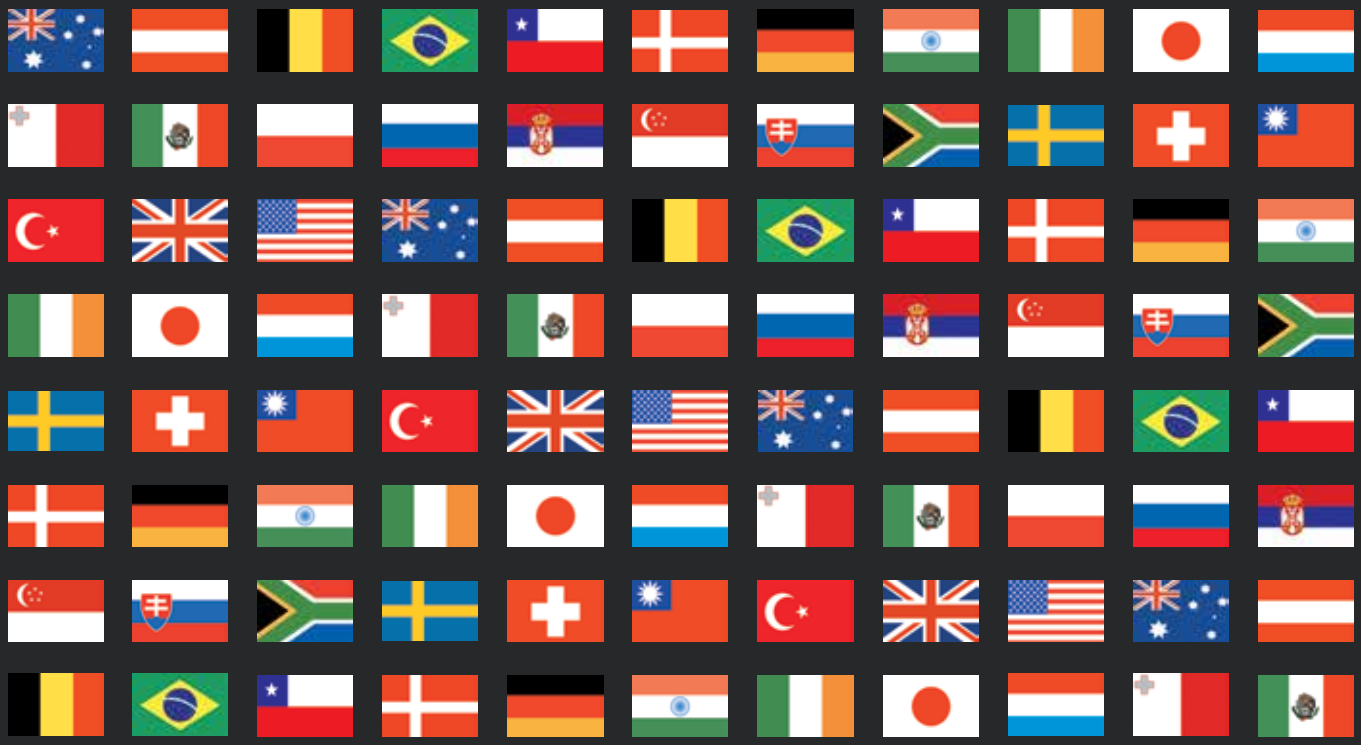
Data Protection & Privacy

Contributing editor
Wim Nauwelaerts



2017

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2017

Contributing editor
Wim Nauwelaerts
Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Fifth edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Poland

Arwid Mednis and Gerard Karp
Wierzbowski Eversheds

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The Polish Personal Data Protection Act of 29 August 1997, (PDPA) is the primary legislation concerning data protection in Poland. The PDPA is the adoption of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The European Convention on Human Rights and Fundamental Freedoms was ratified in 1993. The European Court of Human Rights has jurisdiction over the cases of Convention breaches.

In 2002 Poland also ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

There are eight executive regulations issued on the basis of the PDPA, including the Regulation of 29 April 2004 by the Minister of Internal Affairs and Administration (the Regulation) as regards personal data processing documentation and technical and organisational conditions that should be fulfilled by devices and computer systems used for personal data processing.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Polish data protection authority is the Inspector General for Data Protection (DPA). The DPA's duties include:

- supervising conformity of data processing with the personal data protection legislation;
- issuing administrative decisions and reviewing complaints in cases involving enforcement of the personal data protection legislation;
- ensuring that non-monetary obligations arising from the issued decisions are performed by the obligees by applying the enforcement measures provided for in the Regulation; and
- maintaining a register of filing systems and providing information on the registered filing systems.

The DPA, as well as the authorised employees of the DPA's bureau, to properly supervise data processing and ensure that all legal obligation relating to personal data processing are fulfilled, may:

- access premises in which data is processed;
- request written or oral explanations and summon and interrogate persons insofar as may be necessary to determine the facts;
- review any documents and any data directly associated with the subject matter of the inspection and make copies thereof;
- inspect devices, media and computer systems used for the processing of data; and
- request expert opinion and evaluation.

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

A violation of rules stipulated by the PDPA (and other statutory, if applicable) may result in both administrative and criminal liability.

The authority responsible for compliance of data processing with the provisions on the protection of personal data is the DPA.

The DPA may issue a decision requiring the data controller to cease processing and delete the personal data collected. It may also impose an administrative fine in case of non-compliance with the decision.

The PDPA contains criminal sanctions for a data controller that illegally processes data, including fines, restrictions of personal liberty or imprisonment for up to three years.

Criminal proceedings are handled by the prosecutor's office.

Also, under Polish Civil Code, unlawful processing may be subject to a civil lawsuit.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The PDPA provides for certain exceptions, (ie, there are entities or areas of activity to which it does not apply). These exceptions are:

- natural persons involved in the processing of data exclusively for personal or domestic purposes;
- entities having their seat or residing in a third country that use technical means located within the territory of the Republic of Poland exclusively for the transfer of data;
- press journalistic activity within the meaning of the Act of 26 January 1984 – the Press Law – and literary and artistic activity, unless the freedom of expression and information dissemination considerably violates the rights and freedoms of the data subject (however, provisions of the PDPA regarding the supervision and competences of the DPA, as well as the provisions specifying the security obligations of the data controller still apply); and
- any cases where an international agreement to which the Republic of Poland is a party provides for otherwise.

If any separate laws on the processing of data provide for more extensive protection of the personal data than the provisions of the PDPA, then the provisions of such laws providing more extensive protection take precedence. This does not mean that the PDPA will not apply in any matters unregulated by such laws.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The PDPA and executive regulations do not wholly cover interception of communications, electronic marketing or monitoring and surveillance of individuals. Relevant laws in this regard are:

- the Act of 16 July 2004 – the Telecommunications Law (TL);
- the Act of 18 July 2002 on Electronically Supplied Services (ESSA); and
- the Act on Visual Monitoring (which is currently only a draft making its way through the legislation procedure, so it is impossible to estimate when the it will enter into force).

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas?

The most important regulations that provide specific data protection rules are those regarding: banking law, labour law, regulations on employee documentation, regulations on medical documentation, insurance law, capital markets law, payment services, statistical information and record-keeping, and regulations regarding civil and national security (eg, concerning the police, foreigners, criminal records, mass events, the Central Anti-Corruption Bureau).

7 PII formats

What forms of PII are covered by the law?

The PDPA applies to the following format of processing PII:

- files, indexes, books, lists and other registers; and
- computer systems, also in cases where data are processed outside from a data filing system.

It should be noted that, according to article 2 clause 3 of the PDPA, as regards personal data files that are prepared ad hoc, exclusively for technical, training, or higher education purposes, where the data are immediately removed or rendered anonymous after being used, only the provisions of the PDPA specifying security obligations apply.

8 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Applicability of the PDPA is extended beyond the territory of Poland. Namely, the PDPA applies also to natural and legal persons and organisational units not being legal persons who process personal data as part of their business or professional activity or the implementation of statutory objectives that have their seat or reside in a third country – if such processing of personal data is performed with the use of technical means located within the territory of the Republic of Poland.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?

The PDPA constitutes the general and most important piece of legislation in the scope of personal data protection. It is only superseded by other laws to the extent that they provide for more detailed provisions.

The PDPA covers all processing and use of the PII. There is also a distinction between the data controller (ie, the person or entity who decides upon the purposes of means of personal data processing) and the data processor, who processes the personal data for and on behalf of the data controller, and on the basis of a written agreement. The data processor is not authorised to make decisions with regard to the purposes and means of the data processing. For detailed information on entrusting the personal data for processing, see question 30.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes, Polish law requires that the holding of PII has specific legal ground for processing of personal data. Pursuant to article 23 of the PDPA, the processing of personal data is only permitted on the condition that one of the legal grounds listed in that provision applies. Those legal grounds are as follows:

- the data subject has given his or her consent, unless the processing consists of erasure of personal data;
- processing is necessary for the purpose of exercise of rights and duties resulting from a legal provision;
- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for the performance of tasks provided for by law and carried out in the public interest; or
- processing is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject.

Stricter grounds are stipulated for processing of sensitive personal data.

11 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Yes, Polish law imposes more stringent rules for processing of sensitive data (eg, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade union membership) as well as the processing of data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued in court or administrative proceedings. For example, processing of sensitive data shall not constitute a breach of PDPA where:

- the data subject has given written consent;
- processing relates to the data necessary to pursue a legal claim;
- provisions of the other statues allow processing of such data;
- processing is required for medical and health purposes;
- processing is necessary for employment issues;
- processing is to conduct scientific research including preparation of a thesis required for graduating from university or receiving a degree; and
- processing relates to personal data that were made publicly available.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Yes. The law requires owners of PII to notify individuals about the fact that their data are being processed. Pursuant to article 24 of the PDPA, in cases where personal data are collected from the data subject, the controller is obliged to provide the data subject from whom the data are collected with the following information:

- the address of its seat and its full name, and, in case the controller is a natural person, about the address of his or her residence and his or her full name;
- the purpose of data collection, and, in particular, about the data recipients or categories of recipients, if known at the date of collecting;
- the existence of the data subject's right of access to his or her data and the right to rectify these data; and
- whether providing personal data is obligatory or voluntary, and in case of the existence of an obligation – about its legal basis.

Whereas, in cases where the data have not been obtained from the data subject, pursuant to article 25 of the PDPA, the controller is obliged to provide the data subject, immediately after the recording of his or her personal

data, all the information listed in the bullet points above and, additionally, of the source of data and the data subject's rights stemming from article 32 clause 1 point 7 and 8 (including the right to object to data processing).

13 Exemption from notification

When is notice not required?

In a case where personal data are collected from the data subject, the controller is not obliged to provide the data subject with the proper notice if:

- any provision of another law allows for personal data processing without disclosure of the real purpose for which the data are collected; or
- when the data subject already has the proper information (as described in question 12).

In a case where the personal data have not been obtained from the data subject, the controller is not obliged to provide the data subject with the proper notice if:

- the provision of another law provides or allows for personal data collection without the need to notify the data subject;
- the data are necessary for scientific, didactic, historical, statistical or public opinion research, the processing of such data does not violate the rights or freedoms of the data subject, and the fulfilment of the terms and conditions for providing the proper notice would involve disproportionate efforts or endanger the success of the research;
- the data are processed by the PII on the basis of legal provisions; and
- the data subject already has the proper information.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Yes, the owners of PII are obliged to ensure individuals exercise their statutory rights. Data subjects may: withdraw previous consent to processing; object to the processing of their personal data; ask for incorrect or incomplete data to be corrected or updated; and in some situations can take action to prevent further processing or to claim damages for breach of the legislation. Moreover, in the event of processing personal data that is collected indirectly (ie, from a source other than the data subject), the person to whom the personal data relates is entitled to object to data processing.

Rights of the data subject in the above scope are regulated in article 32 of the PDPA. According to that provision, the data subject has a right to control the processing of his or her personal data contained in filing systems, and in particular he or she has the right to:

(i) demand the data be completed, updated, rectified, temporarily or permanently suspended or erased, in case they are not complete, outdated, untrue or collected with the violation of the PDPA, or in case they are no longer required for the purpose for which they have been collected; and

(ii) make a justified demand in writing, in cases referred to in article 23 clause 1 point 4 and 5 of the PDPA (ie, processing necessary for the performance of tasks provided for by law and carried out in the public interest or processing necessary for the purpose of the legitimate interests pursued by the controllers or data recipients), for the blocking of the processing of his or her data, due to his or her particular situation.

It should be underlined that, under the PDPA, in the case that the data subject objects to the processing of his or her data, as referred to in (ii), the data controller is obliged to immediately stop the processing of the questioned data or without undue delay transmit the demand to the Inspector General, who shall make an appropriate decision.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Yes, article 26 of the PDPA imposes standards on the quality, currency and accuracy of PII. A data controller is under an obligation to ensure that the personal data it is collecting, purchasing or otherwise retaining is relevant, adequate and not excessive for the purposes for which it will be used. For example, if the sole reason for obtaining the personal data of an individual data subject is to contact them about a job application they have made, the company will only need very limited details about them and may not be able to justify at that stage collecting details of their health and fitness. Moreover, personal data should not be collected and used or stored on an individual, unless it has a purpose for which the data subject has, where necessary, been fairly notified and that can be justified.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes, as determined in question 15, the owner of PII is obliged to collect only data that is relevant and adequate for the purposes of processing. Regarding the length of time data may be held, there are no particular provisions regulating that matter. Article 26, section 1, subsection 4 of the PDPA stipulates only that the data controller should ensure that the data are kept no longer than is necessary for the purpose for which it is processed.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

On the basis of article 26 of PDPA, the owners of PII performing the processing of data should protect the interests of data subjects with due care, and in particular ensure that the data are collected for specified and legitimate purposes and not further processed in a way that is incompatible with the intended purposes.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The processing of personal data for a purpose other than that intended at the time of data collection is allowed, provided that it does not violate the rights and freedoms of the data subject and is done:

- for the purposes of scientific, didactic, historical or statistical research;
- subject to the provisions of article 23 and article 25 of the PDPA (ie, on the basis of the one of the legal grounds described in question 10 and subject to notification of the data subject, as described in question 12).

Security

19 Security obligations

What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The Regulation imposes a technical and safety obligation while processing personal data, on both the controller and the processor. The requirements include:

- the requirement to assess the required security level out of the three available (basic, medium, high);
- the requirement to produce a security policy and a computer system management instruction used for personal data processing;
- the requirement that, in cases where a password is used for user authentication in the computer system used for data processing, the password shall consist of at least eight characters, including small and capital letters, numbers and special characters; and
- the requirement to apply cryptographic protection measures for the data used for authentication that are being transferred on the internet.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The PDPA does not provide a general obligation of notification of security breach. Only entities providing telecommunication services are required to notify the DPA of any data security breach within three days, in compliance with the provision of the TL. Under the TL, additional obligations in case of any threat to the integrity of the telecommunications network may apply.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

No. The appointment of a data protection officer (DPO) is voluntary. If the DPO is appointed, the owner of PII must notify the DPA. The responsibilities of the DPO include:

- ensuring compliance with the provisions on the protection of personal data, in particular by:
  - checking compliance of personal data processing with the provisions on the protection of personal data and drawing up a report in this regard for the controller;
  - supervising development and update of the documentation referred to in article 36 paragraph 2 as well as supervising compliance with the principles specified in this documentation; and
  - ensuring that the persons authorised to process personal data become acquainted with the provisions on the protection of personal data; and
- keeping a register of data files processed by the controller.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Yes. If the owner of PII has appointed the DPO and notified the DPA, then he or she is obliged to keep a register of data files (with some exceptions, eg, files containing sensitive data). As mentioned in question 21, the DPO is responsible for keeping this register.

The owner of PII is required to establish the data security policy and the instruction of the management of the computer system processing personal data.

Registration and notification

23 Registration

Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?

The owner of PII is required to register the data filing systems with the DPA, unless he or she has appointed a DPO (if a DPO has been appointed, only the filing systems containing sensitive data have to be registered with the DPA).

The obligation to register data filing systems does not apply to the owners of data that:

- contain classified information;
- were collected as a result of inquiry procedures held by officers of the bodies authorised to conduct such inquiries;
- are processed by relevant bodies for the purpose of court proceedings and on the basis of the provisions on National Criminal Register;
- are processed by the Inspector General of Financial Information;
- are processed by relevant bodies for the purposes of the participation of the Republic of Poland in the Schengen Information System and the Visa Information System;
- are processed by competent authorities on the basis of the provisions on exchange of information with prosecuting bodies of member states of the European Union;
- relate to the members of churches or other religious unions with an established legal status, being processed for the purposes of these churches or religious unions;
- are processed in connection with employment by the controller or providing services for the controller on the grounds of civil law contracts, and also refer to the controller's members and trainees;
- refer to the persons availing themselves of their healthcare services, notarial or legal advice, patent agent, tax consultant or auditor services;
- are created on the basis of electoral regulations concerning the Diet, Senate, European Parliament, communal councils, poviat (county) councils and voivodship regional assemblies, the President of the Republic of Poland, head of the commune, major or president of a city elections, and the acts on referendum and municipal referendum;
- refer to persons deprived of freedom under the relevant law within the scope required for carrying out the provisional detention or deprivation of freedom;
- are processed for the purpose of issuing an invoice, a bill or for accounting purposes;
- are publicly available;
- are processed to prepare a thesis required to graduate from a university or be granted a degree;
- are processed with regard to minor current everyday affairs; and
- are processed in data files that are not kept with the use of IT systems, except for the files containing sensitive data.

The processors of PII are not obliged to register the data filing systems with the DPA.

24 Formalities

What are the formalities for registration?

The motion concerning the data filing system submitted to the registration should contain the following:

- an application for entering the personal data filing system into the register of filing systems;
- specification of the controller and the address of its seat or place of residence, including an identification number from the National Official Business Register if such a number was granted, as well as the legal basis for maintaining the filing system and, in the case of entrusting data processing to the processor, or appointing a representative of the person having its registered seat in the third country, the specification of such entity and the address of its seat or place of residence;
- the purpose of processing the data;
- the description of the categories of data subjects and the scope of the processed data;
- 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;
- the description of technical and organisational security measures;
- information on the ways and means of fulfilling technical and organisational conditions specified in the Regulation; and
- information relating to a possible data transfer to a third country.

There is no fee required for registration. The Regulation provides the form of registration motion to be fulfilled by the owner of PII. The motion can also be submitted online.

25 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

A person who, regardless of the obligation, fails to notify the data filing system for registration, is liable to a fine, the restriction of liberty or imprisonment for up to one year.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The DPA may refuse to register the data filing system if:

- the requirements specified in question 24 have not been fulfilled;
- the processing of data would breach the principles referred to in articles 23–28 (these provisions refer to the legal grounds of data processing, information obligation, adequacy and purpose limitation principle and the processing of sensitive data); and
- the devices and computer systems used for the processing of the data filing system submitted for registration do not meet the basic technical and organisational conditions defined in the Regulation.

27 Public access

Is the register publicly available? How can it be accessed?

Yes. It can be accessed in the DPA's office in Warsaw and online (https://egiodo.giodo.gov.pl/personal_data_register.dhtml).

28 Effect of registration

Does an entry on the register have any specific legal effect?

No, except for sensitive data. Such data can be processed once the DPA has issued a decision on the registration of the file.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the PDPA, personal data may be transferred either to another, independent, data controller (disclosure of personal data) or to a data processor (entrusting the personal data for processing).

In case of the data processor, the transfer of the PII as such is not regulated. However, the PDPA provides for specific requirements in the scope of the agreement that the data controller needs to conclude with the data processor.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

When PII is disclosed to a service provider (data processor), then this is referred to as 'entrusting the data for processing'. In order for such disclosure (and further operations of the processor) to be legitimate, specific requirements stipulated in the PDPA need to be complied with. Otherwise, the processor may be considered to constitute an independent data controller, and, consequently, be found not to act in compliance with the PDPA (eg, by not fulfilling all of the data controller's obligations under the act).

An agreement on entrusted data processing must be executed in writing and state the scope and purpose of data processing. It may form part of a larger agreement (eg, laying down general conditions of cooperation).

The data processor is responsible for ensuring appropriate security measures for data processing, which are laid down in articles 36–39 of the PDPA, as well as adhering to security requirements specified in the Regulation. In the context of complying with security requirements mentioned above, the data processor bears liability as does the data controller (the processor's regulatory obligations). Apart from that, the processor is liable for acting in compliance with the agreement on entrusted data processing (the processor's contractual obligations). The data processor is only authorised to process the entrusted personal data in the scope and for the purposes set out in the agreement and may not use the data for its own purposes.

Since it is the data controller who maintains ultimate responsibility for data protection compliance, it is in his or her interest to appoint a reliable data processor. There is no obligation to carry out a service provider due diligence in the PDPA, nor is it required by the DPA. However, such approach is advisable before an agreement on entrusted data processing is concluded.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Under the PDPA, the transfer of personal data to third countries, (ie, outside of the EEA) is restricted. In general, such transfers are only permissible on the condition that the country of destination ensures an adequate level of personal data protection in its territory.

It should be added that, according to the PDPA, the adequacy of the level of personal data protection (referred to above) is evaluated taking into account all the circumstances concerning a data transfer operation, in particular the nature of the data, the purpose and duration of the proposed data processing operations, the country of origin and the country of final destination of the data as well as the legal provisions being in force in a given third country and the security measures and professional rules applied in this country.

However, there are certain circumstances in which a data transfer may be performed notwithstanding the above restrictions. Namely, those circumstances are:

- where the transfer of personal data results from an obligation imposed on the data controller by legal provisions or by the provisions of any ratified international agreement that guarantee adequate level of data protection;
- where the data subject has given his or her written consent;
- where the transfer is necessary for the performance of a contract between the data subject and the controller or takes place in response to the data subject's request;
- where the transfer is necessary for the performance of a contract concluded in the interests of the data subject between the controller and another subject;
- where the transfer is necessary or required by reasons of public interest or for the establishment of legal claims;
- where the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer relates to data that are publicly available.

32 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

In the event that none of the above situations applies, personal data may be transferred to a third country on the basis of a data transfer agreement (DTA) concluded between the data exporter and data importer. If the DTA is based on EU standard contractual clauses, it does not need to be approved by the DPA. The transfer may also be based, for example, on binding corporate rules, however, they still need the DPA's approval.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

In general, 'onward transfers' are only permissible on the condition that the further data recipient (importer) is also bound by principles that guarantee an adequate level of data protection. It is the data exporter's responsibility to ensure this.

Rights of individuals

34 Access

Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Every individual has control over the processing of his or her personal data contained in filing systems, and in particular this covers the right, among others, to:

- obtain extensive information on whether such a filing system exists and to establish the controller's identity, the address of its seat and its full name, and, in case the controller is a natural person, to obtain his or her address and his or her full name;
- obtain information as to the purpose, scope, and the means of processing of the data contained in the system;
- find out when his or her personal data began to be processed and details of the content of the data; and
- obtain information as to the source of his or her personal data, unless the controller is obliged to keep it confidential as a state, trade or professional secrecy, etc.

There is, however, a limit to the right of access: the data subject may exercise this to obtain information once every six months.

35 Other rights

Do individuals have other substantive rights?

Individuals whose data are being processed, are entitled not only to obtain information but also to:

(i) demand the data to be completed, updated, rectified, temporarily or permanently suspended or erased, in case they are not complete, outdated, untrue or collected with violation of the PDPA, or in case they are no longer required for the purpose for which they have been collected;

(ii) make a justified demand in writing, for the blocking of the processing of his or her data, due to his or her particular situation – in cases where the processing of the data is necessary for the performance of tasks provided for by law and carried out in the public interest or the processing of the data is necessary for the purpose of the legitimate

interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject;

(iii) object to the processing of his or her personal data, should the controller intend to process the data for marketing purposes or object to the transfer of the data to another controller – in cases where the processing of the data is necessary for the performance of tasks provided for by law and carried out in the public interest or the processing of the data is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject; and

(iv) make a demand to a controller for reconsidering the data subject's individual case settled in contravention of article 26a paragraph 1 PDPA (according to which it is inadmissible for a final decision in an individual case of the data subject is to be issued solely based on automated processing of personal data in a computer system).

However, in cases referred to in points (ii) and (iv), if the data controller does not agree with the data subject's demand, he or she may refer the demand and the reasoning behind it to the DPA, who shall issue an appropriate decision.

Also, in the case referred to in point (iii), the data controller is allowed to leave the forename or forenames and the surname of the data subject in his or her filing system, along with his or her PESEL identification number or address – solely in order to avoid the data being used once more for the purposes to which the data subject objected.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals may file a civil law suit if they suffer damages due to a breach of personal data protection legislation. The data subject may claim that his or her 'personal interests' (as defined in the Polish Civil Code) have been injured or, if applicable, may also prove that he or she suffered a substantial loss. However, the payment of damages does not follow automatically – the affected individual needs to go through standard civil court procedure.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The above rights are exercisable either personally towards the data controller or through the judicial system (if the data subject suffered damages). In cases where the data subject feels that the data controller is acting in contravention of the personal data protection legislation, he or she may file a complaint to the DPA; however, this does not automatically lead to the payment of any damages. Nevertheless, on the basis of such a complaint, the DPA may issue an administrative decision that will force the data controller to act in accordance with the DPA's orders included in the decision.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No.

Supervision

39 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

When a decision of the supervisory authority is issued data owners may, in the first instance, file a motion to the supervisory authority to reinvestigate the case. If the authority's decision is to keep the previous decision binding, then a data owner can appeal to the Voivodeship Administrative Court. A data owner can file an appeal from a verdict of the Voivodeship Administrative Court to the High Administrative Court.

Specific data processing

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

A regime of storing information (cookies), in the terminal equipment of subscribers (end users) is provided by the TL.

The TL introduces the opt-in regime based on consent that can be expressed also by the use of software settings of specific equipment. The wording of article 173 (1) TL is as follows:

> *The storing of information or the gaining of access to information already stored in the telecommunications terminal equipment of a subscriber or a user is only allowed on condition that:*
> 1) *the subscriber or the end user is directly informed in advance in an unambiguous, simple and understandable manner with regard to:*
> a) *the purpose of storing and the manner of gaining access to this information,*
> b) *the possibility to define the conditions of the storing or the gaining of access to this information by using settings of the software installed on his telecommunications terminal equipment or a service configuration;*
> 2) *the subscriber or end user, having obtained information referred to in point 1), gives its consent;*
> 3) *the stored information or the gaining of access to this information do not cause changes in the configuration of the subscriber's or end user's telecommunications terminal equipment and in the software installed on this equipment.*

Article 173(2) TL states that 'the subscriber or end-user may give his consent (...) using the settings of the software installed on his telecommunications terminal equipment or a service configuration.' Thus, the TL Act provides for two models of expressing consent by subscribers (end users). The first classic model would be understood as explicit consent (not implied by any declarations of will of a different content). The second model, which derives from point 66 of the preamble to Directive 2009/136EC, is a non-standard model where consent is expressed by using software settings or a service configuration.

41 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Currently a distinction must be made between electronic communications marketing and telecommunication marketing.

According to article 172 of the TL, the use of telecommunications terminal equipment and automated calling systems for the purposes of direct marketing shall not be allowed, unless the end user or subscriber has given his or her prior consent.

The amended article 172 of the TL has its origins in article 13 of the Directive 2002/58/EC. This applies mostly to natural persons and article 13 protects them against unsolicited communications. However, according to article 13, clause 5 of the above Directive: 'Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected'.

Subscribers and end-users, as defined in the TL, may be either natural or legal persons. Thus, article 172 of the TL protects both legal and natural persons who use communication devices, from unsolicited communications. In conclusion, under the TL, communication for direct marketing purposes is only allowed after receiving the end user's prior consent, whether it is a legal or natural person.

According to articles 209 and 210, whoever fails to obtain the end user's consent for direct marketing communications, as stipulated in article 172 of the TL, shall face a monetary fine that may reach up to 3 per cent of that entity's turnover from the last calendar year. Additionally, a fine of up to 300 per cent of the monthly salary may be imposed on the entity's officers in charge, in particular – members of the management board.

According to the ESSA, sending unsolicited commercial information specifically addressed to a natural person by electronic communications means, in particular via electronic mail, is prohibited. Commercial information shall be considered solicited, if the recipient has expressed his or her consent to receive such information. In particular, if he or she has made

available for the purpose of such receipt an electronic address that identifies him or her. The ESSA punishment for sending unsolicited mails is 5,000 zlotys. Additionally, the above-mentioned activity shall be regarded as unfair competition practice within the meaning of provisions of the Act of 16 April 1993 on Fighting Unfair Competition.

42 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Currently in Poland there are no statutory regulations specifically with regard to cloud computing. It should be mentioned, however, that outsourcing personal data to the cloud constitutes entrusting data for processing within the meaning of the PDPA, therefore the provisions of article 31 of that act and underlying regulations (eg, as regards security measures) apply. Moreover, processing personal data in the cloud may require the transfer of data to non-EEA countries, which is also subject to special rules under the PDPA.

A piece of non-binding (although generally applied) regulation that touches upon the subject of cloud computing was issued in the scope of the banking sector – namely: Recommendation D (2013) of the Polish Financial Supervision Authority. The Recommendation lists general security measures that should be applied with regard to the use of cloud computing services by banks.

There are also obligations applicable to cloud computing stipulated in the Polish Telecommunications Law. Those regulations pertain to the obligation of securing data that is subject to telecommunications secrecy ('confidentiality of telecommunications' as referred to in the Telecommunications Law) and data retention requirements.

WIERZBOWSKI EVERSHEDS

Arwid Mednis **arwid.mednis@eversheds.pl**
Gerard Karp **gerard.karp@eversheds.pl**

Centrum Jasna
Ul. Jasna 14/16A
00-041 Warsaw
Poland

Tel: +48 22 50 50 700
Fax: +48 22 50 50 701
www.eversheds.pl

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law