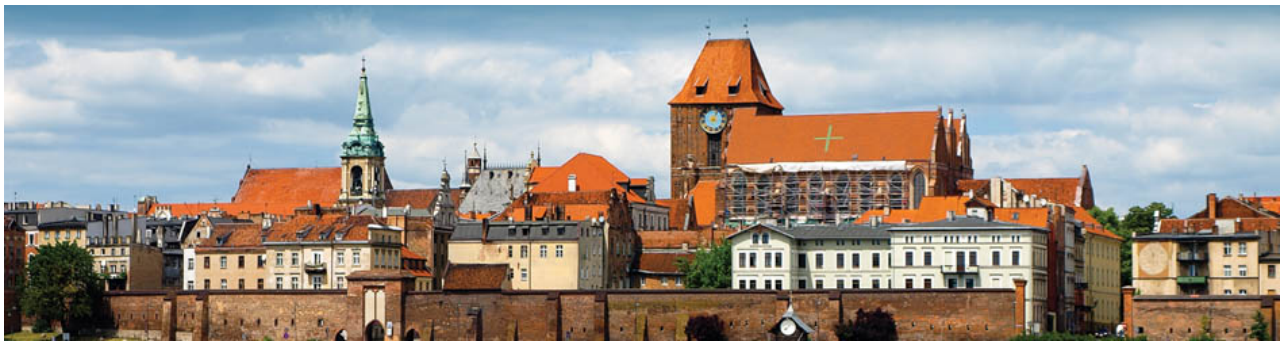
DATA PROTECTION LAWS OF THE WORLD

Poland

DLA PIPER

POLAND



Last modified 15 January 2021

LAW

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

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

Territorial Scope

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

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

As a member of the European Union, Poland implemented the EU Data Protection Directive 95/46/EC in the Personal Data Protection Act of August 29, 1997 (consolidated text: Journal of Laws of 2016, item 922, "**previous PDPA**").

In relation to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**"), on September 12, 2017, two draft acts on personal data protection law were published in Poland. The first one was the draft of the new Personal Data Protection Act of 10 May 2018 (Journal of Laws of 2019, item 1781 ("**PDPA**") which came into force on May 25, 2018, while the second was the Act on the amendments to sectorial acts accompanying the GDPR of 21 February 2019, containing amendments to over 160, sectorial regulations, including banking, insurance and labour law (Journal of Laws of 2019, item 730 "**Implementing act**"), which came into force on 4 May 2019.

The two new pieces of legislation are aimed at implementing the GDPR into the Polish legal order, as well as regulating the matters in which the GDPR leaves a certain regulatory freedom for EU Member States. The new PDPA establishes a new supervisory body – the President of the Office for Personal Data Protection (hereinafter referred to as the "**Polish DPA**"), which has a much wider range of powers than the previous DPA (Inspector General for the Protection of Personal Data – hereinafter referred to as the Inspector General).

A number of provisions of the Telecommunications Act of 16 July 2004 (consolidated text: Journal of Laws 2018, item 1954, hereinafter referred to as the "**Telecommunications Act**") are applicable to the processing of personal data by providers of publicly available telecommunications services and a number of sector specific statutes relating to, among others, employment and banking matters also contain specific regulations on the processing of personal data.

The amendments to the sectorial regulations included in the Implementing act affected, among others, employment, banking and insurance regulations. The act has been passed on February 21, 2019 and entered into force on May 4, 2019.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Implementing act does not include any local derogations to the definitions set out in GDPR.

NATIONAL DATA PROTECTION AUTHORITY

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

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

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

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

The President of the Office for Personal Data Protection.

Office of the President for Personal Data Protection
Urzad Ochrony Danych Osobowych
Stawki 2
00-193 Warsaw
Poland

Tel. +48 22 531 03 00
Fax +48 22 531 03 01
kancelaria@uodo.gov.pl

Helpline (in Polish only): phone no. +48 606-950-000 is open from Monday to Friday from 10 am to 2 pm.

The Office of the President is open from Monday to Friday from 8 am to 4 pm.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the previous PDPA (in force until May 25, 2018), as a general rule, data controllers that process personal data were obligated to notify the Inspector General about the data filing system containing that data. The Inspector General kept a register of data controllers and data filing systems, which was available to the public.

This obligation does not longer exists under the new PDPA and the Implementing act.

DATA PROTECTION OFFICERS

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

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

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger

corporate groups may find it difficult in practice to operate with a single data protection officer).

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

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

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

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

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

According to the new PDPA, the appointment of a Data Protection Officer (DPO) must be notified to the supervisory authority within 14 days. The notification should include the name and email address of the DPO or his or her phone number. Any changes to the information provided or the dismissal of a DPO should also be notified within 14 days. The entity who appointed the DPO shall make available the DPO's details on its website or in a generally accessible manner at a place of pursuit of activity (if it does not have its own website). According to official guidance from the Polish DPA, the contact details of the DPO should be easily accessible, not hidden somewhere in long documents such as a privacy policy etc.

The Implementing act includes the possibility to designate a person to replace the DPO during their absence (*eg* , temporary absence). However, it would be necessary to inform the Polish DPA about the designation in the same way as about the designation of a DPO. All rules and requirements for DPOs, such as the ones stated in article 37 of the GDPR or the obligation to inform the Polish DPA are also applicable to this person.

If a person was officially appointed as an Information Security Officer (ABI) under the previous PDPA, this person automatically became a DPO for the data controller until September 1, 2018, and provided that the appointment was notified to the President of the Office before that date, the person continues to serve as a DPO after that date.

If the data controller is obliged to appoint a DPO in accordance with Article 37 of the GDPR but did not appoint one under the previous PDPA, the appointment of the DPO should have taken place and been notified to the President of the Office before July 31, 2018.

COLLECTION & PROCESSING

Data protection principles

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

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)

- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

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

Legal basis under article 6

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

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special category data

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

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

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

Criminal convictions and offences data

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

Processing for a secondary purpose

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

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

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

Transparency (privacy notices)

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

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

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

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

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

Rights of the data subject

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

Right of access (Article 15)

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

Right to rectify (Article 16)

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

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

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

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

Right to restriction of processing (Article 18)

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

Right to data portability (Article 20)

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

Right to object (Article 21)

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

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

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

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

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law

c. The data subject has given their explicit (*ie,* opt-in) consent

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

The new PDPA includes some derogations from the GDPR. However, the draft of the Implementation act is likely to introduce more provisions which elaborate on the provisions of the GDPR on the collection and processing of personal data. It is important to note that the Polish legislator has decided to include derogations regarding labour law both in the new PDPA and in the Implementation act.

The new PDPA contains provisions amending, among others, the Labour Code. These provisions provide for circumstances under which the employer can carry out video surveillance, email monitoring and other employee monitoring activities. Video surveillance may be implemented if it is necessary to ensure the safety of employees or the protection of property or production control or to keep information, the disclosure of which could cause damage to the employer, confidential. Monitoring of work emails may be implemented if it is necessary to ensure maximum work efficiency and the proper use of work tools made available to the employees. The scope, means and purposes of the employee monitoring must be provided to the employees via workplace regulations or other, exhaustively listed, means at least two weeks before the monitoring starts. The legality of a particular monitoring scheme should be assessed on a case-by-case basis.

The new PDPA also prescribes the maximum retention period of the information obtained from video monitoring (it must not be stored indefinitely). The mater can be retained for three months after the recording took place, unless the recording constitutes (or may constitute) evidence in legal proceedings. In this case, the material may be stored until the final decision in the proceedings is issued. In relation to the retention period of information obtained via any other form of employee monitoring, the general rules of the GDPR apply - the material can be retained as long as is reasonably needed for the purposes for which it was collected. The remaining changes to the Labour Code are included in the Implementation act.

For example, the employer may process the personal data of its employees or job applicants referred to in Article 9(1) with consent however only if the data was given on the data subject's own initiative. Another significant amendment is to the scope of data requested when applying for a job. Although address as well as parents' names are no longer needed, contact details should be provided. Changes in video surveillance would allow an employer to locate cameras in sanitary areas upon prior consent from the enterprise trade union or the employee representative who has been chosen in the way prescribed by an employer. However, the monitoring shall not cover the premises made available to the enterprise trade union.

TRANSFER

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

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, New Zealand and Japan.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

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

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

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

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

In the case of the transfer of personal data to a third country, the Implementing act does not impose any additional requirements concerning notifications to or registrations with the President of the Office.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

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

The Implementing Act does not include any derogations from the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority,

and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

In Poland, the breach notification obligations under the Telecommunications Act were replaced by the breach notification obligations under the terms specified in Commission Regulation (EU) No. 611/2013 of June 24, 2013 regarding measures applicable to notification of personal data breaches under Directive 2002/58/ EC of the European Parliament and of the Council on privacy and electronic communications (Regulation 611/2013).

A personal data breach should be reported by the provider of telecommunications services to the President of the Office immediately, and no later than 24 hours after the detection of the personal data breach. This deadline results from Article 2 section (2) of the Regulation 611/2013. Because this period is shorter than the period indicated in the GDPR, telecommunications undertakings will have to make every effort to send the information required by law within 24, not 72, hours. Therefore, the personal data breach should be notified electronically by filling out the appropriate form.

If a data breach could have a negative impact on the rights of a subscriber or end user (i.e., a natural person), the service provider should also - immediately (i.e., without undue delay) inform the subscriber or end user about the breach (in addition to informing the President of the Office) on terms established in Regulation 611/2013.

ENFORCEMENT

Fines

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

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects' rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The President of the Office is responsible for the enforcement of Polish data protection law and as such is entitled to carry out audits of data controllers in order to determine their compliance with the regulations on the protection of personal data and to impose administrative fines, by means of an administrative decision, pursuant to Article 83 of the GDPR.

The new PDPA provides for a lower level of fines that can be imposed on public authorities for breaching the GDPR – the maximum amount is PLN 100,000 (approx. EUR 25,000).

The new PDPA maintains criminal liability for individuals who process personal data:

- where such processing is forbidden or where he or she is not authorized to carry out such processing; in this

case, the person may be liable to a fine, a partial restriction of liberty, or imprisonment of up to two years (or three years if special categories of personal data are processed).
- and who prevents or hinders the performance of inspection activities conducted by the President of the Office (or its delegated inspectors); in this case the person may be liable to a fine, a restriction of liberty, or imprisonment of up to two years.

As only individuals (and not legal entities) may be prosecuted for criminal offences, the person who may potentially face criminal charges would be a member of the management board (the person performing the role of data controller in a legal entity) or an employee authorized to process personal data (*eg*, a data protection officer or human resources officer).

In 2019, five administrative fines were issued by the Polish DPA.

The first one was issued on 15 March 2019 and concerned a private company processing data gathered from publicly available sources for the purpose of providing its clients with reports on other business entities. As a main concern, the Polish DPA indicated non-compliance with the information obligations from Art. 14 of the GDPR, in particular the exception listed in Art. 14 sec. 5 of the GDPR. As a result, a fine of approximately EUR 220,017 was issued. The company lodged an appeal following the decision. As of December 2019, the administrative court has issued a decision stating that the Polish DPA has to re-examine the amount of fine, but also upholding the main points of the decision, in particular concerning the invalid use of the exception listed in Art. 14 sec. 5 of the GDPR, c and the proceedings are ongoing.

The second fine was issued on 25 April 2019. The case concerned a football association which erroneously made personal data of football referees available, in particular the national personal identification number (PESEL) which is considered sensitive data and indicated as a major risk factor in case of a breach. The amount of fine was EUR 13,000.

The third fine was the highest so far – EUR 660,000. The decision was issued against an online retailer, whose online platform was subject to a hacking attack, resulting in a large amount of personal records to be leaked online. The subsequent proceedings indicated that the organizational and technical measures taken by the retailer were not appropriate to the risk posed by the processing of personal data. Additionally, the Polish DPA questioned the measures taken by the retailer following the incident as inadequate.

The fourth fine was issued against a company providing marketing services (text messages, e-mails, online campaigns)in relation to its complicated procedure for withdrawing the data subject's consent, which was assessed by the Polish DPA as an obstruction of the right to withdraw consent. This company was fined EUR 47,000.

The last fine in 2019 was the first one to be issued against a public entity – a local municipality was fined for not entering into data processing agreements with the external entities to which it transferred personal data. The amount of the administrative fine was approximately EUR 9,328.

In 2020, the Polish DPA issued nine administrative fines. Most of them were connected with a failure to provide information to the Polish DPA or lack of cooperation with the authority.

The first fine was imposed on a school which used a biometric reader at the entrance to its canteen in order to check whether children had paid for their meal. The Polish DPA considered such data processing as disproportionate with respect to its purpose. The school was fined ca. EUR 4,700.

The second fine was imposed on a company from the telemarketing industry as a result of its insufficient cooperation with the authority. This company was fined ca. EUR 4,700.

The third fine was imposed on a person running a nursery and pre-school who failed to provide the Polish DPA with access to personal data and other information necessary for it to perform its tasks - in this case, to assess whether the data controller communicated a data breach to the data subject in accordance with the GDPR. The person was fined ca. EUR 1,700.

The fourth fine was imposed on the owner of a website for failing to provide the DPA with access to personal data and

other information necessary for it to perform its tasks. This was the first cross-border case handled by the Polish DPA. The owner of the website was fined EUR 3,400.

The next two fines were imposed the Surveyor General of Poland ("GGK") in two separate proceedings. The first fine was connected with a failure to provide the supervisory authority - during an inspection - with access to premises, data processing equipment, personal data and information necessary for the Polish DPA to perform its tasks. Furthermore, GGK did not cooperate with the Polish DPA during the inspection. As a result, GGK was fined EUR 22,700. A second fine of the same amount was imposed due to an infringement of the principle of lawfulness of personal data processing and intentionally making personal data available without a legal basis on the Internet (www.geoportal2.pl).

The seventh fine was connected with a personal data breach at the Warsaw University of Life Sciences (SGGW), mainly due to insufficient technical and organisational measures to ensure information security. The university was fined EUR 11,200.

The eighth fine was imposed on a provider of telecommunications services for the lack of appropriate technical and organisational measures to ensure the security of the data it was processing. The company was fined EUR 444,000 – the biggest fine of 2020.

The last fine of 2020 was imposed on an insurance and reinsurance company for the insufficient fulfilment of data breach notification obligations. The Polish DPA received information from a third party about a personal data breach which consisted in the sending by email of an insurance policy by an insurance agent (a data processor of the insurance and reinsurance company) to an unauthorised addressee. Five months after the breach happened, the insurance and reinsurance company itself notified the DPA about the data breach and the two persons affected by it. The Polish DPA considered this as a long-lasting breach, which constitutes an aggravating circumstance, and the company was fined EUR 18,930.

ELECTRONIC MARKETING

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

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

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

Electronic marketing activities are subject to the regulation of Polish data protection law, i.e. the Act of July 18, 2002 on Providing Services by Electronic Means (consolidated text: Journal of Laws of 2018, item 123, hereinafter referred to as the PSEM) and the Telecommunications Act.

The processing of personal data for its own marketing purposes by a data controller (as well as other companies from the group) may be based on Article 6 sec. 1(f) of the GDPR – legitimate interests of the data controller, and it does not

require separate consent. However, the data subject may always object to such processing. Nevertheless, if marketing activities relate to products and services of third parties, prior consent for such processing is necessary.

Apart from consent to the processing of personal data (if it is required), the PSEM imposes an obligation to obtain separate consent to the sending of commercial information by electronic means, (*eg*, by email and SMS) to a specified recipient (natural person). Therefore, a service provider is obliged to obtain the relevant consent before sending the commercial information (by email or SMS) to a natural person. On the other hand, it is permitted to send such information without prior consent to recipients that are legal persons to a general email addresses (such as office@company.com) and to a specific employee's business email address (such as name.surname@company.com). According to the Implementing act, the consent under the PSEM must comply with the GDPR requirements as regards the format. Sending commercial information without consent is considered to be an act of unfair competition and a service provider should be able to provide evidence that it has obtained consent.

Pursuant to the Telecommunications Act, using end telecommunications devices (for instance, to present a marketing offer during a telephone call) or automated calling systems for direct marketing requires the obtaining of another consent declaration from the recipient (subscriber or end user). In practice, the relationship between the abovementioned regulations (especially between the provisions of the new PDPA and the Telecommunications Act) and the scope of particular consent declarations that should be obtained by service providers is not perfectly clear in this regard. However, it seems that, generally, the consent to direct marketing by means of telecommunications devices and automated calling systems should be obtained separately from the consent to the processing of personal data (if required) and to consent to the sending of commercial information by electronic means. According to the Implementing act, the consent of the subscriber or the end user must comply with the GDPR requirements as regards the format.

ONLINE PRIVACY

The Telecommunications Act regulates the collection of transmission and location data and the use of cookies (and similar technologies).

Transmission data

The processing of transmission data (understood as data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data, which should be understood as any data processed in a telecommunications network or as a part of telecommunications services indicating the geographic location of the terminal equipment of a user of publicly available telecommunications services) for marketing telecommunications services or for providing value-added services is permitted if the user (i.e. subscriber or end user) gives his or her consent.

Location data

In order to use data about location (understood as location data beyond the data necessary for message transmission or billing), a provider of publicly available telecommunications services has to:

- Obtain the consent of the user to process data about location concerning this user, which may be withdrawn for a given period or in relation to a given call, or
- Anonymize this data.

A provider of publicly available telecommunications services is obliged to inform the user, prior to receiving its consent, about the type of data about location which is to be processed, about the purpose and time limits of the processing, and whether this data is to be passed on to another entity in order to provide a value-added service.

Processing data about location may only be performed by entities that:

- Are authorized by a public telecommunications network operator
- Are authorized by a provider of publicly available telecommunications services

- Provide a value-added service

Data about location may be processed only for purposes necessary to provide value-added services.

Cookies

The use and storage of cookies and similar technologies is only allowed on the condition that:

- The subscriber or the end user is directly informed in advance in an unambiguous, simple and understandable manner about:
- The purpose of storing and the manner of gaining access to this information
- The possibility to define the condition of the storing or the gaining of access to this information by using settings of the software installed on his or her telecommunications terminal equipment or service configuration
- The subscriber or end user, having obtained the information referred to above, gives his/her consent, and
- The stored information or the gaining of access to this information does not cause changes in the configuration of the subscriber's or end user's telecommunications terminal equipment or in the software installed on this equipment (the end user may grant consent by using the settings of the software installed in the final telecommunications device that he/she uses or by the service configuration)

The consent of the subscriber or end user is not required if storage or gaining access to cookies is necessary for:

- Transmitting a message using a public telecommunications network
- Delivering a service rendered electronically, as required by the subscriber or the end user

Entities providing telecommunications services or services by electronic means may install software on the subscriber's or end user's terminal equipment intended for using these services or use this software, provided that the subscriber or end user:

- Is directly informed, before the installation of the software, in an unambiguous, simple and understandable manner, about the purpose of installing this software and about the manner in which the service provider uses this software
- Is directly informed, in an unambiguous, simple and understandable manner, about the manner in which the software may be removed from the end user's or subscriber's terminal equipment
- Gives its consent to the installation and use of the software prior to its installation

According the current draft of the second act, the consent of the subscriber or the end user must comply with the GDPR requirements as regards the format. The legislative procedure is still ongoing and we will update you once the final version of the amendments takes shape.

Enforcement and sanctions

A company that processes transmission data contrary to the Telecommunications Act or fails to meet obligations to obtain consent to process data about location or to store and to gain access to cookies may be subject to a fine of up to 3% of the company's revenues for the previous calendar year. The fine is imposed by the President of the OEC. In addition, the President of the OEC may impose a fine on a person holding a managerial position in the company (such as a member of the management board) of up to 300% of his or her monthly remuneration.

Enforcement and sanctions

Failing to meet the obligations to obtain consent to direct marketing by means of telecommunications devices and automated calling systems may be subject to a fine of up to 3% of the revenues of the fined company for the previous calendar year. The fine is imposed by the President of the Office of Electronic Communication (hereinafter referred to as the President of the OEC). In addition, the President of the OEC may impose a fine on a person holding a managerial position in the company (such as a member of the management board) of up to 300% of his or her monthly remuneration.

Sending marketing information by electronic means without the consent of the recipient may be subject to a fine of up to

PLN 5,000 (approx. EUR 1,200) under the provisions of the PSEM and is considered to be an act of unfair competition (*ie* , a practice that infringes collective consumer interests) and thus may be subject to a fine of up to 10% of the revenues of the fined company for the previous calendar year (subject to separate regulations).

KEY CONTACTS

Ewa Kurowska-Tober
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +48 22 540 74 1502
ewa.kurowska-tober@dlapiper.com

Lukasz Czynienik
Counsel
T +48 22 540 74 67
lukasz.czynienik@dlapiper.com

DATA PRIVACY TOOL

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