Journal of Laws 2019, item 125

ACT

of 14 December 2018

on the protection of personal data processed in connection with preventing and combating crime

Prepared based on: consolidated text, Journal of Laws 2023, item 1206.

Chapter 1[(1)]

General provisions

Article 1. The Act lays down:

1) the rules and conditions for the protection of personal data processed by the competent authorities for the purposes of the identification, prevention, detection and combating of criminal offences, including threats to security and public order, as well as executing pre-trial detention, penalties, fines and coercive measures resulting in the deprivation of liberty;

2) the rights of data subjects whose personal data are processed by the competent authorities for the purposes referred to in subparagraph 1 and the legal remedies available to those persons;

3) the way of exercising supervision over the protection of personal data processed by the competent authorities for the purposes referred to in subparagraph 1, with the exception of personal data processed by public prosecutor's office and courts;

4) the tasks of the supervisory authority and the form and procedure of their implementation;

5) the obligations of the controller and processor as well as the data protection officer and the procedure for their appointment;

6) the method of safeguarding personal data;

7) the mode of cooperation with supervisory authorities in other Member States of the European Union;

8) criminal liability for the violation of the provisions of this Act.

Article 2. The Act shall apply to the processing of personal data by the competent authorities

(1) This Act implements, within the scope of its regulation, Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 04.05.2016, p. 89).

for the purposes referred to in Article 1(1) in a manner:

1) fully or partly automated;

2) other than automated, where the data form or are intended to form a part of a filing system.

Article 3. The provisions of the Act shall not apply to the protection of personal data:

1) contained in case or activity files or record-keeping devices, including those created and processed with the use of IT techniques, maintained pursuant to the Act of 6 June 1997 - Executive Penal Code (Journal of Laws of 2023, item 127 and of 2022, item 2600), the Act of 6 June 1997 - Code of Criminal Procedure (Journal of Laws of 2022, items 1375, 1855, 2582 and 2600 and of 2023, items 289 and 535), the Act of 10 September 1999 - Penal Fiscal Code (Journal of Laws of 2023, item 654), the Act of 24 August 2001 – Petty Offences Procedure Code (Journal of Laws of 2022, item 1124), the Act of 22 November 2013 on the Treatment of Persons with Mental Disorders who Pose a Threat to the Life, Health or Sexual Freedom of Others (Journal of Laws of 2022, item 1689), the Act of 28 January 2016 – Law on the Public Prosecutor's Office (Journal of Laws of 2022, items 1247, 1259 and 2582 and of 2023, item 240), the Act of 9 June 2022 on the Support and Rehabilitation of Minors (Journal of Laws, item 1700 and of 2023, item 289);

2) processed in connection with ensuring national security, including in the execution of the statutory tasks of the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service and the Central Anti-Corruption Bureau.

Article 4. Whenever this Act refers to:

1) controller - it shall mean the competent authority which alone or jointly with other competent authority or authorities determines the purposes and means of personal data processing, the entity designated by the Act as the controller, if the purposes and means of personal data processing are determined by the Act, or the entity indicated by the law of the European Union or by the law of a Member State of the European Union, or the entity designated in accordance with the criteria laid down in the law of that state;

2) biometric data - it shall mean personal data concerning the physical, physiological or behavioural characteristics of a natural person and allowing or confirming the unique identification of that natural person, including facial image or dactyloscopic data obtained through specific technical processing;

3) data concerning health - it shall mean personal data related to the physical or mental health

of a natural person, including data on the provision of health care services, which reveal information about his or her health status;

4) genetic data - it shall mean personal data concerning the inherited or acquired genetic characteristics of a natural person which reveal unique information about that person's physiology or health and which are obtained in particular from the analysis of a biological sample originating from that person;

5) personal data - it shall mean personal data referred to in Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 04.05.2016, p. 1, as amended[2)] [2)]);

6) personal data breach - it shall mean a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or unauthorised access to personal data transmitted, stored or otherwise processed;

7) recipient - it shall mean a natural or legal person, public authority, agency or other body, to which the personal data are disclosed, with the exception of public authorities which may receive personal data in the framework of a particular inquiry in accordance with European Union law or the law of a Member State of the European Union, the processing of which shall be in compliance with the applicable data protection rules according to the purposes of the processing;

8) restriction of processing - it shall mean the marking of stored personal data with the aim of limiting their processing in the future;

9) supervisory authority in other European Union Member States - it shall mean an independent public authority established by a European Union Member State other than the Republic of Poland, appointed to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the European Union;

10) international organisation - it shall mean an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

[2)] The amendments to the aforementioned regulation were announced in OJ L 227 of 23.05.2018, p. 2.

11) third country - it shall mean a country which is not a Member State of the European Union and which does not apply the provisions of the Schengen acquis;

12) processor - it shall mean a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

13) profiling - it shall mean any form of automated processing of personal data consisting of their use to evaluate certain features of a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

14) processing - it shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

15) pseudonymisation - it shall mean the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

16) competent authority - it shall mean any public authority, any other body or entity entrusted to process personal data under separate regulations;

17) filing system - it shall mean any structured set of personal data which are accessible according to specified criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Chapter 2

Tasks of the supervisory authority

Article 5. 1. The tasks of the President of the Personal Data Protection Office, hereinafter referred to as the “President of the Office”, include:

1) monitoring and enforcing the application of the provisions of this Act and the implementing acts issued pursuant to it;

2) promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data for the purpose referred to in Article 1(1);

3) advising public institutions on measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data for the purpose referred to in Article 1(1);

4) promoting the awareness in the scope of application of this Act and the implementing acts issued on its basis among controllers and processors;

5) upon request, providing information to any data subject concerning the exercise of their rights under this Act and, if appropriate, cooperation with the supervisory authorities in other Member States of the European Union to this end;

6) handling and investigating complaints lodged by data subjects whose personal data are processed unlawfully;

7) unless specifically provided otherwise, inspecting the compliance of the processing of personal data with the provisions of this Act;

8) conducting proceedings on the application of this Act, including on the basis of information received from another public authority;

9) exercising the consultative functions referred to in Article 38 concerning the processing operations under this Act;

10) cooperation with supervisory authorities in other Member States of the European Union;

11) issuing opinions to the Sejm, the Senate and other public authorities on matters of personal data protection;

12) issuing opinions on draft acts and regulations on matters concerning the protection of personal data processed for the purposes referred to in Article 1(1).

2. Where request for the performance of a task is manifestly unfounded or excessive, in particular because of its repetitive character, the President of the Office may charge a fee in the amount corresponding to the expected costs incurred for the performance of the task, or may refuse to act on the request. The President of the Office is obliged to demonstrate that the request is manifestly unfounded or excessive. The President of the Office takes action after the fee has been collected. The fee collected by the President of the Office constitutes revenue for the state budget.

3. Draft acts and regulations concerning personal data processed for the purposes referred to in Article 1(1) shall be submitted to the President of the Office for issuance of an opinion.

Article 6. In order to perform the tasks referred to in Article 5(1)(1) and (6) to (8), the

President of the Office may carry out inspection of personal data processing, hereinafter referred to as the "inspection". The provisions of the Chapter 9 of the Act of 10 May 2018 on the Protection of Personal Data shall apply to the performance of the inspection (Journal of Laws of 2019, item 1781), excluding Article 79(1)(2), Article 83, Article 84(4) and Article 85 of that Act.

Article 7. In the course of the inspection, an employee of the Personal Data Protection Office authorised by the President of the Office, hereinafter referred to as the "inspector", shall have to the right to inspect the data filing system subject to the inspection and other documents directly related to the subject of the inspection. The inspector shall have the right to inspect the data filing system and other documents referred to in the first sentence only in the presence of an authorised representative of the competent authority where the inspection is conducted.

Article 8. 1. In case of a reasonable suspicion that the planned processing operations may result in a breach of the provisions of this Act, the President of the Office shall issue a warning to the controller or the processor.

2. In the event of a breach of the provisions on the protection of personal data collected for the purposes referred to in Article 1(1), the President of the Office shall, by means of an administrative decision, order the controller or the processor to restore the status of compliance with the law, in particular:

1) to remedy any deficiencies;

2) to complete, update, rectify, make available or withhold personal data;

3) to apply additional security measures for collected personal data;

4) to secure personal data or transfer them to other entities;

5) to erase personal data;

6) to impose temporary or permanent restrictions on data processing and transfer, including a ban on processing.

3. The decisions of the President of the Office, referred to in subparagraph 2, may not order to delete personal data collected in the course of operational and exploratory activities carried out under the applicable legal provisions. If the controller recognises that the data so collected is redundant, it is obliged to erase such data. If the controller fails to comply with the obligation to erase personal data, the President of the Office may order the erasure of the data. In order to exercise the right, the President of the Office shall not be granted access to the personal data referred to in the first sentence. The controller or the processor of the personal data referred

to in the first sentence shall be obliged to immediately restore their lawful processing.

Article 9. 1. The proceedings referred to in Article 8(2) shall take place in one instance.

2. The decision of the President of the Office referred to in Article 8(2) may be appealed to an administrative court.

Article 10. 1. In order to perform the tasks referred to in Article 5(1)(5) and (9), the President of the Office may address requests to the controller or the processor with the aim to ensure effective protection of personal data collected for the purposes referred to in Article 1(1).

2. The controller or the processor to which a request referred to in subparagraph 1 has been addressed shall be obliged to respond to that request in writing in paper or electronic form within 30 days of its receipt.

Article 11. 1. The President of the Office may directly request the data protection officer referred to in Article 46 to carry out a check on the application of the provisions of this Act by the controller who has appointed him/her, indicating the scope and time of the check.

2. Following the check referred to in subparagraph 1, the data protection officer, through the controller, shall submit to the President of the Office a report on the check performed.

3. The performance by the data protection officer of a check in the case referred to in subparagraph 1 shall not prejudice the right of the President of the Office to carry out the check referred to in Article 7.

Article 12. The proceedings in matters subject to the regulations of this chapter shall be carried out pursuant to the provisions of the Act of 14 June 1960– Code of Administrative Procedure (Journal of Laws of 2023, item 775), hereinafter referred to as the "Code of Administrative Procedure", unless otherwise provided for in this Act.

Chapter 3

Principles relating to processing of personal data

Article 13. 1. Competent authorities shall process personal data only to the extent necessary to fulfil a legal entitlement or obligation.

2. It shall be permitted to process personal data originally collected for one of the purposes referred to in Article 1(1) for other new purposes referred to in Article 1(1) provided that:

1) the controller is allowed to process such personal data for another new purpose under separate legislation;

2) the processing is necessary and proportionate for such another new purpose under separate legislation.

3. The processing of personal data for purposes other than those referred to in Article 1(1) shall be allowed if the processing is permitted by law.

4. The processing of personal data collected for the purposes referred to in Article 1(1) shall be permitted to the extent necessary for archiving in the public interest and for scientific, statistical or historical purposes insofar as it is subject to appropriate safeguards for the rights and freedoms of the data subjects.

Article 14. 1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, hereinafter referred to as "sensitive data", is not permitted.

2. The processing of sensitive data shall be permitted if:

1) the relevant legal regulations authorise their processing; or

2) it is necessary for the protection of the life or health or interests of the data subject or of another natural person; or

3) such data have been made public by the data subject.

Article 15. 1. The final determination of an individual case of a data subject with adverse legal effects for him or her, or significantly affecting him or her, solely as a result of the processing of personal data by automated means, including profiling, is not permitted, unless it is permitted by any legal regulation to which the controller is subject and which provides for adequate safeguards for the rights and freedoms of the data subject, or at least the right to obtain intervention on the part of the controller.

2. The decisions referred to in subparagraph 1 shall not be based on sensitive data, unless suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.

3. It is prohibited to profile natural persons on the basis of sensitive data, resulting in discrimination against them.

Article 16. 1. The controller shall verify personal data within the time limits laid down by the specific legislation governing the activities of the competent authority and, if no time limit is

laid down by such legislation, at least every 10 years from the date the data were collected, obtained, retrieved or updated.

2. The verification is carried out to determine whether any data exist whose continued storage is unnecessary. The redundant data shall be erased, subject to Article 17.

Article 17. Personal data deemed unnecessary may be transformed in such a way that individual personal or material information cannot be attributed to an identified or identifiable natural person, or in such a way that such attribution would require disproportionate cost, time or effort.

Article 18. Where personal data is processed in connection with the documentation of activities carried out by the competent authorities, as an electronic copy of control files, the data shall be retained after it is anonymised.

Article 19. When processing personal data, the controller shall ensure that a distinction is made, where applicable and as far as possible, between personal data concerning:

1) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

2) persons convicted of a criminal offence;

3) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that they could be victims of a criminal offence;

4) other parties to a criminal offence, such as persons who might be called on to testify in connection with the criminal offence or at a later stage of the proceedings, persons who can provide information on criminal offences, or persons who have contacts or associates of one of the persons referred to in subparagraphs 1 and 2.

Article 20. When processing personal data, the controller shall ensure that a distinction is made, where applicable and as far as possible, between personal data derived from facts and personal data derived from individual assessments.

Article 21. 1. The competent authority may transfer or make available personal data to other competent authorities, a third country or an international organisation after verifying, where necessary and possible, the accuracy and completeness of the data and whether they are up to date.

2. When communicating personal data to a recipient referred to in paragraph 1, the competent authority shall, where necessary and feasible, communicate to that recipient the necessary additional information to allow the recipient to evaluate the degree of accuracy and

completeness of the personal data transmitted and whether they are up to date.

3. A competent authority that has transmitted to a recipient referred to in paragraph 1 inaccurate, incomplete or no longer up to date personal data or has transmitted such data in violation of the provisions of this Act shall, without undue delay, inform the recipient thereof and:

1) rectify, complete or update the data and send the relevant data to that recipient, unless this is manifestly unreasonable due to the lapse of time, or

2) erase or restrict the processing of the data, and inform that recipient in order to allow that recipient to erase or restrict the processing of such data.

4. The limitation of the data processing referred to in subparagraph 3(2) shall take place whenever:

1) the data subject contests the accuracy of the personal data and their accuracy or inaccuracy cannot be ascertained; or

2) personal data must be retained for evidence purposes.

5. The provisions of paragraphs 1 to 3 shall not apply where the transmission or making available of personal data to the recipient referred to in subparagraph 1 could constitute a threat to the rights and freedoms of a human being and a citizen and in the cases referred to in Article 25(1).

6. Where specific conditions of processing are permitted by law, the competent transmitting authority is obliged to inform the recipient of such personal data of such conditions and of the obligation to comply with them.

Chapter 4

Rights of the data subject

Article 22. 1. The controller provides information on:

1) the name, registered office and contact details of the controller;

2) where applicable, the contact details of the data protection officer;

3) the purpose for which the personal data are intended;

4) the right to lodge a complaint with the President of the Office or any other supervisory authority under separate legislation if a person's rights have been infringed as a result of the processing of their personal data, as well as the contact details of the President of the Office or any other supervisory authority;

5) the right to request from the controller access to and rectification or erasure of personal data, or the restriction of the processing of personal data concerning that person.

2. The information referred to in subparagraph 1 shall be made available on the website, in the Public Information Bulletin on the homepage of the competent authority or office or at its registered office.

3. In specific cases, the data subject shall be provided by the controller with at least the following information in order to enable him/her to exercise his/her rights:

1) the legal basis for data processing;

2) the period for which the personal data will be stored or, where this is not possible, the criteria used to determine that period;

3) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations.

4. The data subject shall have the right, upon request, to be informed by the controller whether his or her data are processed and, in the case of processing, the right to be informed of:

1) the purpose and legal basis of data processing;

2) categories of personal data and the data processed;

3) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;

4) the period of retention of personal data or when this is not possible,

the criteria for determining this period;

5) the possibility to request from the controller the rectification or erasure of personal data or the restriction of the processing of personal data concerning that person;

6) the right to lodge a complaint with the President of the Office or any other supervisory authority under separate legislation if a person's rights have been infringed as a result of the processing of their personal data, as well as the contact details of the President of the Office or any other supervisory authority;

7) source of data origin.

Article 23. 1. The data subject shall, upon request, have the right of access to his/her personal data.

2. When granting a request for access to personal data, the controller shall make available or provide the applicant with a copy of the data or an extract of the data in an accessible format.

3. The controller shall inform the data subject of the reasons for the refusal or restriction of access and of the possibility of lodging a complaint with the President of the Office if the person's rights are infringed as a result of the processing of his/her personal data.

4. The controller shall document the factual or legal reasons for refusing or limiting access to the data. Such information shall be made available to the President of the Office upon request.

Article 24. 1. The data subject may request that the controller should immediately:

1) complete, update or rectify personal data in cases where such data are incomplete, no longer up to date or inaccurate;

2) erase personal data - where the data have been collected or are processed in violation of the provisions of this Act.

2. When granting the request referred to in subparagraph 1, the controller shall, without undue delay, complete, update, rectify or erase personal data, as appropriate.

3. If the request for rectification or updating refers to data that are also contained in a document containing a testimony, statement or declaration by a natural person and it is established that the data are inaccurate or no longer up to date, the controller shall leave the data unchanged. The request shall be granted only by making a note to that effect in the data file.

4. If the circumstance referred to in subparagraph 1(2) is determined *ex officio*, the controller shall erase the personal data.

5. The controller shall inform the applicant of the rectification or erasure of the data or of the refusal to rectify or erase the data.

6. In the event of a refusal to rectify or erase personal data, the controller shall instruct the data subject to lodge a complaint if his or her personal data are unlawfully processed.

Article 25. 1. Whenever:

1) the data subject contests the accuracy of the personal data and their accuracy or inaccuracy cannot be ascertained,

2) personal data subject to erasure must be retained for evidence purposes,

-the controller shall be obliged, without undue delay, to temporarily restrict the processing of the contested data by refraining from making them available to the recipients.

2. The controller is obliged to inform the competent authority from which the inaccurate personal data originated without undue delay of the rectification of such data.

3. The controller shall inform the recipients without undue delay of the rectification or erasure of personal data or the restriction of data processing. The recipients are obliged to update, rectify or erase personal data, or restrict data processing.

4. Before lifting a restriction on the processing of contested personal data, the controller shall inform the data subject.

5. The controller shall inform the data subject of the restriction of the processing of personal data, as well as of the possibility of lodging a complaint if their personal data are processed unlawfully.

Article 26. 1. The information referred to in the provisions of this Chapter shall not be communicated and personal data shall not be made available where this could give rise to:

1) disclosure of information obtained as a result of operational and exploratory activities;

2) obstructing or preventing the identification, prevention, detection or combating of criminal offences;

3) obstructing the conduct of criminal proceedings, criminal enforcement proceedings, criminal fiscal proceedings or proceedings in cases of petty offences or tax offences, or in cases referred to in Article 359(1) of the Act of 9 June 2022 on the Support and Rehabilitation of Minors;

4) threat to human life, health or public safety and order;

5) threat to national security, including defence or security and the economic bases of the functioning of the state;

6) substantial infringement of the personal rights of others.

2. The controller may communicate the information referred to in subparagraph 1 to the data subject where its disclosure would be necessary for the protection of human life or health.

Article 27. With regard to personal data collected in proceedings conducted on the basis of the legislation referred to in Article 3(1), the rights of data subjects shall be exercised only on the basis of, and to the extent provided for by, the regulations governing those proceedings.

Article 28. When submitting application request under Article 22(4), Article 23(1) or Article 24(1), the applicant shall provide at least his or her full name and postal address. If the controller

has reasonable doubt as to the identity of the person who submitted the request, it may request additional information necessary to confirm the identity of that person.

Article 29. The controller shall, in the case referred to in Article 26(1), instruct the data subject to lodge a complaint with the President of the Office in the manner laid down in Article 30(2).

Article 30. 1. The controller shall take steps to facilitate the exercise of the data subject's rights referred to in Article 15 and Articles 22 to 25.

2. The controller shall provide the information referred to in Articles 15, 22 to 25 and 45 to the data subject in clear and plain language, in the same form in which the request was submitted, unless providing the information in that form could give rise to undue difficulty or expenses or unless otherwise provided by this Act.

3. The controller shall, without undue delay, inform in writing in paper or electronic form or by means of electronic communication means within the meaning of Article 2(5) of the Act of 18 July 2002 on the Provision of Services by Electronic Means (Journal of Laws of 2020, item 344) of the data subject about the action taken on his/her request or, if possible, provide the requested information.

4. The communication provided by the controller with the data subject pursuant to Articles 15, 22-25 and 45 shall be free of charge. If the data subject's requests are unfounded or excessive, in particular because of their repetitive nature, the controller may:

1) charge a fee to cover the administrative costs of providing the information, or communication or taking the action requested, or

2) refuse to act on the request.

5. The fee referred to in subparagraph 4(1) shall be paid before the controller provides the information, makes the communication or takes the action requested. The fee charged by the controller operating within a state budget unit or a local government budget unit constitutes revenue for the state budget or a local government unit, respectively.

6. The controller shall, without undue delay but no later than 14 days from the date of submission of the request referred to in Article 22(4), Article 23(1) or Article 24(1), notify the applicant of the amount of the fee referred to in paragraph 4(1). Information shall be provided in accordance with the request within 14 days of the payment of the fee, unless the applicant changes the request within this period as to the scope of the data requested, the manner or form in which

the data is to be made available or withdraws the request.

7. The controller is obliged to demonstrate that the data subject's request is manifestly unfounded or excessive.

Chapter 5

The controller and the processor

Section 1

General provisions

Article 31. 1. The controller shall ensure that personal data are:

1) processed lawfully and fairly and using the necessary technical and organisational measures, taking into account the nature, scope, context and purposes of the processing and the risk of varying likelihood and severity for the rights or freedoms of natural persons;

2) processed for specified and legitimate purposes;

3) adequate, relevant and not excessive in relation to the purposes for which they are processed;

4) accurate and, where necessary, kept up to date;

5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

6) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using technical and organisational measures appropriate to the risks and the category of the data to be protected, and in particular protected against unauthorised access or unauthorised possession.

2. The controller shall take all steps to ensure that personal data which are inaccurate, in the light of the purposes for which they are processed, are erased or rectified without delay.

3. The controller shall be responsible for compliance with the principles relating to the processing of personal data and for the due performance of the activities in this regard referred to in subparagraphs 1 and 2 and in Articles 13 to 21, and shall be obliged to keep records relating to the performance of such activities. It is permissible to keep these records in electronic form.

4. The controller shall draw up and implement a personal data protection policy taking into account the method of documenting the measures referred to in subparagraph 1(1).

5. The controller shall keep the measures referred to in paragraph 1(1) under review with a view to updating them.

6. Other processors of personal data for the purposes referred to in Article 1(1) shall be bound to fulfil the obligations referred to in subparagraphs 1 to 5.

7. The controller shall document the factual or legal reasons for refusing to provide information or to make available personal data.

Article 32. 1. The controller shall, at the time of determining the means of processing and at the time of the processing itself, apply appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement personal data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into processing, in order to meet the requirements of this Act, protect the rights of data subjects and take into account the state of art, the cost of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

2 The controller shall apply appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the natural person's intervention to an indefinite number of natural persons or other entities.

3 The controller shall determine the appropriate technical measures and the necessary safeguards applicable to the processing of personal data in the data protection policy for the purpose of performance of the activities referred to in subparagraphs 1 and 2.

Article 33. 1. Where two or more controllers jointly determine the purposes and means of personal data processing within a single personal filing system, they become joint controllers.

2. Joint controllers:

1) agree by a written agreement the distribution of their responsibilities, in particular with regard to:

   a) exercising of the rights of the data subject under this Act,

   b) providing information referred to in Article 22(4)

   - unless the legal regulations applicable to these controllers specify the obligations assigned

to them and their scope;

2) designate a point of contact for data subjects in order to fulfil the obligation referred to in item 1(a).

Article 34. 1. The controller can entrust under a contract the processing of personal data to a processor.

2. The processor shall implement the necessary technical and organisational measures to ensure that the data are processed lawfully and in a manner that protects the rights of the data subjects.

3. The Contract referred to in subparagraph1 shall define, in particular:

1) its subject matter and effective term;

2) nature and purpose of the processing;

3) type of personal data processed;

4) categories of data subjects referred to in Article 19;

5) rights and obligations of the controller;

6) obligations of the processor referred to in subparagraph 5;

7) the manner in which the processing is controlled by the controller.

4. The Contract referred to in subparagraph 1 shall be drawn up in written form. It is also possible to draw up the contract in electronic form.

5. The processor shall be obliged to:

1) process the data only to the extent and for the purpose provided for in the contract;

2) act only as authorised by the controller;

3) ensure that persons authorised to process personal data have committed themselves to confidentiality, including as regards the technical means of securing the data;

4) assist the controller in complying with the provisions determining the data subject's rights;

5) after the completion of the provision of the processing service, at the controller's discretion:

a) erase or return to the controller any personal data and

b) delete any existing copies of personal data

- unless the retention of personal data is required by law;

6) make available to the controller any information relating to the verification of the correct execution of the data processing contract referred to in subparagraph 1;

7) respect the terms and conditions of use of services of another processor to whom it has entrusted the processing of personal data.

6. The processor may entrust the processing of data to another processor on a case-by-case basis only under a written contract, where the contract referred to in subparagraph 1 provides for such a right, on the terms and to the extent specified therein.

7. In cases where the processing of personal data is entrusted to a processor, the controller shall be responsible for compliance with the provisions of this Act, which shall not exclude the responsibility of the processor for processing of the data contrary to the Act or the contract referred to in subparagraph 1.

8. If the processor violates the provisions of this Act in the scope of determining the purposes or means of processing, it shall be considered to be the controller in respect of that processing.

Article 35. 1. The controller shall keep a record of the categories of processing activities for which it is responsible.

2. The record referred to in subparagraph 1 shall contain the following information:

1) name and surname or name and contact details of:

   a) the controller,

   b) the joint controller - in cases referred to in Article 33(1),

   c) the data protection officer,

   d) the processor - in the case referred to in Article 34(2) and (6);

2) the purposes of the processing;

3) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

4) a description of categories of data subjects and of categories of personal data;

5) information on the use of profiling - where it has been applied;

6) categories of transfers of personal data to a third country or an international organisation - where the transfer has taken place;

7) indication of the legal basis of the processing operations, including transfers for which the

personal data are intended;

8) the envisaged time limits for erasure of different categories of personal data - where possible;

9) a general description of the technical and organisational security measures to ensure the protection of personal data processed, as referred to in Article 39, where feasible.

3. The processor shall maintain a record of categories of the processing activities carried out on behalf of the controller.

4. The record referred to in subparagraph 3 shall contain the following information:

1) name and surname or name and contact details of:

a) the processor - in the case referred to in Article 34(2) and (6),

b) any controller, on behalf of which the processor is acting,

c) the data protection officer;

2) categories of processing carried out on behalf of each controller;

3) transfers of personal data to third countries or an international organisation, where explicitly instructed to do so by the controller, including the identification of that third country or international organisation, where applicable;

4) general description of the technical and organisational security measures referred to in Article 39, where possible.

5. The records referred to in subparagraphs 1 and 3 shall be kept in written, paper or electronic form.

6. The controller and the processor shall make the records referred to in subparagraphs 1 and 3 available to the President of the Office on request.

Article 36. 1. Processing operations in automated processing systems are logged.

2. The logs apply, in particular, to the following processing operations:

1) collection;

2) alteration;

3) consultation;

4) disclosure including transfer;

5) combination;

6) erasure.

3. The logs are kept automatically, in a way that makes it possible to determine the justification of the operations based on information indicating:

1) date and time of such operation;

2) identity of the person who consulted or disclosed personal data – as far as possible;

3) identity of recipients of personal data – as far as possible.

4. In the logs which are not kept in an automated manner, information on justification of the operation shall be additionally included.

5. The logs covering processing activities are intended solely for:

1) verification of the lawfulness of the processing;

2) self-monitoring;

3) ensuring the integrity and security of personal data;

4) for criminal proceedings.

6. The controller and the processor shall make the logs covering the processing activities available to the President of the Office on request.

Article 37. 1. Where a type of processing of personal data, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing of personal data, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The assessment referred to in subparagraph 1 shall contain at least:

1) a general description of the envisaged personal data processing operations;

2) an assessment of the risk to the rights and freedoms of data subjects;

3) measures envisaged to address those risks;

4) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act.

3. The controller may assign the implementation of the obligation referred to in subparagraph 1 to the data protection officer.

Article 38. 1. Prior to processing of personal data which will form part of a new filing system to be created, the controller or the processor shall apply to the President of the Office for consultation where:

1) the assessment referred to in Article 37(1) indicates that the processing of personal data would result in a high risk to natural persons' rights and freedoms in the absence of measures taken by controller to mitigate the risk, or

2) the type of personal data processing involves a high risk to the rights and freedoms of data subjects.

2. The President of the Office may establish a list of processing operations which are subject to prior consultation pursuant to paragraph 1. The President of the Office shall publish this list in the form of an announcement in the Official Journal of the Republic of Poland "Monitor Polski".

3. The controller shall present to the President of the Office:

1) the assessment referred to in Article 37(1), and

2) at the request of the President of the Office, any other information enabling the President of the Office to assess the compliance of the processing with the law and, in particular, to assess the risks in the area of protection of personal data of the data subject and the related safeguards.

4. If the President of the Office is of the opinion that the intended processing referred to in subparagraphs 1 and 2 would infringe the provisions of this Act, in particular where the President of the Office recognises that the controller has insufficiently identified or mitigated the risk, shall provide within a period of up to six weeks of receipt of the request for consultation referred to in subparagraph 1, written advice to the controller or the processor.

5. Taking into account the complexity of the matter, the period referred to in subparagraph 4 may be extended by one month, of which the President of the Office shall inform the controller or the processor within one month of receipt of the request referred to in subparagraph 1, together with the reasons for the extension.

6. The controller or the processor may assign the implementation of the obligations referred to in subparagraphs 1-4 to the data protection officer.

Section 2

Security of personal data

Article 39. The controller and the processor shall apply technical and organisational measures to ensure the protection of the personal data processed, adequate to the risks and the categories of data to be protected, which are aimed in particular at:

1) denying unauthorised persons access to processing equipment used for processing (‘equipment access control’);

2) preventing the unauthorised reading, copying, modification or removal of data media (‘data media control’);

3) preventing the unauthorised input of personal data and unauthorised inspection, modification or deletion of stored personal data (‘storage control’);

4) preventing the use of automated processing systems by unauthorised persons using data communication equipment (‘user control’);

5) ensuring that persons authorised to use an automated processing system have access only to the personal data covered by their authorisation (‘data access control’);

6) enabling that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (‘data communication control’);

7) ensuring that it is subsequently possible to verify and establish which personal data has been input into automated processing systems, when and by whom the personal data were input (‘input control’);

8) preventing the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (‘transport control’);

9) ensuring that installed systems may, in the case of interruption, be restored (‘recovery’);

10) ensuring that the functions of the system perform, that the appearance of faults in the functions is reported (‘reliability’) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (‘integrity’).

Article 40. The controller and the processor shall permanently destroy non-archivable computer storage media used for the processing of personal data decommissioned using appropriate tools and technical means. Decommissioner media may not be disposed of. A report shall be drawn up on the destruction of the media, including an indication of how they were destroyed.

Article 41. 1. Only a person who ensures the security of the personal data processed and who

has an authorisation to process personal data within a given category of processing activities, granted by the controller or the processor, may be allowed to process personal data. An application approved by the controller or the processor for the authorisation of access to personal data within a given category of processing activities shall be recognised as granting of such authorisation.

2. The application for access rights to personal data should contain:

1) name and surname, position, place of employment of the person concerned;

2) scope and duration of access to personal data;

3) type of personal data and the method of their processing.

3. The application must be accompanied by a declaration of the person concerned of his or her commitment to ensure the security of personal data, including the protection against unauthorised or unlawful processing of personal data and its accidental loss, destruction or damage.

4. The application and the declaration referred to in subparagraphs 2 and 3, respectively may be prepared in electronic form.

Article 42. 1. The controller or the processor shall keep records of persons authorised to process personal data, which shall include:

1) name and surname of the authorised person;

2) date of granting and expiry and the scope of the authorisation to process personal data;

3) identifier, if the data are processed in an ICT system.

2. The list of authorised persons, maintained on the basis of the applications for granting access rights to the data filing system referred to in Article 41 approved by the controller or the processor, may fulfil the role of the records referred to in subparagraph 1.

Article 43. Persons who have been authorised to process personal data are obliged to ensure the security of personal data, including the protection against unauthorised or unlawful processing of personal data and against its accidental loss, destruction or damage, as well as to maintain the confidentiality of the personal data provided and the means of securing the data.

Article 44. 1. In the case of a personal data breach, the controller shall, without undue delay but not later than 72 hours after having become aware of the breach, notify the breach to the President of the Office. The provision shall not apply if there is no risk to the rights and freedoms of natural persons.

2. Where the time limit referred to in subparagraph 1 is not met, the controller shall

immediately notify the breach and prepare and communicate to the President of the Office the reasons for the delay.

3. The processor shall notify the controller without undue delay but no later than within 48 hours after having become aware of a personal data breach.

4. The notification referred to in subparagraph 1 and 3 shall contain at least the following information:

1) description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2) name and surname or name and contact details of the data protection officer or other contact point that can provide additional information;

3) description of the likely consequences of the personal data breach;

4) description of the measures taken or proposed to be taken by the controller to address the personal data breach, including mitigating its possible adverse effects.

5. Where it is not possible to provide the information referred to in subparagraph 4 in a single notification, the information may be provided in phases without undue further delay.

6. The controller shall document for control purposes the personal data breaches referred to in subparagraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken, attaching a copy certified by him/her of the notification referred to in subparagraph 4.

7. Where the data breach involved personal data:

1) received from a controller of another Member State of the European Union,

2) transmitted to the controller of another Member State of the European Union

– the information referred to in subparagraph 4 shall be communicated to the controller of that Member State of the European Union without undue delay.

8. The President of the Office may conduct the inspection of the implementation by the controller of the obligations referred to in subparagraphs 1 to 7.

Article 45. 1. Where a personal data breach is likely to result in a high risk to the rights or freedoms of natural persons, the controller shall communicate the personal data breach to the data subject of, without undue delay.

2. The communication referred to in subparagraph 1 shall contain, in particular:

1) description of the nature of the personal data breach;

2) information referred to in Article 44 item 4 (2)-(4).

3. The communication referred to in subparagraph 1 shall not be required if any of the following conditions are met:

1) the controller has implemented appropriate technical and organisational protection measures, in particular those that render the personal data unintelligible to any person who is not unauthorised to access them it, such an encryption;

2) the controller has taken subsequent measures which ensure that the high risk to the rights or freedoms of data subjects referred in subparagraph 1 is no longer likely to materialise;

3) the notification would involve a disproportionate effort.

4. In the case referred to in subparagraph 3(3), the controller shall issue a public communication or use similar measure, containing the elements indicated in subparagraph 2, whereby the data subjects are informed in an equally effective manner.

5. If the controller has not already communicated the personal data breach to the data subject, the President of the Office, having considered the likelihood of the personal data breach resulting in a high risk, may:

1) require the controller to issue a notice;

2) decide that any of conditions referred to in subparagraph 3 are met.

6. In the case referred to in Article 26(1), the communication referred to in subparagraph 1 may be delayed, restricted or omitted.

Section 3

Data protection officer

Article 46. 1. The controller shall appoint the data protection officer.

2. The data protection officer may be a person who:

1) has full capacity to exercise legal acts and uses full public rights;

2) has adequate professional qualifications, in particular expertise in the scope of data protection law and practice, as well as the skills required to perform the tasks referred to in Article 47(1);

3) has not been convicted of an intentional crime or a fiscal offence by a final judgement.

3. The controllers may appoint a single data protection officer for several competent authorities, taking into account their organisational structure and size.

4. The controller who has appointed the officer may appoint a replacement for the officer during his/her absence, taking into account the criteria referred to in subparagraph 2.

5. In connection with the performance of the duties of the officer during his/her absence, the provisions relating to the officer shall apply *mutatis mutandis* to the person replacing him/her.

6. The authority that has appointed a replacement officer shall notify the President of the Office of the appointment in accordance with the procedure set out in subparagraph 10 and shall make his/her details available in accordance with subparagraph 11.

7. The data protection officer reports directly to the head of the organisational unit or to the natural person who acts as the controller or the processor.

8. The controller shall ensure that the data protection officer is properly and promptly involved in all matters concerning the protection of personal data.

9. The controller shall notify the appointment of the data protection officer to the President of the Office within 14 days from the date of appointment, indicating the name, surname, e-mail address or telephone number of the data protection officer. The notification shall be drawn up in electronic form and bear either a qualified electronic signature or a trusted signature. The notification may be issued by proxy. The notification shall be accompanied by a power of attorney granted in electronic form.

10. The controller shall notify the President of the Office of any change of the data referred to in subparagraph 9 and of the dismissal of the data protection officer within 14 days from the date of the change or the dismissal.

11. The controller shall make available the details of the data protection officer referred to in subparagraph 9 as soon as he or she has been appointed, on its website or, if it does not have its own website, in a manner generally accessible at the place of business.

Article 47. 1. The tasks of the data protection officer include:

1) informing the controller and the persons who carry out processing of their obligations under this Act and other data protection legislation;

2) conducting awareness-raising activities and providing training for staff involved in the processing operations;

3) monitoring the compliance of data processing by the controller and persons involved in the processing of personal data with the provisions of this Act and other data protection legislation;

4) monitoring the implementation of the controller's policies on the protection of personal data, including the assignment of responsibilities to the persons involved in the processing under these policies;

5) cooperation with the President of the Office;

6) monitoring the implementation of the recommendations referred to in Article 38(4) and reporting the status of their implementation to the President of the Office;

7) acting as a contact point for the President of the Office on issues relating to processing, including the prior consultation referred to in Article 38 and consulting the President of the Office on any other matters;

8) acting as a contact point for data subjects regarding their rights as referred to in Chapter 4;

9) preparing recommendations for a personal data protection impact assessment, in the case referred to in Article 37 and monitoring the implementation of those recommendations;

10) preparing and submitting to the controller once a year, by the end of the first quarter for the previous year, a report on the performance of tasks concerning the protection and the manner of processing personal data.

2. The controller shall support the data protection officer in performing the tasks referred to in subparagraph 1 by providing the resources necessary for the performance of those tasks and by ensuring access to personal data and processing operations as well as by enabling enhancement of his or her expert knowledge.

3. The controller may entrust the data protection officer with the performance of other duties where this will not prejudice the due performance of the data protection officer's tasks and will not result in a conflict of interest.

4. The Prime Minister shall determine, by way of a regulation, the procedure and the manner of performance of the tasks referred to in subparagraph 1, taking into consideration the necessity to ensure the due performance of the data protection officer's tasks as well as the independence and organisational autonomy in performing his/her tasks.

Chapter 6

Cooperation with supervisory authorities in other Member States of the European Union

Article 48. 1. The President of the Office shall provide assistance to supervisory authorities in other Member States of the European Union on their request.

2. The request for assistance refers in particular to:

1) providing information;

2) performing:

a) consultations,

b) inspection,

c) proceedings.

3. The President of the Office shall take any necessary steps to ensure that a request for assistance is implemented without undue delay, not later than within one month of receipt of the request.

4. The President of the Office may refuse to implement a request for assistance only if:

1) it is not the competent authority for the subject-matter of this request;

2) execution of this request would infringe any legal provisions.

5. The President of the Office shall inform the requesting supervisory authority in other Member States of the European Union of the refusal to execute the request and state the reasons for the refusal.

6. The President of the Office shall inform the requesting supervisory authority in other Member States of the European Union of the results or, where appropriate, of the progress or steps taken to respond to that request.

7. The President of the Office shall provide the information to the requesting supervisory authority in other Member States of the European Union in writing in paper form or electronically in an agreed format.

8. The President of the Office shall not charge a fee for acting on the request from the requesting supervisory authority in other Member States of the European Union.

9. In particularly justified cases, the President of the Office and the supervisory authority in other Member States of the European Union may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance.

Article 49. 1. The President of the Office may request assistance from a supervisory authority in other Member States of the European Union, in particular for the provision of information, conducting consultations, inspections or proceedings.

2. The request for assistance shall contain all necessary information, including the purpose and reasons for the request.

3. The President of the Office may only use information received from a supervisory authority in other Member States of the European Union for the purpose specified in the request for assistance.

4. The President of the Office may apply for obtaining from the supervisory authority in other Member States of the European Union information on the results or, if necessary, on the progress or measures taken to respond to that request.

Chapter 7

Remedies and liability

Article 50. 1. A person whose personal data are processed unlawfully has the right to lodge a complaint with the President of the Office within 30 days of becoming aware of the breach or receiving information from the controller.

2. The President of the Office shall provide the person who has lodged the complaint with legal assistance on such person's request pending the examination of the complaint by the President of the Office.

3. A complaint can be lodged using the form posted in the Public Information Bulletin on the homepage of the President of the Office, in writing, by fax, electronically or using the electronic platform of public administration services - ePUAP.

4. The President of the Office shall inform the person who has lodged the complaint of the progress of its investigation, the manner in which it was handled and the possibility of lodging a complaint with the administrative court. The provisions of Articles 225, 231 and Articles 237-239 of the Code of Administrative Procedure shall apply *mutatis mutandis* to the handling of complaints.

5. The President of the Office shall not provide the person lodging the complaint with information which may indicate that personal data are processed by the competent authorities in the situations referred to in Article 26(1).

6. The right to notifying a breach of the processing of personal data shall also apply to

persons other than those mentioned in subparagraph 1 if they become aware of such a breach in a reliable manner. Article 225 of the Code of Administrative Procedure shall apply *mutatis mutandis* to the processing of applications.

7. The data of the notifying party referred to in subparagraph 6 shall be kept confidential by the President of the Office upon a justified request of that party.

Article 51. 1. Any entity against whom the President of the Office has issued a decision shall have the right to lodge a complaint against that decision with an administrative court.

2. Every data subject shall have the right to lodge a complaint with an administrative court if the President of the Office has not handled a complaint or a notification lodged pursuant to Article 50 or has failed to inform the data subject within 3 months of the receipt of the complaint of the progress or outcome of the complaint.

3. The provisions of the Act of 30 August 2002 - Law on proceedings before administrative courts shall apply to the examination of complaints (Journal of Laws of 2023, item 259), except that:

1) the forwarding of the file and the response to the complaint shall take place within 30 days of receipt of the complaint;

2) the complaint shall be examined within 30 days from the day of receipt of the file together with the reply to the complaint.

Article 52. The data subject may authorise a non-profit social organisation which performs statutory activities in the public interest and which is active in protecting the rights and freedoms of data subjects in relation to the protection of their personal data to exercise the rights on his or her behalf, including the exercise of the remedies provided for in this Chapter.

Article 53. 1. A person who has suffered damage or harm as a result of an act violating this Act shall be entitled to compensation or damages from the controller.

2. The provisions of the Chapter 10 of the Act of 10 May 2018 on the Protection of Personal Data shall apply in proceedings for damages referred to in subparagraph 1.

3. In cases for declaring that controller's activities are incompatible with the provisions of this Act, the President of the Office may bring an action for and on behalf of the person referred to in subparagraph 1 and may intervene in the proceedings before the court at any stage thereof.

4. In the event that the President of the Office joins the pending proceedings before the court, the provisions of the Act of 17 November 1964 - Code of Civil Procedure on outside intervener

shall apply accordingly (Journal of Laws of 2021, item 1805, as amended)[3)]).

Chapter 8

Penal provisions

Article 54. 1. Whoever processes personal data referred to in the provisions on the protection of personal data processed in connection with preventing and combating crime, although the processing of such data is not permitted or the processing of such data is not authorised, shall be subject to a fine, restriction of liberty or imprisonment for up to two years.

2. If the act referred to in subparagraph 1 relates to sensitive data, the offender shall be liable to a fine, restriction of liberty or imprisonment for up to three years.

Article 55. Whoever frustrates or substantially hinders the inspector in carrying out an inspection of compliance with the provisions on the protection of personal data processed in connection with preventing and combating crime shall be liable to a fine, restriction of liberty or imprisonment for up to two years.

Chapter 9

Amendments to the regulations in Articles 56-97 (omitted)[4)]

Chapter 10

Transitional, adjusting and final provisions

Article 98. 1. A person acting as a data protection officer on the date of entry into force of this Act pursuant to the provisions of the Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws item 1000 and 1669), shall become the data protection officer and shall perform his/her function not longer, however, than 3 months from the date of entry into force of this Act, unless before that date the controller notifies the President of the Personal Data Protection Office of appointing another person as the data protection officer in the manner specified in Article 46.

1) A person who has become a data protection officer pursuant to paragraph (1) shall continue to perform his/her function also after the expiry of 3 months from the date of entry into force of this Act, if by that date the controller notifies the President of the Personal Data

3) The amendments to the consolidated text of the aforementioned Act were announced in Journal of Laws of 2021 items 1981, 2052, 2262, 2270, 2289, 2328 and 2459, of 2022 items 1, 366, 480, 807, 830, 974, 1098, 1301, 1371, 1692, 1855, 1967, 2127, 2140, 2180, 2339, 2436, 2600 and 2687 and of 2023 items 289, 326, 403, 535, 556, 614 and 739.

4) Published in the announcement of the Marshal of the Sejm of the Republic of Poland of 11 May 2023 concerning the announcement of the uniform text of the Act on the protection of personal data processed in connection with preventing and combating crime (Journal of Laws, item 1206).

Protection Office of his/her appointment, in the manner specified in Article 46.

2) A controller who, by the date of entry into force of this Act, has not appointed a data protection officer, as referred to in the Act of 10 May 2018 on the Protection of Personal Data, shall be obliged to appoint a data protection officer and notify the President of the Personal Data Protection Office of his/her appointment within 1 month from the date of entry into force of this Act.

Article 99. 1. The existing provisions shall apply to inspections initiated pursuant to the provisions of the Act of 29 August 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922 and of 2018, items 138 and 723) and not completed before the date of entry into force of this Act.

2. Authorisations and service cards issued before the date of entry into force of this Act shall remain valid until the inspections referred to in subparagraph 1 are completed.

Article 100. 1. Proceedings conducted by the President of the Personal Data Protection Office, initiated and not concluded before the date of entry into force of this Act, shall be conducted on the basis of the existing provisions.

2 Acts completed in the proceedings referred to in subparagraph 1 shall remain effective provided that they were performed in accordance with the rules in force at the time they were performed.

3 If a request for reconsideration of a case is filed before the date of entry into force of this Act, pursuant to Article 21 of the Act of 29 August 1997 on the Protection of Personal Data, the pending proceedings initiated by such request shall be discontinued by operation of law as of the date of entry into force of this Act.

4 The party who initiated the proceedings referred to in subparagraph 3 shall be notified by the authority of the right to lodge a complaint with an administrative court against the decision against which the party has lodged a request for reconsideration.

5 The time limit for lodging a complaint in the case referred to in subparagraph 4 shall be 3 months from the date of notification. Until this time limit expires, a decision against which a party has filed a request for reconsideration shall not be enforced.

Article 101. The entity to which the address or request referred to in Article 19a(1) and (2) of the Act of 29 August 1997 on the Protection of Personal Data was served before the date of entry into force of this Act, shall be obliged to provide the President of the Personal Data Protection

Office with a reply to the address or request, in writing, within 30 days from the date of entry into force of this Act.

Article 102. 1. Within 1 year from the date of entry into force of this Act, the controller shall adapt the principles of personal data processing to the technical and organisational measures referred to in Article 39.

2. Where this requires disproportionate effort or expense, the controller may adapt the automated systems for processing personal data to technical and organisational measures, within a period longer than that indicated in subparagraph 1, but no later than 6 May 2023.

3. The previous decisions determining the rules of providing access to information and personal data from the Central Database of Persons Deprived of Liberty, via the ICT system, shall remain in force until the date of entry into force of the decisions issued on the basis of Article 25d(1) of the Act of 9 April 2010 on the Prison Service, but no longer than for a period of 2 years from the date of entry into force of this Act.

4. The adaptation of the rules of processing of information and personal data in the data filing system established before the date of entry into force of this Act to the requirements referred to in Article 19, Article 20 and Article 36 shall take place no later than 6 May 2023.

Article 103. Authorisations to process personal data issued prior to the date of entry into force of the Act shall remain in force for a period of 12 months from the date of entry into force of this Act.

Article 104. Any consents issued by state services, state institutions and public authorities for making available by means of telecommunication devices or by means of tele-transmission of information, including personal data, to organisational units of the Police, organisational units of the Border Guard, the State Protection Service and bodies of the National Revenue Administration shall remain in force, subject to Article 102(3).

Article 105. The existing implementing provisions issued pursuant to:

1) Article 15(8) and Article 20(19) of the Act amended in Article 58,

2) Article 10a(8) and Article 11(2) of the Act amended by Article 59,

3) Article 25(3) of the Act amended in Article 80,

4) Article 29(8) of the Act amended in Article 72,

5) Article 42(6) of the Act amended in Article 81,

6) Article (10) of the Act amended in Article 85

– shall remain in force until the date of entry into force of new implementing provisions issued on the basis of, respectively:

1) Article 15(8), Article 20(1n) and Article 20(1o) of the Act amended by Article 58, in its wording provided under this Act,

2) Article 10a(18) and Article 11(2) of the Act amended in Article 59, in its wording provided under this Act,

3) Article 25(3) of the Act amended in Article 80, in its wording provided under this Act,

4) Article 29(17) of the Act amended in Article 72, in its wording provided under this Act,

5) Article 42(6) of the Act amended in Article 81, in its wording provided under this Act,

6) Article 10 of the Act amended in Article 85, in its wording provided under this Act,

– however, no longer than for a period of 12 months from the date of entry into force of this Act.

Article 106. 1. The maximum limit on expenditure from the state budget for the performance of tasks under this Act shall amount to:

1) in 2019 – PLN 1,250,000;

2) in 2020 – PLN 1,350,000;

3) in 2021 – PLN 1,380,000;

4) in 2022 – PLN 1,410,000;

5) in 2023 – PLN 1,450,000;

6) in 2024 – PLN 1,490,000;

7) in 2025 – PLN 1,530,000;

8) in 2026 – PLN 1,570,000;

9) in 2027 – PLN 1,610,000;

10) in 2028 – PLN 1,650,000.

2. The President of the Personal Data Protection Office shall monitor the use of the expenditure limit referred to in subparagraph 1 and evaluate the use of that limit as at the end of each quarter. The assessment for the fourth quarter is performed as at 20 November of the year in

question.

3. In the event that the maximum expenditure limit set out in subparagraph 1 for a given financial year is exceeded or a risk exists that it may be exceeded, and in the event that, in the period from the beginning of the calendar year to the date of the last assessment referred to in subparagraph 2, a part of the annual limit proportionally attributable to that period is exceeded by at least 10%, a corrective mechanism shall be applied to reduce the expenditure of the State budget that is the financial consequence of this Act.

4. The authority competent to implement the corrective mechanism referred to in subparagraph 3 shall be the President of the Protection of Personal Data Office.

Article 107. Article 1, Article 2, Article 3 (1), Articles 4-7, Articles 14-22, Articles 23-28, Article 31 and Chapters 4, 5 and 7 of the Act of 29 August 1997 on the Protection of Personal Data shall be repealed, remaining in force with regard to the processing of personal data for the purposes of recognition, prevention, detection and combating of criminal offences, the conduct of proceedings relating to such offences and the enforcement of decisions made therein, order penalties and coercive measures to the extent specified in the provisions constituting the basis for the operation of the services and authorities authorised to perform tasks in this respect, until the date of entry into force of the provisions implementing Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119 of 04.05.2016, p. 89) under Article 175 of the Act of 10 May 2018 on the Protection of Personal Data.

Article 108. The Act shall enter into force following the lapse of a period of 14 days as of the date of its promulgation[5)], with the exception of:

1) Article 58(12) that shall enter into force as of 1 November 2019;

2) Article 82(5) as regards Articles 25c to 25h that shall enter into force one year after the date of promulgation.

[5)] The Act was announced on 22 January 2019.