DATA PROTECTION & PRIVACY

INTERNATIONAL SERIES

Monika Kuschewsky
Covington & Burling LLP

THOMSON REUTERS

General Editor
Monika Kuschewsky

Commissioning Editor
Emily Kyriacou
emily.kyriacou@thomsonreuters.com

Commercial Director
Katie Burrington
katie.burrington@thomsonreuters.com

Publishing Editor
Dawn McGovern
dawn.mcgovern@thomsonreuters.com

Editor
Chris Myers
chris@forewords.co.uk

Editorial Publishing Co-ordinator
Gaby Mills-O'Brien
gaby.millso'brien@thomsonreuters.com

Published in August 2016 by Thomson Reuters (Professional) UK Limited, trading as Sweet & Maxwell
Friars House, 160 Blackfriars Road, London, SE1 8EZ
(Registered in England & Wales, Company No 1679046.
Registered Office and address for service:
2nd floor, 1 Mark Square, Leonard Street, London EC2A 4EG)
A CIP catalogue record for this book is available from the British Library.

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY.

ISBN: 9780414057333

CONTENTS

CONTENTS

POLAND

Agata Szeliga and Katarzyna Paziewska | Sołtysiński Kawecki & Szlęzak

1. LEGISLATION

1.1 Name/title of the law

The basic rules on the processing of personal data are set forth in the Act on Personal Data Protection of 29 August 1997 (PDP), which implements EU Data Protection Directive 95/46/EC (the Directive) in the Polish legal system. More specific rules concerning the processing of personal data may be found in other laws, such as the Telecommunications Act, the Labour Code, and banking and insurance Acts, or in regulations concerning medical services or e-services. According to the PDP, if other Acts establish a higher level of personal data protection than the level provided for in the PDP, these Acts will prevail.

1.2 Pending legislation

The adoption of the General Data Protection Regulation (GDPR) and its entry into force in May 2018 will greatly influence the current Polish data protection regime. Pursuant to the Polish data protection authority, the General Inspector for Personal Data Protection (GIODO), approximately 800 Acts will need to be revised and some even repealed to ensure Polish law compliance with the GDPR. Moreover, the GIODO points out that a number of new laws would have to be introduced locally to implement GDPR. The GIODO's organisational structure would also need to be modified to allow him to perform his new duties under the GDPR. At present, there are no draft Bills relating to the GDPR.

The consultation on the draft Act on video surveillance is ongoing. The law will apply to both public and private entities, and will determine the conditions of video surveillance in open public areas, as well as in closed areas designated for public use (such as shops or banks), to ensure safety and public order and to protect people and property. Anybody will have a right to access information about being subjected to video surveillance, and the right to protect their image against distribution. There will be restrictions on the use of video surveillance systems that allow the combination of an image with other data which would lead to the identification of individuals.

1.3 Scope of the law

The PDP is a basic law which applies to data processing through all sectors of the economy. It applies to both public and private entities.

1.3.1 The main players

The PDP defines a "data controller" as a public authority, organisational unit, entity or person who determines the purposes and means of personal data processing. Based on a recent amendment to the PDP, the public authorities who process personal data for the purpose of the same public interest are considered as one data controller. Another category which is clearly defined in the PDP is the "data recipient", which is anyone to whom personal data is disclosed. However, a data recipient does not include the following: the data subject, a person authorised to carry out the data processing, a representative of the data controller from countries not being within the EEA, a data processor, and state authorities or bodies of local government authorities to whom the data is disclosed in connection with ongoing proceedings.

The PDP does not ascribe precise meanings to terms such as "third party", "data processor" or "data subject". These terms may be defined on the basis of other provisions in the PDP, jurisprudence and in light of the Directive. In particular, a "data processor" is viewed as an entity which processes personal data on behalf of the data controller; however, it does not have to be a separate legal entity. For example, a branch office may be a data processor for the headquarters, which is the data controller.

1.3.2 Types of data

Under the PDP, the term "personal data" means any information relating to an identified or identifiable natural person. An "identifiable person" is someone who can be identified directly or indirectly, in particular, by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. Information is not regarded as identifying where the identification would require an unreasonable amount of time, cost or manpower.

Under the PDP, special rules apply to "sensitive data", which is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religion, party or trade union membership; data concerning health, genetic code, addictions or sex life; or data relating to convictions, decisions imposing penalties and fines, and other decisions issued in court or administrative proceedings.

Personal data does not include data on companies, authorities or other bodies. Data belonging to self-employed individuals constitutes personal data. The PDP does not, however, apply to self-employed individuals' personal data that has been made available to the public in the Central Registration and Information on Business Register (CRIB). The only provisions of the PDP that apply to the above data are those relating to the GIODO's power to inspect personal data processing and data security (*see Section 2.2 below*). As regards data not disclosed by the CRIB, the PDP applies fully.

1.3.3 Types of acts/operations

The PDP determines the principles of "personal data processing" as any operation which is performed upon personal data, such as collection, recording, storage, organisation, alteration, disclosure and erasure. The PDP applies to processing in files, indexes, books or other registers; to processing in IT systems; and also when the data is processed outside of a data filing system. The "data filing system" is any structured set of personal data which is accessible pursuant to specific criteria, whether centralised, decentralised or dispersed on a functional basis.

1.3.4 Exceptions

The PDP does not apply to:

- Individuals who process personal data only for personal or domestic purposes.
- Entities having their seat or place of residence outside of the EEA which use technical means located in Poland only for the transit of personal data.

Moreover, except for the provisions concerning the security of processing and inspections, the PDP does not apply to journalistic activity as defined in the Polish Press Act. Nor does the PDP apply to literary and artistic activity, unless the freedom of expression and distribution of information significantly violates the data subject's rights and freedoms. Similarly, only provisions on the security of processing apply to data files prepared ad hoc, exclusively for

technical or training purposes, or in connection with education in high school, where the data is immediately deleted or is anonymised after being used.

1.3.5 Geographical scope of application

The PDP applies to individuals and legal persons, as well as organisational units that are not legal persons, if they are involved in the processing of personal data as a part of their business or professional activity, or in order to implement the statutory objectives, having their seat or place of residence either (i) in Poland or (ii) in a country outside the EEA, provided they are involved in the processing of personal data by means of technical devices (for example, equipment) located in Poland which are not used for the transit of data only. Legal entities which have their core business operations in Poland but perform some operations on such data abroad are obliged to apply the PDP to such operations, irrespective of the application of foreign law, which may impose additional burdens. There is some uncertainty whether the PDP applies to the Polish branch or representative offices of data controllers from other EEA countries. However, most legal commentators agree that the PDP applies to such branches or offices.

1.3.6 Particularities

The civil courts may assess whether the terms and conditions relating to data processing (that is, available online) constitute abusive clauses within the meaning of Directive 93/13. For example, the courts have held that the clause in an online shop's terms and conditions stating that the controller will process the personal data to perform the sale agreement and for marketing purposes infringes consumer interests. This is because the controller has linked the processing for a legitimate purpose (that is performance of the agreement) to marketing purposes without offering the customer the right to opt out of the processing of such personal data for marketing purposes.

In a similar case, the Polish regulator competent for protecting consumer rights fined a data controller for including a consumer's consent to process personal data for marketing purposes and for receiving marketing communication by electronic means in the terms and conditions of an online shop.

2. DATA PROTECTION AUTHORITY

General Inspector for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych)
ul. Stawki 2
00-193 Warszawa
Poland
t +48 22 860 7086
f +48 22 860 7086
e kancelaria@giodo.gov.pl
w www.giodo.gov.pl

2.1 Role and tasks

The GIODO is the state authority responsible for the protection of personal data.

The GIODO's key tasks include:

- Supervising entities to ensure compliance of the data processing with the PDP.

- Issuing administrative decisions (in particular, approving the transfer of personal data to third countries or issuing post-inspection decisions) and reviewing complaints.
- Applying administrative enforcement measures to ensure the performance of non-monetary obligations arising from an administrative decision.
- Keeping a register of data filing systems and providing information regarding registered data filing systems.
- Issuing opinions on bills and regulations relating to the protection of personal data.
- Initiating and undertaking activities to improve the protection of personal data.
- Participating in the work of international organisations and institutions involved in personal data protection.

2.2 Powers

The GIODO and its authorised employees, have the right to access private and public facilities where data filing systems or personal data is kept or processed, and to carry out inspections of such facilities or documents to assess data processing compliance with the PDP. This power has certain limitations and, for example, cannot be exercised regarding data filing systems which include classified information (that is, information the unauthorised disclosure of which will cause damage to Poland or have an adverse effect on its interests).

The GIODO also reviews the complaints and requests made under the PDP.

If the GIODO finds that the PDP has been violated, it may issue an administrative decision ordering the addressee to restore the proper legal status, in particular through completion, updating, correction, disclosure (or not), deletion of personal data or suspension of the data transfer to third countries. Moreover, if the GIODO concludes that a given act or omission constitutes a criminal offence described in the PDP, it must report this offence to the competent authorities.

The GIODO also has the right to apply to other authorities or entities with petitions aimed at ensuring a more appropriate protection of personal data, and the addressee of such petition is required to respond within 30 days of receipt. The GIODO may also request competent authorities to initiate legislative processes or issue opinions regarding bills concerning personal data protection.

2.3 Priorities

The GIODO's priority is to prepare for the GDPR's entry into force. Numerous acts will have to be amended and adopted. The GIODO also reports that matters relating to the recent rapid technological development, such as profiling, biometrics, video surveillance, the Internet of Things, the use of radio identification (RFID) technology and big data, are on his list of priorities. The GIODO wants to intensify his educational activity concerning individual rights and principles of personal data protection by organising meetings, debates and conferences.

In his 2014 annual report, the GIODO indicated that rapid technological changes and globalisation have extended the scope of matters covered by the authority's activities. The issues that the GIODO is now prioritising include:

- Ensuring privacy and personal data protection in profiling.

- Gaining access to data collected by means of RFID technology.
- Protecting individuals' rights regarding use of devices collecting biometric data.
- Gaining access to telecommunications data by police and other governmental authorities.
- Conducting video surveillance.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

A data subject's "consent" is the statement of will specifying his/her consent to the processing of personal data. This consent cannot be implied or derived from a different statement of will. Consent may be revoked at any time. According to jurisprudence, consent is not a valid ground to process personal data in an employment context, unless it is given in a separate document to the employment contract and it may be proven that it has been genuinely given free of coercion (the employee can refuse such consent without having to fear any adverse consequences).

3.1.2 Form

Consent to the processing of sensitive data and the transfer of personal data to third countries which do not ensure an adequate level of personal data protection should be given in writing. When a data subject's written consent is required, it means either a document with a handwritten signature or a document "signed" with a secure electronic signature verifiable by a valid qualified certificate.

Consent to other forms of data processing does not require a special form: it may be given orally or by clicking on the website.

3.2 Other legal grounds for data processing

Personal data may be processed without the data subject's consent if the processing is necessary:

- To exercise the rights and duties resulting from a legal provision.
- To fulfil a contract to which the data subject is a party or to take steps at the data subject's request prior to entering into a contract.
- To perform tasks provided for by law and carried out in the public interest.
- For the purpose of legitimate interests pursued by the data controllers or data recipients, and the processing does not violate the data subject's rights and freedoms. According to the PDP, data controllers' "legitimate interests" are, in particular, the direct marketing of a data controller's own products or services or the enforcement of claims relating to the conducted business activity.

It is prohibited to process sensitive data, save for a few exceptions listed in the PDP:

- The data subject has given his/her written consent, unless the processing consists of the deletion of personal data.

- Specific provisions found within other laws allow the processing of such data without the data subject's consent and provide appropriate safeguards.
- The processing is necessary to protect the data subject's or another person's vital interests where the data subject is physically or legally incapable of giving his/her consent until a guardian or a probation officer is appointed.
- The processing is necessary to carry out the statutory objectives of churches and other religious unions, associations, foundations and other non-profit-seeking organisations, or institutions with a political, scientific, religious, philosophical or trade union aim. To achieve the statutory objectives of the above groups, the processing can only concern the members of those organisations or institutions, or persons who have regular contact with them in connection with their activity, and if appropriate safeguards for the processed data are taken.
- The processing relates to data necessary to pursue a legal claim.
- The processing is necessary to carry out a data controller's obligations with regard to the employment of its employees and other persons, and the law allows that kind of processing.
- The processing is required for preventive medicine, the provision of care or treatment, provided the data is processed by a health-care professional involved in treatment, other health-care services or the management of health-care services and appropriate safeguards are in place.
- The processing relates to personal data which the data subject has made public.
- The processing is necessary for the conducting of scientific research, including the preparations of a thesis required to graduate from university or to receive a degree; however, the results of scientific research must not be published in a way that allows a data subject to be identified.
- The processing is conducted by a party to exercise the rights and duties resulting from decisions issued in court or administrative proceedings.

3.3 Codes of conduct

Several codes of conduct have been implemented in Poland, including codes of conduct regarding:

- The processing of personal data of (potential) customers of motor vehicle distributors.
- Direct marketing activity.
- The banking sector.
- The insurance sector.

The code of conduct on direct marketing activity was prepared upon the initiative of the Polish Association of Direct Marketing, which is a member of FEDMA (Federation of European Direct and Interactive Marketing). The code implements the key bases adopted by FEDMA in its European code of conduct (see the EU Chapter).

Together with the Catholic and Orthodox churches, the GIODO issues guidelines on the application of personal data protection rules in their operations. Moreover, the GIODO has concluded several agreements with various entities active in such sectors as interactive advertising or real estate management on cooperation in promoting the right to personal data protection and the right to privacy. Work on the appropriate codes of conduct was supposed to have commenced within the frameworks of these agreements. The GIODO has also concluded agreements on cooperation regarding privacy and personal data protection with other entities, such as public universities or administrative bodies.

4. SPECIAL RULES

4.1 Employment

The Polish Labour Code modifies the general rules of data processing in employment relationships. An employer may only request that its employees provide the following data:

- First and last names.
- Parents' first names.
- Date of birth.
- Address.
- Education.
- Work history.
- Other personal data, including children's names and dates of birth, to the extent it is necessary for the employee to enjoy the various rights labour law grants him/her.
- Personal identification number (PESEL).
- Other personal data, if the obligation to provide it stems from separate provisions of law.

The employer cannot request any data other than that listed above from an employee, even if the employee expressly agrees to provide such additional data. In particular, even if the employer sends the employee for a temporary medical examination or covers the costs of private medical care, an employer does not have the right to obtain information about the employee's health, except for a statement of whether the employee is capable of performing the work that his/her post requires. However, the GIODO and Polish legal doctrine emphasise that the above provision of the Polish Labour Code should be amended in light of technological development and for the sake of business safety, for example, in banking or transport sectors. The employer may find it necessary to collect employees' personal data, such as geolocalisation data, information on online activity, data included in the references or information from previous workplaces, besides the limited information contained in an employment certificate which an employee is obliged to provide.

The employer may process the personal data which the candidate provided voluntarily during the recruitment process when the candidate gave consent to the further processing of such data during employment. In most cases,

this consent includes the photograph of the candidate. However, such consent should be voluntary and cannot be used to circumvent the rule restricting the scope of personal data which the employer may process.

There are no specific rules concerning Bring Your Own Device (BYOD). However, it is recommended that the use of an employee's device be regulated in a written agreement with the employer or at least in internal employment regulations. The use of social media and the private use of the employer's equipment (including email or hardware) is usually regulated in internal employment regulations. As far as internal investigations are concerned, the business-related content the employee created or received, including email communication, is regarded as the employer's content. Internal investigations should be conducted on the basis of internal employment policies.

4.2 Health

At present, rules on the processing of health-care data may be found in several laws and regulations, including the Act on Patients' Rights, the Ordinance issued by the Ministry of Health on the Kinds and Scope of Medical Documentation, the Act on Physician and Dentist professions, and the respective codes of conduct for the medical professions. The GIODO expressed the view that the laws on medical professional secrecy set forth higher data protection standards and should be applied instead of the PDP.

The Act on Patients' Rights guarantees patients the confidentiality of their medical information and obliges the persons who have access to medical documentation to maintain the secrecy of any information relating to patients, especially their health. The obligation lies with health professionals, support staff and entities providing outsourcing services, which are explicitly regulated.

There are special security requirements which should be met if medical documentation is to be handled in an electronic form. From 1 August 2017, medical documentation will be processed only in electronic form.

4.3 Finance

The provisions of banking law and insurance law concerning banking and insurance secrets set a higher standard of personal data protection than the PDP and thus prevail over the PDP.

A "banking secret" encompasses all information concerning banking operations, where such information is obtained during negotiations or the conclusion and performance of an agreement under which the bank performs such operation, including customers or potential customers' personal data. The obligation to maintain a banking secret lies with the bank, its employees and persons involved in the performance of banking operations. The obligation to maintain a banking secret does not apply in certain cases. For example, the banking secret does not apply towards the person whose information is the subject of the banking secret. Such information may be disclosed to third parties only where the person to whom the information relates authorises the bank in writing to forward the specified information to a given person or organisation, subject to the exceptions stated in banking law (for example, allowing information to be provided to other banks or law enforcement agencies). Courts have also held clauses to be abusive by which a consumer agreed that:

- The bank may give his/her personal data to an unspecified group of entities cooperating with the bank.
- The company may transfer his/her personal data to third countries

Pursuant to insurance law, an insurance company and its employees or persons and entities through which the insurance company performs insurance-related activities, including insurance agents and brokers, are required to maintain secrets concerning particular insurance contracts. According to jurisprudence, an insurance secret encompasses data on particular insurance contracts.

Insurance law lays down a number of specific exceptions from the duty to maintain an insurance secret, for instance, if information concerning the policyholder, the insured, the beneficiary or those entitled under insurance contracts is provided at the request of an entity processing data on the instructions of the insurance company.

4.4 Telecommunications

A telecommunication secret encompasses the user's data, contents of individual messages, transmission data (that is, data processed to transmit messages on telecommunication networks or charging fees for telecommunication services, including location data), non-transmission location data and data on attempted connections between network terminals, including data on failed connections. A telecommunication secret should be kept by the entities participating in telecommunication activity and the entities cooperating with them. A telecommunication company is liable for breach of a telecommunication secret by the entities acting on its behalf.

The operator of publicly available telecommunication services should notify the GIODO of the data protection's security breach (*see Section 10.3 below*).

The operator of a public telecommunication network and the provider of public telecommunication services must, at their own cost, retain and store data (such as: the identity of the terminal initiating connection, and to which the connection is directed; the time, date, type and duration of the connection; and location of the terminal, which is generated in a telecommunications network or processed by them, in the territory of Poland) for 12 months from the day of a successful or attempted connection and destroy the data upon the lapse of that period, except for data secured under separate laws. The obligation to store and retain data has been implemented pursuant to Directive 2006/24/EC (Data Retention Directive), which was declared invalid by the CJEU (*see European Union chapter*). For the time being, there are no plans to remove this obligation.

4.5 Historical, statistical and scientific research purposes

The processing of personal data for research purposes is subject to the general rules with the following modifications. The personal data may be processed for a purpose different from that for which it was collected if this does not infringe data subjects' rights and freedoms and is performed for a scientific, didactic, historical and statistic purpose, provided there are reasons to process the data and the information obligation towards the data subject is observed.

The data controller does not have to inform the data subject if the personal data is processed for scientific, didactic, historical, statistical or archival purposes and the performance of the information obligation would require disproportionate resources. When the personal data is not collected from the data subject, in addition to the exceptions listed above, information is not necessary if the data is necessary for scientific, didactic, historical, statistical or public opinion research and the processing of such data does not violate the rights or freedoms of the data subject, whereas the fulfilment of the information obligation would involve disproportionate efforts or endanger the success of the research; or, if the state or local authorities are processing the data, their organisational units or non-public entities are performing their public duties on the basis of a law.

The processing of sensitive data is permitted for scientific research, including the preparation of a thesis or diploma, or scientific degree; however, the published results of such research should not allow for the identification of the processed data.

There is no obligation to register a data filing system processed only to obtain a diploma or scientific degree.

4.6 Children

The general rules apply. The Polish Civil Code specifies that minors under the age of 13 do not have the capacity to make legal acts and should be represented only by their parents or guardians. Between the ages of 13 and 18, they only have a limited capacity to perform such acts, and the parents/guardians must give consent for the validity of such acts. Consequently, in principle, the parents or guardians should act on the minor's behalf if under 13 years old, or confirm consent for the processing of a minor's personal data between the ages of 13 and 18. Currently, changes are not expected in the light of the GDPR.

4.7 Whistleblowing

There are no specific data protection rules or legal bases to implement whistleblowing schemes. Hotlines may be established for the purpose of legitimate interests pursued by the data controllers or data recipients if the processing does not violate data subjects' rights and freedoms. In practice, data controllers rely on the opinion of the Article 29 Data Protection Working Party (Working Party) (*see EU Chapter*).

4.8 Email, internet and video monitoring

There is no single law in Poland that regulates all aspects of email, internet and video monitoring. Specific issues concerning monitoring may be found in certain legal Acts, such as sports legislation law, legislation on mass events or various criminal laws. However, work on a Bill on the general rules of video monitoring has begun (*see Section 1.2 above*).

In civil law relationships, the rules concerning email, internet and video monitoring are currently derived from the concept of protection of a data subject's so-called "personal interests" expressed in the Civil Code, which includes the right to protect privacy, image and communication secrets, as well as from the PDP, the Telecommunications Act and the Postal Law.

Due to the lack of detailed legal regulations concerning email, internet and video monitoring, the GIODO and the courts usually follow the recommendations expressed in the opinions of the Working Party.

Based on the above, as well as on limited jurisprudence, the following basic rules apply:

- The data subjects must be made aware that monitoring will be performed.
- General rules for the legitimate processing of personal data, such as legitimacy, proportionality and transparency, should be observed.
- The rules of accessing the data collected through the monitoring should be determined.

There are no specific rules concerning the monitoring of employees in Poland, but the GIODO has issued guidelines, which are available on his website, and jurisprudence exists. An employee's consent to such monitoring would not

legitimise such operations because it is likely that the employee will feel forced to give consent so that the consent to such monitoring is not given freely. In practice, the main problem with monitoring employees is related to private use. For example, the constitutional freedom of correspondence may protect email communication. Therefore, the employer's right to monitor an employee's emails differs depending on whether these emails are an employee's private emails or emails sent in connection with an employee's performance of his/her employment obligations. The latter emails are regarded as having been sent on the employer's behalf and the employer may review them without the employee's consent if the above-mentioned conditions are met.

Regarding private emails, they may be reviewed in principle only upon the employee's consent if there are clear provisions of law which allow such review or if the employee abuses his/her freedom of correspondence.

4.9 Direct marketing and cookies

The direct marketing of a data controller's own goods and services is regarded as a legally justified purpose for data processing. Thus, data controllers in principle do not need to procure the consent of data subjects to process their personal data for that purpose – subject to exceptions (*see below*). However, to safeguard the data subjects' interests, the PDP grants a data subject two basic rights. First, the data subject may submit a written reasoned request to stop the processing of his/her data for marketing due to his/her special situation. If the data controller receives such a request, it must either stop processing the data or forward the request to the GIODO, who will issue a decision on the matter.

Secondly, the data subject may raise objections if the data controller intends to process his/her data for direct marketing purposes. If such an objection is filed, the data controller cannot continue to process the data. He/she may only retain the first and last name, address and PESEL number to avoid a situation where that person's data is used again for marketing purposes (the so-called "Robinson" list).

Consent for direct marketing is required in case of the marketing of the data controller's goods or services pursuant to the regulations regarding unsolicited mailing or using telecommunication equipment for marketing purposes.

Retention of information (for example, in the form of so-called "cookies") or accessing such information already retained in the subscriber's or end user's telecommunication terminal equipment is only permitted if:

- The subscriber or end user had received clear and comprehensive information about the purpose of storing and obtaining access to such data, and the possibility of determining the conditions of storage and accessing such data through the settings of the terminal's software or service.
- The subscriber or end user, after receiving such information, agrees to that (whereby such consent may be granted through the settings of the software installed in the terminal or the setting of the service).
- The stored data does not cause changes in the configuration of the terminal equipment or in the software installed on the equipment.

The above rules do not apply if the storage of data or access to the stored data is necessary to perform the transmission through a public network or delivering telecommunication services or services provided via electronic means requested by the end user or the subscriber.

Entities which provide telecommunication services or services through electronic means may install software on an end user's or a subscriber's terminal equipment and use such software. However, before starting such operations, the service provider should give the end user or the subscriber clear and comprehensive information regarding the purposes of the installing the software and the ways in which it will be used, and with information as to how to delete the software. The end user or subscriber should agree to the installation and the service provider's use of such software; however, as mentioned above, consent may be granted through the settings of the software installed in the terminal or the setting of the service.

4.10 Big data

Not applicable.

4.11 Mobile apps

Not applicable.

5. DATA QUALITY REQUIREMENTS

The data controller should protect the interests of data subjects with due care and, in particular, ensure that personal data is:

- Processed lawfully.
- Collected for specified and legitimate purposes and not processed further in a way which is incompatible with the intended purposes, unless stated in the PDP.
- Relevant and adequate for the purposes it is processed.
- Kept in a form which permits the identification of the data subject no longer than is necessary for the purposes for which the data is processed.

The processing of personal data for purposes other than intended at the time of data collection is allowed if it does not violate the data subject's rights and freedoms and is done for the purposes of scientific, didactic, historical or statistical research, or for one of the legitimate purposes of data processing specified in the PDP and the fulfilment of a disclosure obligation.

6. OUTSOURCING AND DUE DILIGENCE

6.1 Outsourcing

Under the PDP, a data controller may entrust a data processor with the processing of personal data. This requires a contract between the data controller and the data processor which should be concluded in writing (this is not the case for the entrustment of personal data between public authorities). The contract should specify the scope and the purpose of the data processing. Moreover, the PDP requires the data processor to implement security measures, and with respect to complying with this obligation, the data processor is liable in the same way as the data controller. The data controller is liable to data subjects or other third parties for the data processor's compliance with the PDP.

Specific outsourcing rules exist in the health-care, banking and telecommunication sectors. There are no specific rules applicable to cloud computing.

6.2 Due diligence

There are no specific rules or guidelines on the effect the data protection law could have on due diligence, but it is quite clear that the PDP applies to the disclosure of personal data during due diligence. The general assumption is that employees' personal data should not be disclosed during due diligence unless absolutely necessary. The data can be transferred only when it is certain that the company itself will also be transferred as part of an asset or share deal. It is considered inappropriate to transfer the data prematurely. Any information about the employees should be disclosed in an anonymised form, unless impossible or unfeasible given the purpose of the transfer. It may be in the legitimate interests of the data controller to provide some personal data during the final/confirmatory due diligence (for example, under specific circumstances it would be acceptable to provide the key management's conditions of employment to the other party of the transaction to allow it to make a final offer). Such disclosure of personal data would be possible only if it does not infringe relevant employees' freedoms and rights. If any personal data is provided, the data provider and data recipient should conclude the agreement in writing. This determines the scope of the data provided, the purpose for which the transferred personal data may be used and the data recipient's obligation to safeguard the personal data.

7. INTERNATIONAL DATA TRANSFERS

7.1 Applicable rules

The transfer of personal data within the EEA is allowed on the basis of the PDP. The transfer of personal data to a third country outside the EEA is allowed if that third country ensures an adequate level of personal data protection, such as the countries which the European Commission has officially recognised as "adequate".

7.2 Legal basis for international data transfers

If a given third country does not ensure the level of personal data protection that the PDP requires, the data controller may still transfer personal data to that country if it can rely on one of the statutory derogations (*see Section 7.2.4 below*). The transfer would also be allowed if these requirements are not met but the GIODO authorises such transfer. The GIODO grants its authorisation if the data controller ensures adequate safeguards regarding the protection of the data subject's privacy, rights and freedoms.

However, the GIODO's authorisation is not required if the data controller ensures adequate safeguards regarding the protection of the data subject's privacy, rights and freedoms by means of:

- A data transfer agreement based on the standard contractual clauses approved by the European Commission under the Directive.
- Legally binding personal data protection principles or policies (binding corporate rules; BCRs) adopted within a given group of companies allowing the data controller/data processor to transfer personal data to another data controller/data processor within the same corporate group in a third country, provided the BCRs as such have been approved by the GIODO.

7.2.1 Data transfer agreements

The PDP does not set any special requirements for data transfer agreements, but the use of the European Commission's standard contractual clauses is common.

7.2.2 Binding corporate rules

The transfer of personal data to third countries which do not ensure an adequate level of personal data protection based on BCRs requires the GIODO's prior approval. Before the GIODO approves the BCRs in question, the authority might consult the appropriate data protection authorities in the EEA countries where the affiliates from that group have their registered seats. When issuing the relevant decision, the GIODO takes into account the outcome of such consultations and might also take into account any earlier decisions by the above authorities regarding the BCRs within the group.

The approval procedure is the same as for transfers of personal data to third countries. The GIODO is not a party to the mutual recognition procedure; however, if the BCRs have been approved by one of the EEA's data protection authorities, the process of approving BCRs in Poland is simplified.

7.2.3 Safe Harbour and Privacy Shield

According to the GIODO's official statement, due to the ruling of the Court of Justice of the EU (CJEU) in the *Schrems* case (*see EU Chapter*), data controllers cannot transfer personal data to the US on the basis of the annulled European Commission's Safe Harbour decision. The GIODO stresses that, currently, personal data transfer to the US requires the fulfilment of one of the conditions specified in the PDP: for example, it is possible to use standard contractual clauses or BCRs approved by the GIODO or rely on the statutory derogations (*see Sections 7.2, 7.2.2 above and Section 7.2.4 below*).

The GIODO emphasises that, at the time his statement was published (11 February 2016), it was necessary to apply alternative data transfer mechanisms when transferring personal data to the US, as the CJEU has decided not to grant a transitional period.

The GIODO has not yet officially commented on the EU–US Privacy Shield.

7.2.4 Other legal bases

The data controller may also transfer personal data to a third country if:

- The transfer is required by legal provisions or by any ratified international agreement.
- The data subject has given his/her written consent.
- The transfer is necessary for the performance of a contract between the data subject and the data controller, or takes place in response to the data subject's request.
- The transfer is necessary to perform a contract concluded for the benefit of the data subject between the data controller and another party.
- The transfer is necessary or required due to public interest or to establish legal claims.
- The transfer is necessary to protect the data subject's vital interests.

- The transfer relates to personal data which is publicly available.

7.3 E-discovery and law enforcement requests

Poland is a party to the Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters. However, Poland made a reservation under the Convention's article 23, that it will not execute letters of request issued to obtain the pre-trial discovery of documents.

Enforcement of business claims is one of the examples of a data controller's legitimate interest under the PDP that may justify the processing of personal data for the purposes of e-discovery and law enforcement requests. Thus, the data controller may process the personal data necessary to enforce its business claims as long as such processing does not infringe the data subject's rights and freedoms. Furthermore, the PDP allows the transfer of personal data to third countries which do not ensure an adequate level of personal data protection if it is necessary to justify legal claims.

7.4 Representative

A data controller from outside the EEA which is processing personal data in Poland should appoint a representative in Poland. Information about the representative (name, address, contact details) should be entered into the data filing system register kept by the GIODO when the registration obligation applies. The PDP does not specify the rights or obligation of such representative.

8. INFORMATION OBLIGATIONS

8.1 Who

Data controllers have information obligations towards data subjects.

8.2 What

The data controller should provide the data subjects with its name and address, together with information regarding the purpose of the data processing, the data recipients or their categories, the rights to access the data and rectify it, as well as whether the data is collected voluntarily or under an obligation arising from law (in the latter case, the legal basis should also be provided). When data controllers collect personal data from persons other than the data subject, in addition to the aforementioned information, they should also inform the data subject about the source of the data and the right to object or request (with reasons) the stopping of the data processing which is carried out for the performance of tasks provided for by law and carried out in the public interest or for the purpose of the legitimate interests pursued by the data controllers or data recipients.

8.3 Exceptions

When the data controller collects personal data directly from the data subject, it does not have to inform him/her if the law allows for personal data processing without the disclosure of the purpose for which the data is collected or if the data subject already has the required information.

Further exemptions apply to the processing of personal data necessary for scientific, didactic, historical, statistical or public opinion (*see Section 4.5 above*).

8.4 When

The data subjects must be informed prior to the collection of their personal data or promptly after recording the personal data collected from a third party. According to legal doctrine, this should be done without delay.

8.5 How

There are no special requirements. For evidence purposes, the written form or email is often used.

9. RIGHTS OF INDIVIDUALS

9.1 Who

The right to control the processing of personal data is vested with data subjects. If the personal data relates to a data subject who is underage or does not have full legal capacity, the general civil law rules of representation apply (*see Section 4.6 above*).

9.2 What

The data subject has the right to control the processing of personal data processed in databases and, in particular, the right to:

(i) Obtain information on whether a database exists and to establish the data controller's identity, the address of its seat (address for individuals) and its full name.

(ii) Obtain information as to the purpose, scope and means of processing the personal data in the database.

(iii) Obtain information since his/her personal data was processed and provide him/her with such information in an intelligible form with the content of the data.

(iv) Obtain information as to the source of his/her personal data, unless the data controller is obliged to keep it confidential as a state, trade or professional secret.

(v) Obtain information about the means in which the data is disclosed and, in particular, about the (categories of) recipients of the data.

(vi) Obtain information about the prerequisites of taking the decision made through automated means of processing.

(vii) Demand that the personal data be completed, updated, rectified, temporarily or permanently suspended or erased if it is incomplete, outdated, untrue or collected in violation of the PDP, or if it is no longer required for the purpose for which it has been collected.

(viii) Demand in writing that the processing of his/her data be blocked, due to his/her particular situation, if the personal data is processed for the performance of tasks provided for by law and carried out in the public interest; or when processing is necessary for the legitimate interests of the data controller or the data recipient.

(ix) Object to the processing of his/her personal data if the data is processed for the performance of tasks provided for by law and carried out in the public interest or when processing is necessary for the purpose of the legitimate

interests of the data controller or data recipient, or the data controller intends to process the personal data for marketing purposes or to transfer the data to another data controller.

(x) Demand that the data controller reconsider his/her individual case in case of automated decision-making.

9.3 Exceptions

The information referred to in items (i)–(vi) of *Section 9.2* above does not have to be provided if it would cause:

- Disclosure of information which includes classified information.
- A threat to state defence or security, the life or health of people or public safety and order.
- A threat to the basic economic or financial interests of the state.
- A significant infringement of data subjects' or other persons' personal interests.

Moreover, there is no obligation to provide information referred to in items (i)–(vi) of *Section 9.2* above more often than once every six months. Finally, if an objection referred to in item (ix) of *Section 9.2* above is raised, the data controller may still process the first and last names, as well as the identification number and the address of the data subject, but only to prevent that person's personal data from being used for the purposes subject to the objection.

Further exemptions apply to the processing of personal data necessary for scientific, didactic, historical, statistical or public opinion (*see Section 4.5 above*).

9.4 When

The data subject may request the information referred to in items (i)–(vi) of *Section 9.2* above once every six months. The information should be provided within 30 days.

If the demand referred to in item (viii) is raised, the data controller must stop processing the questioned data or, without delay, send the request to the GIODO, who will issue a decision.

If the objection referred to in item (ix) is made, the controller must stop processing the personal data.

If the data subject proves that his/her data is incomplete, outdated, untrue or collected in violation of the PDP, or the personal data is no longer required for the purpose for which it has been collected, the data controller should, without delay, correct, update or permanently or temporarily suspend the processing of the data or delete it from the database, unless the request applies to personal data which has been updated, corrected or modified based on different rules.

9.5 How

The data subject may make the request in any form. The data controller should deliver information referred to in items (i)–(vi) of *Section 9.2* above in writing if the data subject makes such request.

9.6 Charges

The PDP does not give the data controller the right to charge the data subject for exercising his/her rights. The courts have confirmed that such charges cannot be levied.

10. SECURITY OF DATA PROCESSING

10.1 Confidentiality

Persons authorised to process personal data are obliged to keep personal data and the ways in which it is protected confidential. That obligation is not limited in time.

10.2 Security requirements

Data controllers and data processors must implement technical and organisational measures to protect the personal data being processed, appropriate to the risks and category of the data being protected.

In particular, they are obligated to protect personal data against: unauthorised disclosure, access by an unauthorised person, processing in violation of the PDP, and any change, loss, damage or destruction.

Detailed security requirements are specified in the Decree issued by the Minister for Internal Affairs and Administration of 29 April 2004. The Decree establishes three security levels for the processing of personal data in an IT system. Each level of security requires implementation of certain security measures. The Decree specifies, in particular, the length of passwords to users' accounts, the frequency of password changes, the main requirements for authorisation methods and the storing of back-up copies.

The PDP obliges data controllers and data processors to keep documentation (namely a security policy and IT system management instruction) describing the way in which personal data is processed and the measures implemented to safeguard the data. Such documentation should be constantly updated. The GIODO has adopted detailed guidelines concerning the content of these documents and these are available on his website.

10.3 Data security breach notification obligation

Under the PDP, there is no obligation to notify the data subjects or the GIODO of any data security breaches. However, the providers of publicly available telecommunication services are obligated by the Telecommunication Act to notify the GIODO of every personal data security breach. If it may adversely affect an individual subscriber or end users, the operator should also notify those individuals.

Data controllers who intentionally or unintentionally violate the obligation to protect personal data against unauthorised takeover, damage or destruction are subject to criminal liability (a fine, the penalty of restriction of liberty or imprisonment for up to one year). As the GIODO is under a statutory obligation to report such offences, even voluntary notification to the GIODO may lead to criminal sanctions. However, the data controllers should balance their risks and the risks of the data subject. In particular, if the data breach relates to data which could easily be used to the detriment of the data subject (for example, if the data could be used to apply for online loans), the data controller should strongly consider notifying the data subjects of the data breach and offer them assistance in protecting their interests.

10.3.1 Who

Providers of publicly available telecommunication services.

10.3.2 What

"Personal data security breaches" are defined as the accidental or illegal destruction, loss, change, unauthorised disclosure or access to personal data processed by the telecom operator in connection with publicly provided available telecommunication services.

10.3.3 Exceptions

A subscriber or end user does not have to be notified if the provider implemented technical and organisational security measures envisaged in personal data laws which make it impossible for unauthorised persons to read the data, and applied those measures to that data the security of which was breached.

10.3.4 When

Without delay but not later than three days from the detection of the breach.

10.3.5 How

The form of notification is not specified. For evidencing purposes, the notification should be made in writing. However, as time may be of the essence, the service provider should make the notification in a form which will mitigate the adverse effect of the breach. The notification should contain, for example, a description of the breach, contact details, information about recommended actions that will mitigate the potential negative consequences of the breach, a description of the consequences of the breach and proposed remedies. In the notification to the GIODO, the provider should also provide information about the risks relating to the breach and whether subscribers or end users were notified.

10.4 Cybersecurity

Not applicable. However, providers of publicly available telecommunication services and, if also appropriate, operators of a public telecommunication network are obliged to implement technical and organisational measures to ensure the safety and integrity of the network, services and transmission of communications in connection with services provided. The measures should ensure security levels adequate to the involved risk, taking into account recent technological advances and the associated implementation costs.

The telecommunication companies may inform other telecommunications companies and entities active in the field of IT security about the identified risks regarding network or service security, and such information may contain the data required for identifying and limiting such risk. The prevailing opinion is that such information does not violate the telecommunication secret.

Telecommunication companies are required to perform tasks for defence, state security and public order. In particular, they need to prepare and update contingency plans.

11. DATA PROTECTION IMPACT ASSESSMENTS, AUDITS AND SEALS

See *Section 13.2* below.

12. REGISTRATION OBLIGATIONS

Data controllers are obliged to register their data filing systems and security information officers (SIOs) if appointed by a data controller. When an SIO is appointed and registered, the SIO is obliged to manage an internal register of data filing systems. The internal register must be available to the public via a website, on the data controller's premises using terminal equipment connected to the IT system or in the form of a printout. If the register is kept in paper form, the SIO is obliged to make it available for inspection by everyone on the data controller's premises.

The register of SIOs is kept by the GIODO. Each data controller who appoints a SIO is obliged to notify this fact to the GIODO.

12.1 Notification requirements

12.1.1 Who

The notification obligations rest with the data controller or, in the case of non-EEA data controllers, their representative.

12.1.2 What

The data controller should submit the data filing system for registration to the GIODO (if applicable) and notify the authority of the appointment or dismissal of an SIO, which the GIODO should then enter into the relevant register.

12.1.3 Exceptions

The data controller is obliged to notify a data filing system for registration to the GIODO except when: (i) the data controller appointed an SIO and notified the appointment to the GIODO (except for data filing systems that include sensitive data, which should be registered by the GIODO); or (ii) in the absence of such SIO, if one of the statutory exemptions from registration applies, namely in case this concerns data filing systems which contain personal data, for example:

- Which the data controller processes in connection with the employment or the provision of services on the grounds of civil law contracts.
- Which refer to persons availing themselves of health-care services, notarial or legal advice, patent agent, tax consultant or auditor services.
- Which are processed to issue an invoice or a bill, or for accounting purposes.
- Which is publicly available.
- Which is processed with regard to minor current everyday affairs.
- Which is processed in data filing systems not kept within an IT system, unless they contain sensitive data.

Furthermore, the data controllers who appointed the SIO and notified the GIODO of such an appointment for registration are not obligated to register data filing systems with the GIODO except for data filing systems containing sensitive data.

12.1.4 When

The GIODO's decision regarding registration of a data filing system containing sensitive data should be obtained before the data controller starts processing that data in the data filing system. With respect to non-sensitive data, the notification should be made prior to the start of data processing, unless the data controller is released from the notification obligation. The data controller should notify the GIODO of any changes in information submitted to the GIODO within 30 days from making the change in the data filing system, except when the data controller extends the scope of processed data to include sensitive data, the data controller should notify the GIODO of that change before it is actually made.

As regards the registration of SIOs, the data controller should notify the GIODO of the appointment and dismissal of the SIO within 30 days from the day of his appointment or dismissal. Any changes in the information submitted to the GIODO concerning the SIO should be notified within 14 days from making such change.

12.1.5 How

The notification of a data filing system should be made in Polish using the standard form which is provided for in the Decree issued by the Minister for Internal Affairs and Administration of 11 December 2008. The notification is submitted to the GIODO as a hard copy, online via the website (*www.giodo.gov.pl*) or by email. If the notification is submitted via the website or email, it should be signed with a secure electronic signature. In the absence of an electronic signature, the applicant should submit a hard copy in addition to the electronic application.

The notification for registration of the data filing system should include:

- The application to enter the data filing system into the register.
- The data controller's name and address, including its identification number in the register of enterprises (REGON), and the legal grounds on which the data controller is authorised to run the data filing system; and in the case of outsourcing or appointing a representative, the name and the address of the data processor or the representative.
- The purpose of the data processing.
- A description of the categories of data subjects and the scope of the data processed.
- Information on the ways and means of data collection and disclosure.
- Information on the recipients or categories of recipients to whom the data may be transferred.
- A description of the technical and organisational measures employed to protect personal data and information regarding the ways and means of fulfilling such technical and organisational conditions.
- Information relating to a possible data transfer to a third country.

The SIO's registration should be made in Polish using the standard form which is provided for in the Decree issued by the Minister for Administration and Digitalisation of 10 December 2014.

The application to register a SIO should include:

- The data controller's name and address, including its REGON if such a number was granted.
- The SIO's data: name and surname, PESEL number or, if this number has not been granted, the type and number of the appropriate document stating the SIO's identity.
- The date of appointment.
- The data controller's statement that the SIO meets the requirements specified in the PDP.

If the application is signed by an attorney, the power of attorney should be attached.

According to the information on the GIODO's website, in 2015, the GIODO received 31,501 notifications and registered 10,737 data filing systems. The duration of the notification process differs and may last from one month to several months.

According to the information on the GIODO's website, there are approximately 18,400 SIOs registered and the number of SIOs is still increasing. The duration of the registration process differs and may last from a few weeks to several months.

12.1.6 Charges

Not applicable.

12.2 Authorisation requirements

12.2.1 Who

The obligation to obtain authorisation rests with the data controllers.

12.2.2 What

At present, authorisation is required for the transfer of personal data to a third country outside the EEA which does not ensure an adequate level of personal data protection.

12.2.3 Exceptions

If the transfer can be based on one of the statutory exceptions (*see Sections 7.2, 7.2.2 and 7.2.4 above*), authorisation is not required.

12.2.4 When

The GIODO's authorisation for the transfer of personal data to third countries should be procured before the transfer takes place. It is not necessary to renew such authorisation.

12.2.5 How

To obtain the approval of the data transfer, the applicant should file an application with the GIODO. The application should be made in Polish. There is no standard form for this application. The application is submitted to the GIODO in a hard copy, or online via the website or via email. If the notification is submitted via the website or email, it should be signed with a secure electronic signature. In the absence of an electronic signature, the applicant should submit a hard copy in addition to the electronic application.

If the application is signed by an attorney, the power of attorney should be attached to the notification.

In 2015, GIODO issued 48 authorisations of data transfers to third countries. The duration of the authorisation proceedings differs, but usually lasts several months.

12.2.6 Charges

The issuance of the decision is subject to a fee in the amount of PLN 10 (approximately EUR 2.5). The fee should be paid to the GIODO when the application is submitted.

12.3 Other registration requirements

Not applicable.

12.4 Register

The registers of data filing systems and SIOs kept by the GIODO are publically available and can be accessed at *www.giodo.gov.pl*. The register of data filing systems contains data included in the notification form except for a description of the technical and organisational measures employed to protect personal data, and information regarding the ways and means of fulfilling such technical and organisational requirements (*see Section 12.1.5 above*).

The register of SIOs contains data included in the application form except for the date of appointment, the PESEL number (or number of the appropriate identification document) and the data controller's statement (*see Section 12.1.5 above*).

The internal register of data filing systems that are kept by data controllers who appointed and registered the SIO should also be available to the public and should include the same scope of information (*see above and Section 12.1.5*).

13. DATA PROTECTION OFFICER

13.1 Function recognised by law

The data controller may appoint an SIO. This function may be performed only by an individual. If the data controller does not appoint an SIO, the data controller performs the duties of the SIO himself (with a few exceptions). When a company does not appoint an SIO, the members of the management board should perform such duties.

The SIO should have full legal capacity, enjoy full public rights and have appropriate knowledge regarding personal data protection. The SIO cannot have a criminal record for an intentional offence. The data controller may also appoint substitute SIOs.

13.2 Tasks and powers

The SIO must be independent and reports directly to the head of an organisational unit – for example, to the members of the management board of a given company. The entity should provide the SIO with organisational autonomy and appropriate tools to ensure the proper performance of the SIO's duties; the SIO may also perform

other duties not relating to personal data protection, insofar as this does not impede or compromise the due performance of the duties set out in the PDP.

The SIO performs all obligations regarding personal data protection, including:

- Verifying the compliance of personal data processing with data protection laws.
- Conducting internal audits and drawing up reports for the data controller or the GIODO concerning compliance with personal data protection laws.
- Supervising, drafting and updating data protection documentation and supervising compliance with the principles indicated in such documentation.
- Ensuring that the persons authorised to process personal data are acquainted with the provisions on the protection of personal data.
- Keeping a register of data filing systems containing personal data processed by the data controller (*see Section 12 above*).

The SIO is obliged to prepare a plan of inspections (audits). The plan should cover a period no shorter than a quarter and no longer than a year, and provide for at least one internal audit. The SIO should prepare a report on the internal audit and submit it to the data controller.

Besides conducting scheduled audits, the SIO is also entitled to conduct ad hoc audits in cases not provided for in the inspection plan whenever the SIO receives information of a breach of personal data security or arrives at a reasonable suspicion that such breach might have occurred.

In addition, the GIODO may ask the SIO to carry out an internal audit in the company's structure and to prepare a report for the authority. Regardless of such audits by the SIO, the GIODO may still conduct regular inspections of the data controller.

If the data controller does not appoint the SIO, the data controller has no obligation to prepare audit plans and cannot be requested by the GIODO to carry out an internal audit and prepare a report for the authority.

14. ENFORCEMENT AND SANCTIONS

14.1 Enforcement action

The GIODO may issue a decision obliging the addressee to comply with the PDP. In particular, the GIODO may demand that the personal data be completed, updated, corrected, disclosed or not disclosed to a third party. The GIODO may also suspend the transfer of personal data to third countries or order that the data be deleted. The decisions may be issued upon the request of an interested party or *ex officio*. In 2015, the GIODO issued 57 decisions in relation to its inspections, while 646 decisions were issued as a result of complaints of interested parties.

The GIODO has the power to enforce non-pecuniary obligations arising from its decisions through administrative enforcement proceedings. In 2015, the GIODO issued 27 decisions ordering performance and these were subject to administrative enforcement.

The GIODO is also obliged to report offences relating to the processing of personal data to competent law enforcement authorities. In 2015, GIODO reported 24 offences (more than a 100% increase compared to the previous year). In the first half of 2016, it has already reported 18 offences.

14.2 Sanctions

The PDP provides for criminal sanctions such as fines, the restriction of liberty or imprisonment. These may be imposed in the following cases:

- Where personal data has been processed in a data filing system when such processing is not allowed or a person who processes the data is not authorised to perform such processing.
- Where personal data has been disclosed or unauthorised persons have been given access to personal data by a data controller or the person obliged to protect personal data, for instance an SIO.
- Where a data controller or the person obliged to protect personal data has failed to protect personal data against unauthorised takeover, damage or destruction.
- Where a data filing system has not been registered.
- Where a data controller fails to inform the data subject about his/her rights.
- Where an inspection has been obstructed.

The GIODO does not currently have the right to impose financial penalties for violations under the PDP. However, if its decisions are not complied with within set deadlines, it may impose an enforcement penalty in the amount of PLN 50,000 (approximately EUR 11,760) on legal entities and organisations, which may be increased up to PLN 200,000 (approximately EUR 47,000) in total. Pursuant to the GIODO's 2015 Annual Report, such enforcement fines were imposed in 2014 in two cases in the amount of PLN 25,000 (approximately EUR 5,895) in each case. In 2015, enforcement fines were repeated – in both cases the fines amounted to PLN 40,000 (approximately EUR 9,434).

14.3 Examples of recent enforcement of data protection rules

The PDP is enforced in practice. The GIODO acts through its decisions, which are subject to judicial control. In 2015, the administrative courts issued 212 rulings in cases concerning the GIODO.

For instance, in one ruling the administrative court analysed the case when the bank's client objected to his personal data being processed for marketing purposes. The bank received the objection, but continued to post marketing advertisements of the bank's product on the client's personal online account. The court held that the online account is a personalised channel of communication with a client, and therefore each client may expect to receive personalised information from his/her bank. If, after logging on to the personal online account, the customer sees advertisements of bank's products, this confirms that the bank is performing operations on his/her personal data for marketing purposes. If the customer objects to the processing of his/her personal data for marketing purposes, the bank should not send marketing materials to the client's online account.

In another ruling, the Supreme Administrative Court analysed the GIODO's decision concerning the disclosure of an internet user's personal data. The National Museum in Warsaw claimed that a user posted on the internet

forum comments which infringed the Museum's so-called "personal interest". The GIODO ordered the forum's administrator to disclose the user's personal data to the Museum, as in GIODO's view such disclosure was justified by legitimate interests pursued by the Museum and the processing of the user's personal data did not violate the data subject's rights and freedoms (the Museum stated that it intends to bring a civil action against the user). The Supreme Administrative Court did not agree with the GIODO's view and stated that the GIODO should pay more attention to balancing the interests of the data subject and the data controller. The GIODO should analyse each case and verify whether: (i) the legal basis for bringing a civil action against a user is reasonably justified; and (ii) the intention to sue the user is real. This means that GIODO should assess whether there is any "hidden" intention behind the request to disclose the user's personal data.

The GIODO also reports offences relating to data processing to the competent law enforcement authorities. However, most of these notifications are not pursued by the law enforcement authorities. For example, in 2015, five investigations were discontinued, and in five cases the authorities refused to start the investigations and no conviction (or conditional discontinuation of the proceedings) was issued.

15. REMEDIES AND LIABILITY

15.1 Judicial remedies

The addressee of a decision issued by the GIODO has the right to apply to the GIODO for re-examination of the case. The decision issued by the GIODO after such re-examination may be challenged by the party before the administrative court of first instance. Both the GIODO and the other party may appeal against such ruling to the Supreme Administrative Court.

Data subjects and other competent authorities, for example the Office of Competition and Consumer Protection, may challenge the clauses concerning personal data processing contained in the terms and conditions or regulations used by business entities (*see Section 1.3.6 above*).

Data subjects may also challenge the violation of their personal data through civil proceedings (*see Section 15.3 below*).

15.2 Class actions

As a legal instrument, class actions are not very popular in Poland. The first cases brought did not refer to personal data processing.

15.3 Liability

The data controller is primarily liable for damages resulting from a breach of the PDP. Moreover, the data controller may also be liable with respect to the violation of the provisions of the PDP which regulate the protection of personal data and the implementation of appropriate technical and organisational measures for protecting the personal data.

The liability for damages resulting from a breach of the PDP is based on the general principles of Polish civil law as the PDP does not contain any specific regulations in this respect. In principle, claims for compensation or damages may be based on two legal principles. The first is the infringement of the data subject's so-called "personal interest",

which includes, for example, the right to privacy. A data subject whose personal interests are infringed may claim non-pecuniary compensation or claim damages based on general rules. Court awards of compensation are not substantial. For example, in 2013, the court awarded two claimants compensation in the amount of PLN 2,000 (approximately EUR 470) each, instead of the claimed PLN 15,000 (approximately EUR 3,530), for the unauthorised disclosure of their personal data by a housing community (defendant) which the court held violated their personal interests. Local authorities had to pay the same amount of compensation for the unauthorised disclosure of personal data to a bank, which subsequently used it to bring claims against its clients. In another case, the court found that the request for compensation in the amount of PLN 10,000 (approximately EUR 2,350) for using a claimant's email once to send unsolicited communication was excessive, and that the defendant's voluntary payment of PLN 500 (approximately EUR 118) to the foundation indicated by the claimant together with apologies was sufficient.

In 2015, the court awarded the claimant, a public transport ticket inspector, compensation in the amount of PLN 25,000 (approximately EUR 5,880) for the unauthorised disclosure of his personal data by a newspaper. The claimant did not give consent for the publication of his personal data, including his name, surname and health information, in an article describing an attack upon the victim in which the victim was bitten by an aggressive HIV-positive passenger. The court decided that the editor's conduct was negligent and therefore constituted an infringement of the plaintiff's right to privacy.

In another case in 2015, the court awarded compensation in the amount of PLN 15,000 (approximately EUR 3,530), instead of the requested amount of PLN 50,000 (approximately EUR 11,760), to a claimant whose personal data (including name and surname) was disclosed unlawfully by local authorities on their official website containing resolutions and protocols of the municipal council. The court stated that such disclosure infringed the claimant's personal rights, as the universal right to access public information is limited by individual rights to privacy (unless the concerned person consents to such disclosure or performs a public function).

In employment relationships, the courts are inclined to award higher levels of compensation. In particular, the court awarded compensation of approximately PLN 11,000 (approximately EUR 2,590), instead of the requested PLN 40,950 (approximately EUR 9,630), to a former employee for infringement of his personal interests, including the unauthorised disclosure of personal data from the former employer (a bank). The case involved another employee of the bank sending an email to all persons working in the same branch office containing information regarding the termination of the claimant's employment contract and the fact that the termination was justified by the claimant's lack of effectiveness in selling bank products. The court found that such act violated the PDP.

The second basis of damage claims is tortious liability; however, this has not been used in practice so far. Moreover, if the data subject and the data controller are bound by a contract, the data subject may potentially raise claims for damages arising from the breach of such contract.

Claims for damages resulting from a breach of the PDP are not very common. In practice, they usually accompany claims for compensation for the infringement of personal interest. Therefore, it is difficult to identify the precise amount of damages awarded for a breach of the PDP.