Unofficial translation

Act No. 110/2019 Coll.

Act of 12 March 2019 on personal data processing

(Consolidated version of 24 April 2019)

Issue	**47/2019**
Valid from	**24 April 2019**
Effective from	**24 April 2019**

The Parliament has adopted the following Act of the Czech Republic:

PART ONE

PERSONAL DATA PROCESSING

TITLE I

BASIC PROVISIONS

Section 1

Subject Matter

This Act transposes the applicable regulations of the European Union[1]); simultaneously, it follows on from directly applicable regulation of the European Union[2]) and, to satisfy the right of every person to protection of privacy, provides for the rights and obligations in personal data processing.

Section 2

Scope of the Act

This Act provides for the following:

(a) personal data processing pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council[2]);

(b) personal data processing by the competent authorities for the purpose of prevention, investigation or detection of criminal offences, prosecution of criminal offences, execution of criminal penalties and protective measures, ensuring security of the Czech Republic and ensuring public policy and national security, including search for persons and objects;

(c) personal data processing in ensuring defence and security interests of the Czech Republic;

(d) other processing of personal data that form or are intended to form part of a filing system or that are processed wholly or partly by automated means, other than personal data processing by a natural person in the course of a purely personal or household activity; and

(e) the status and powers of the Office for Personal Data Protection (hereinafter the “Office”).

Section 3

Data Subject

Data subject shall mean a natural person to whom personal data are related.

TITLE II

PERSONAL DATA PROCESSING PURSUANT TO DIRECTLY APPLICABLE REGULATION OF THE EUROPEAN UNION

Chapter 1

General Provisions

Section 4

Scope

(1) The provisions of this Title shall apply to personal data processing pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(2) The provisions of this Title and Regulation (EU) 2016/679 of the European Parliament and of

the Council shall also apply to processing of personal data that form or are intended to form part of a filing system or that is wholly or partly carried out by automated means, other than personal data processing by a natural person in the course of a purely personal or household activity;

(a) in the course of activities which fall outside the scope of Union law or the scope of Title III or IV; or

(b) in the course of activities which fall within the scope of Chapter 2 of Title V of the Treaty on the EU.

Section 5
Authorisation to Process Personal Data in Complying with Legal Obligation or Exercising Competence

Controllers may process personal data where it is necessary for compliance

(a) with their legal obligation stipulated by law; or

(b) with a task carried out in the public interest or in the exercise of official authority vested in the controller.

Section 6
Exemption from Compatibility of Purposes Assessment

(1) In ensuring a protected interest, controllers are not obliged to assess compatibility of purposes other than for which personal data were collected before processing of personal data for such other purpose, unless another legal regulation lays down otherwise and if this is necessary and proportionate for compliance with

(a) an obligation imposed on the controller; or

(b) a task carried out in the public interest laid down by a legal regulation or in the exercise of official authority vested in the controller.

(2) Protected interest pursuant to paragraph 1 above shall mean

(a) defence or security interests of the Czech Republic;

(b) public policy and national security, prevention, investigation or detection of criminal offences, prosecution of criminal offences, execution of criminal penalties and protective measures, ensuring security of the Czech Republic and ensuring public policy and national security, including search for persons and objects;

(c) some other important objective of public interest of the European Union or of a Member State of the European Union, in particular an important economic or financial interest of the European Union or of a Member State of the European Union, including monetary, pecuniary, budgetary and taxation matters, matters of financial market, public health and social security;

(d) protection of independence of courts and judges;

(e) prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(f) a monitoring, inspection or regulatory function connected to the exercise of official authority in the cases referred to in subparagraphs (a) to (e) above;

(g) protection of rights and freedoms of persons; or (h) enforcement of civil law claims.

Section 7
Capacity of Child to Grant Consent to Personal Data Processing

A child shall enjoy capacity to grant consent to personal data processing in relation to an offer of information society services addressed directly to the child from fifteen years of age.

Section 8
Obligation Regulated by Law to Provide Information on Processing

If the controller carries out personal data processing pursuant to Section 5 above and is obliged to provide information to the data subject pursuant to Art. 13 or Art. 14 (1),(2) and (4) of

Regulation (EU) 2016/679 of the European Parliament and of the Council, the controller may provide such information in a manner enabling remote access within a scope appropriate to the personal data processing usually carried out by the controller.

Section 9
Communication by Means of Change to Initial Filing System

If the controller has the obligation to communicate to the recipient a rectification, restriction of processing and/or erasure of personal data, it may do so by means of a change of the personal data in the filing system provided that the controller regularly discloses its valid contents to the recipient.

Section 10
Exemption from Assessment of Impact of Data Processing on Personal Data Protection

The controller need not carry out assessment of the impact of data processing on personal data protection prior to commencement of personal data processing if it is required to carry out such processing under a legal regulation.

Section 11
Limitation of Certain Rights and Obligations

(1) Unless another legal regulation lays down otherwise, Articles 12 to 22 and, as far as relevant, also Article 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply *mutatis mutandis* or the compliance with the controller's or processor's obligations or exercise of the data subject's right laid down in those articles shall be postponed if this is necessary and reasonable in terms of scope to ensure a protected interest set out in Section 6 (2) above.

(2) The controller or processor shall notify the Office of the limitation of some rights or obligations pursuant to paragraph 1 above without undue delay, specifying to a reasonable extent the facts pursuant to Art. 23 (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council; this shall not apply to courts carrying out personal data processing pursuant to Art. 55 (3) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

Section 12
Exemption from Obligation to Communicate Personal Data Breaches to Data Subject

If the controller is obliged to communicate personal data breaches to the data subject, it shall postpone the communication or limit its scope if this is necessary and reasonable in terms of scope to ensure a protected interest set out in Section 6 (2) above. Section 11 (2) shall apply *mutatis mutandis* to the notification of the above procedure to the Office.

Section 13
Personal Data with Restricted Processing

If personal data processing has been restricted pursuant to Art. 18 (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council, this is without prejudice to the obligation of the controller or processor to transfer or disclose such personal data if this obligation is laid down by a legal regulation. Such data shall be marked in transfer or disclosure as data specified in Art. 18 (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

Section 14
Designation of Data Protection Officer

In addition to public authorities, authorities established by law that perform tasks laid down by law in public interest also have the obligation to designate the data protection officer pursuant to Art 37 (1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

Section 15

Accreditation of Certification Bodies

Bodies authorised to issue personal data protection certification shall be accredited by an entity authorised to exercise the competence of an accreditation body under the law governing accreditation of bodies assessing conformity[3]).

Section 16
Personal Data Processing for Purposes of Scientific or Historical Research or for Statistical Purposes

(1) In processing personal data for the purpose of scientific or historical research or for statistical purposes, the controller or processor shall provide for compliance with specific measures for the protection of interests of the data subject appropriate to the state of the art, costs of implementation, nature, scope, context and purpose of processing, as well as risks to the rights and freedoms of natural persons of varying likelihood and severity. Such measures may include, in particular

(a) technical and organisational measures aimed at a consistent application of the obligation pursuant to Art. 5 (1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council;

(b) logging of at least all operations of collection, entering, alteration and erasure of personal data, which will make it possible to determine and verify the identity of the person performing the operation, and retaining such records for a period of at least 2 years from the operation;

(c) provision of information to persons who process personal data concerning obligations in the area of personal data protection;

(d) designation of the data protection officer;

(e) special limitation of access to personal data at the controller or processor,

(f) pseudonymisation of personal data;

(g) encryption of personal data;

(h) measures for ensuring permanent confidentiality, integrity, availability and resilience of processing systems and services;

(i) measures enabling restoration of the availability of and timely access to personal data in the event of an incident;

(j) process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(k) special limitation of transmission of personal data to a third country; or

(l) special limitation of personal data processing for some other purposes.

(2) If it allows for attaining the purpose set out in paragraph 1 above, the controller or processor shall further process the personal data set out in Art. 9 (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council in a form that does not permit identification of data subjects unless this is prevented by legitimate interests of the data subject.

(3) Unless another legal regulation lays down otherwise, Articles 15, 16, 18 and 21 and, as far as relevant, also Article 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply *mutatis mutandis* or the compliance with the controller's or processor's obligations or exercise of the data subject's right laid down in those articles shall be postponed if this is necessary and reasonable in terms of scope to fulfilment of the purpose of the processing set out in paragraph 1 above. Article 15 and, as far as relevant, also Article 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council shall not apply if the processing is necessary for purposes of scientific research and the provision of such information would involve disproportionate effort.

Chapter 2
Personal Data Processing for Journalistic Purposes or Purposes of Academic, Artistic or Literary Expression

Section 17
Lawfulness of processing

(1) Personal data may also be processed if it serves appropriately for journalistic purposes or the purposes of academic, artistic or literary expression. In assessing appropriateness pursuant to the first sentence, account shall be taken of whether the processing includes personal data set out in Art. 9 (1) or Art. 10 of Regulation (EU) 2016/679 of the European Parliament and of the Council.

(2) Personal data processing for the purposes set out in paragraph 1 above is not conditional on authorisation or approval by the Office and enjoys the right to protection of the source and contents of the information, including in case that the personal data are processed in a manner enabling remote access.

Section 18
Exemptions from Controller's Obligation to Provide Advice and Information

(1) In processing personal data for the purposes set out in Section 17 (1) above, the controller may perform its obligations following from Art. 12 (1) and (2), Art. 13 (1) to (3) and Art. 21 (4) and, as far as relevant, also from Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council, also by informing the data subject of the controller's identity in any suitable manner. Information on the controller's identity may also be provided by virtue of suitable declaration of association with the controller, which may be carried out by a graphic designation, orally or by way of other appropriate means. Information on the controller's identity is sufficient if the advice provided by the controller concerning the rights of the data subject and other facts necessary for protection of the rights of the data subject, within a scope appropriate to the personal data processing usually performed by the controller, is publicly available in a manner enabling remote access.

(2) Information on the controller's identity need not be provided in justified cases, in particular if:

(a) it is impossible or it would involve disproportionate effort;

(b) the data subject can legitimately expect the processing set out in Section 17 (1);

(c) the data subject possesses the information; or

(d) provision of such information would endanger or frustrate the purpose of personal data processing, if such a procedure is necessary to achieve a legitimate purpose of processing, especially in matters of public interest.

Instead of excluding the provision of information on the controller's identity, the controller may postpone the provision of such information.

Section 19
Protection of Source and Contents of Information

(1) The obligation to provide information pursuant to Art. 14 (1) to (4) and Art. 21 (4) and, as far as relevant, also Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council, as well as to provide information on other rights of the data subject, can also be performed by publishing such information in a manner enabling remote access; in that case, it is sufficient to provide information on the personal data processing usually performed by the controller.

(2) The right to access to personal data pursuant to Art. 15 and, as far as relevant, pursuant to Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council shall not apply

if the personal data concerned were not published by the controller and are processed only for the purpose set out in Section 17 (1). In other cases, the controller may exclude access to personal data in justified cases, especially if a legitimate purpose of personal data processing would otherwise be endangered or frustrated or if the provision of access would involve disproportionate effort.

(3) Art. 14 (2)(f) and Art. 15 (1)(g) and, as far as relevant, also Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council shall not apply to personal data processing for the purposes set out in Section 17 (1).

(4) If the controller is obliged to notify personal data breach pursuant to Art. 33 (1) or Art. 34 (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council, it need not notify information enabling determination of the source or contents of the personal data whose security was breached.

Section 20
Exemption from Rights to Rectification, Erasure and Restriction of Personal Data Processing

(1) If the rights to erasure or rectification are exercised with respect to personal data processed for the purposes set out in Section 17 (1), other legal regulations shall apply[4]).

(2) If personal data are processed for the purposes set out in Section 17 (1), the data subject has the right to restriction of personal data processing pursuant to Art. 18 and, as far as relevant, also pursuant to Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council only if the controller no longer needs the personal data for the purposes of processing but the data subject requires the data for the establishment, exercise or defence of legal claims. This shall not apply if the above would involve disproportionate effort.

Section 21
Providing Information on Rectification, Erasure and Restriction of Processing

(1) If, in connection with personal data processing for the purposes set out in Section 17 (1) performed also in a manner enabling remote access, the controller is obliged to communicate to the recipients rectification, erasure or restriction of personal data processing pursuant to Art. 17 (2) or Art. 19 and, as far as relevant, also pursuant to Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council, it may perform this obligation also by specifying the time of the last update of the contents in which the personal data are or were contained, or using some other appropriate measure.

(2) Rectification, erasure or restriction of processing pursuant to Art. 19 and, as far as relevant, also pursuant to Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council, shall be communicated to the party to which the controller transmitted personal data processed for the purposes set out in Section 17 (1) if this is required for protection of the rights or justified interests of the data subject and does not involve disproportionate effort.

(3) The controller may inform the data subject only about categories of recipients if, in connection with personal data processing for the purposes set out in Section 17 (1), the provision of information to the data subject on recipients pursuant to Art. 19 and, as far as relevant, also pursuant to Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council involves disproportionate effort or if a legitimate purpose of processing would be endangered or frustrated.

Section 22
Restriction of Right to Object

(1) The right to object pursuant to Art. 21 and, as far as relevant, also pursuant to Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council, is available only with

regard to a specific disclosure or publishing of personal data processed for the purposes set out in Section 17 (1); the data subject shall indicate specific reasons suggesting that a justified interest in the protection of his or her rights and freedoms overrides the interest in such disclosure or publishing.

(2) If an objection has been made pursuant to paragraph 1 above, the controller is obliged to discontinue such disclosure or publishing if in its opinion the data subject has proven that the justified interest in protection of his or her rights and freedoms overrides the interest in such publishing. The controller shall inform the data subject without undue delay whether it has complied with the data subject's objection.

Section 23
Other Exemptions for Special Cases

(1) Sections 18 to 22 and Art. 12 to 19, 21, 33 and 34 and, as far as relevant, also pursuant to Art. 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council shall not apply, shall apply *mutatis mutandis* or the compliance with the obligations of the controller or processor or exercise of the right of the data subject laid down therein shall be postponed

(a) if such a procedure is necessary to achieve a legitimate purpose of processing set out in Section 17 (1); and

(b) if such a procedure is not likely to result in a high risk for the justified interests of the data subject.

(2) Chapter VII of Regulation (EU) 2016/679 of the European Parliament and of the Council shall not apply in the processing set out in Section 17 (1). Art. 20, 22, 56 and 58 (1)(a),(b),(e) and (f) and Art. 58 (2)(d),(f) and (g) and Chapters II, IV, V and IX of Regulation (EU) 2016/679 of the European Parliament and of the Council shall not apply, shall apply *mutatis mutandis* or the compliance with the controller's or processor's obligations or exercise of the data subject's right laid down in those provisions shall be postponed if this is necessary to attain the purpose of processing set out in Section 17 (1).

(3) If the exclusion or restriction of some rights or obligations pursuant to paragraph 2 above would likely result in a high risk for the justified interests of the data subject, the controller or processor shall without undue delay implement and document suitable measures to mitigate these risks or any similar risk.

TITLE III

PROTECTION OF PERSONAL DATA IN THEIR PROCESSING FOR THE PURPOSE OF PREVENTION, INVESTIGATION OR DETECTION OF CRIMINAL OFFENCES, PROSECUTION OF CRIMINAL OFFENCES, EXECUTION OF CRIMINAL PENALTIES AND PROTECTIVE MEASURES, ENSURING SECURITY OF THE CZECH REPUBLIC AND ENSURING PUBLIC POLICY AND NATIONAL SECURITY

Section 24
General Provisions

(1) Unless laid down otherwise by law, this Title shall apply in personal data processing that is necessary for performing the task and exercise of public powers by the controlling authority laid down by other laws[5)] for the purpose of prevention, investigation or detection of criminal offences, prosecution of criminal offences, execution of criminal penalties and protective measures, ensuring security of the Czech Republic and ensuring public policy and national security, including search for persons and objects.

(2) For the purposes of this title, Art. 4 (1) to (6), (8), (9), (12) to (15) and (26) of Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply *mutatis mutandis*.

(3) Controlling authority shall mean a public authority other than an intelligence service or municipal police that is competent to perform the task set out in paragraph 1 above.

(4) This Title shall apply to processing of personal data that form or are intended to form part of a filing system or to processing carried out wholly or partly by automated means.

Section 25
Principles Relating to Processing of Personal Data

(1) In personal data processing, the controlling authority shall

(a) determine a specific purpose of personal data processing in connection with performance of the task set out in Section 24 (1);

(b) implement measures ensuring that personal data are accurate in relation to the nature and purpose of the processing; and

(c) keep personal data in a form enabling identification of the data subject only for the period necessary for achieving the purpose of their processing.

(2) Personal data may be processed for a purpose unrelated to the performance of a task set out in Section 24 (1) only if the controlling authority is authorised to do so and the purpose concerned is not incompatible with the set specific purpose of their processing.

Section 26
Categories of Data Subjects and Personal Data Quality

If possible, the controlling authority

(a) shall attach information to the personal data being processed on the status of the data subject in criminal proceedings and, where appropriate, also information on final decisions of prosecuting bodies relating to such data if this is justified by the purpose of their processing; and

(b) shall indicate any inaccurate personal data or personal data that are based on personal evaluations.

Section 27
Information for Data Subject

The controlling authority shall publish, in a manner enabling remote access, information on

(a) its name and contact details;

(b) contact details of the data protection officer (hereinafter the “officer”);

(c) the purpose of personal data processing;

(d) the right to lodge a complaint with the Office and the contact details of the Office; and

(e) the right of access to, rectification and erasure of personal data and restriction of their processing.

Section 28
Right of Access to Personal Data

(1) At the data subject’s request, the controlling authority shall specify whether it processes personal data relating to him or her. If the controlling authority processes such data, it shall transmit them to the data subject and inform the data subject about

(a) the purpose of personal data processing;

(b) the main legal regulations under which it processes such data;

(c) the recipients or, where appropriate, categories of recipients;

(d) the anticipated storage period or a manner in which it is determined;

(e) the right to request rectification, restriction of processing or erasure of personal data; and

(f) the source of such data.

(2) The controlling authority shall not comply with the request pursuant to paragraph 1 above, or comply only partly, if complying with the request would endanger

(a) performance of a task in the area of prevention, investigation and detection of criminal

offences, prosecution of criminal offences, execution of criminal penalties and protective measures, ensuring security of the Czech Republic and ensuring public policy and national security, including search for persons and objects;

(b) any proceedings concerning an infraction, disciplinary infraction or conduct having the elements of infraction;

(c) protection of classified information; or

(d) justified interests of a third party.

(3) If any of the dangers listed in paragraph 2 above would arise by complying with the request or communication of non-compliance with the request, including justification, the controlling authority shall inform the data subject as well as those applicants whose personal data are not processed by the controlling authority.

(4) The controlling authority shall keep records of the reasons for the procedure pursuant to paragraphs 2 and 3 above and keep these records at least for a period of 3 years.

Section 29
Right to Rectification, Restriction of Processing or Erasure of Personal Data

(1) At request of the data subject, the controlling authority shall carry out rectification or completion of personal data relating to the data subject. If required by the purpose of personal data processing, the controlling authority may, instead of rectification, supplement the personal data or attach to them an additional declaration.

(2) At request of the data subject, the controlling authority shall erase the personal data relating to that data subject if the controlling authority has breached the principles of personal data processing pursuant to Section 25 or some other legal regulation[5]) or the principles of processing of some categories of personal data or if the controlling authority is obliged to erase such data.

(3) Instead of rectification or erasure of personal data, the controlling authority may restrict the processing of personal data by specifically marking them

(a) if the data subject contests their accuracy without it being possible to ascertain whether the data are accurate; or

(b) if such data must be kept for the purposes of taking of evidence.

(4) If personal data processing is restricted pursuant to paragraph 3(a) above, the controlling authority shall inform the data subject prior to reversal of such a restriction; the controlling authority shall also inform the data subject whether the restriction is to be reversed on the basis of a decision of the Office or the competent court.

(5) The controlling authority shall not comply with the request pursuant to paragraphs 1 to 3 above, or comply only partly, if any of the dangers pursuant to Section 28 (2) would arise as a result of complying with the request. If any of the dangers pursuant to Section 28 (2) would arise through a communication of non-compliance with the request, including justification, the controlling authority shall inform the applicant in such a way as to prevent such a danger.

(6) The controlling authority shall keep records of the reasons for the procedure pursuant to paragraph 5 above and keep these records at least for a period of 3 years.

Section 30
Joint Provision on Data Subjects' Requests

(1) The controlling authority shall process a request pursuant to Section 28 or 29 without undue delay, not later than 60 days of the date of its lodging.

(2) If the controlling authority demonstrates that the request pursuant to Section 28 or 29 is manifestly unfounded or excessive, in particular because it has been lodged repeatedly within a short period of time in the same matter, the controlling authority need not comply with the

request.

(3) Within processing of the request pursuant to Section 28 or 29, the controlling authority shall inform the data subject of the possibility to

(a) request verification of legality of the personal data processing through the Office, and shall provide information on the contact details of the Office;

(b) lodge a complaint with the Office; and

(c) seek a judicial remedy.

(4) The controlling authority shall inform the data subject in writing about the processing of the request pursuant to Section 28 or 29. Information on the processing of the request shall contain reasoning, unless the request is complied with to the full extent. If the data subject is represented, the controlling authority may request that the signature on the written power of attorney be authenticated; authentication is not required if the power of attorney was granted before the controlling authority.

(5) Paragraph 3(a) and (b) above shall not apply if the controlling authority is a court or the Public Prosecutor's Office.

Section 31
Instigation of Data Subject for Verification of Lawfulness of Personal Data Processing

(1) Based on an instigation of the data subject, the Office may verify lawfulness of personal data processing.

(2) The Office need not comply with an instigation pursuant to paragraph 1 above especially when it proves that the instigation is manifestly unfounded or excessive, for example because it has been made repeatedly within a short period of time in the same matter.

(3) Within 4 months of the date of lodging the instigation for verification of lawfulness of personal data processing, the Office shall inform the data subject as to whether or not it has verified lawfulness of the processing; if the Office has not carried out the verification, it shall attach information substantiating its procedure.

(4) The Office shall also inform the data subject of the possibility to seek a judicial remedy.

Section 32
General Obligations of Controlling Authority and Personal Data Protection by Design

(1) Taking account of the nature, scope, circumstances, purposes and risks of personal data processing, the controlling authority shall take such technical and organisational measures as to ensure and document compliance with its obligations in personal data protection.

(2) Taking account of the nature, scope, circumstances, purposes and risks of personal data processing, state of the art and costs, the controlling authority shall take technical and organisational measures with the objective of

(a) protecting personal data as efficiently as possible;

(b) limiting inappropriate personal data processing;

(c) limiting personal data processing that is not essential with regard to its scope, quantity of data, storage period or availability of data;

(d) providing necessary safeguards for the rights of the data subject; and

(e) preventing automatic publication of personal data.

(3) The controlling authority shall document the measures taken pursuant to paragraph 1 and 2 above and retain the documentation during the period of personal data processing.

(4) The controlling authority shall keep written overviews of all typified activities of personal data processing, which shall contain

(a) name and contact details of the controlling authority and the officer;

(b) purpose of personal data processing;
(c) categories of recipients or future recipients;
(d) categories of data subjects and categories of personal data;
(e) information on whether and how profiling is applied;
(f) categories of transmissions to third countries or international organisations;
(g) legal basis for the processing operations for which the personal data are intended;
(h) time limits for erasure or review of necessity of personal data categories; and
(i) general description of personal data security.

(5) If an incorrect transfer or transfer of inaccurate personal data occurs, the controlling authority shall inform of this fact without undue delay the recipient of such data and the authority competent to carry out the purpose set out in Section 24 (1), which is the originator of the data. If the controlling authority has performed a rectification, completion, restriction of processing or erasure of personal data, it shall advise also the recipient of the data about the necessity to take this procedure.

Section 33
Jointly Controlling Authorities

If several controlling authorities jointly determine purposes and means of personal data processing, they shall enter into a written agreement providing for the manner of performance of the obligations under this Part and a point of contact for collection of data subjects' requests, unless laid down otherwise by the law.

Section 34
Processor

(1) Only a processor who is able to effectively ensure compliance with obligations in personal data protection by taking the measures pursuant to Section 32 (1) shall be entrusted by the controlling authority with personal data processing.

(2) If the processor's mandate does not follow from a legal regulation, the controlling authority shall enter into a written contract for personal data processing with the processor. Unless this follows directly from a legal regulation, the contract shall determine, in particular, the following:
(a) subject-matter and duration of the personal data processing;
(b) nature and purpose of the personal data processing;
(c) type of personal data to be processed;
(d) categories of data subjects; and
(e) rights and obligations of the controlling authority.

(3) The contract for personal data processing shall further determine, unless this follows directly from a legal regulation, that the processor
(a) shall act only on the instructions of the controlling authority;
(b) shall ensure that persons authorised to process the personal data have committed themselves to confidentiality;
(c) shall assist the controller in ensuring compliance with the obligations pursuant to this Title;
(d) upon completion of its activities shall transfer, on instruction of the controlling authority, the personal data to the controlling authority or erase them, unless the law requires otherwise; and
(e) shall provide the controlling authority with information necessary for documenting compliance with the obligations pursuant to subparagraphs (a) to (d) and paragraphs 1 and 2 above.

(4) The processor shall keep written overviews of all typified activities of personal data processing, which shall contain
(a) name and contact details of the controlling authority, the processor and the officer;

(b) categories of personal data processing for the individual controlling authorities;
(c) information on transfer of personal data to specific third countries or international organisations; and
(d) general description of personal data security.
(5) The processor shall without undue delay notify the controlling authority of any personal data breach.
(6) The processor may mandate some other processor only with the prior written consent of the controlling authority. If the consent of the controlling authority is granted generally for an unspecified other processor, the processor with which the controlling authority entered into the contract for personal data processing shall inform the controlling authority in advance of all envisaged mandates of other processors. Paragraphs 1 to 3 above shall apply *mutatis mutandis* to the relationship between the processor with which the controlling authority entered into the contract for personal data processing and the other processor.

Section 35
Binding Nature of Controlling Authority's Instructions

The processor or a natural person acting under the authority of the controlling authority or the processor may process personal data only under the instructions of the controlling authority unless laid down otherwise by the law.

Section 36
Automated Logging

(1) If the controlling authority performs automated personal data processing, it shall log at least the operations of collection, entering, alteration, combining, consultation, transfer, disclosure and erasure of personal data.
(2) Logs of operations of collecting, entering, consultation and disclosure pursuant to paragraph 1 above enable determination and verification of the reason and time of such operations, identity of the person performing the operation and identity of the recipient unless the identity of the aforementioned persons cannot be identified due to technical reasons.
(3) The logs pursuant to paragraph 1 above may be used only for the purposes of criminal proceedings, verification of lawfulness of personal data processing, ensuring integrity of personal data and ensuring performance of the tasks of the controlling authority or processor and performance of obligations by the persons to whom access to personal data is provided.
(4) The records pursuant to paragraph 1 above shall be kept for a period of 3 years of erasure of the personal data to which they pertain.
(5) The obligations of the controlling authority laid down in paragraphs 1 to 4 above shall apply to the processors *mutatis mutandis*.

Section 37
Data Protection Impact Assessment

If a specific kind of envisaged personal data processing, considering its nature, scope, circumstances or purpose, is likely to result in a high risk of unauthorised interference with the rights and freedoms of the data subject, the controlling authority shall draw up an assessment of impact of such processing on personal data protection, which shall contain at least the following:
(a) general description of the envisaged personal data processing and its operations;
(b) assessment of the risk of unauthorised interference with the rights and freedoms of data subjects; and
(c) planned measures and appropriate safeguards to mitigate the risk pursuant to subparagraph (b) above and compliance with the obligations pursuant to this Title.

Section 38

Consultation with the Office

(1) If an envisaged personal data processing is to give rise to new records, the controlling authority shall lodge with the Office a request for consultation of the processing concerned, if

(a) high risk of unauthorised interference with the rights and freedoms of data subjects follows from the assessment pursuant to Section 37; or

(b) the type of personal data processing concerned, taking into account the use of new technologies or procedures, results in a high risk of interference with the rights and freedoms of data subjects.

(2) The request pursuant to paragraph 1 above shall include the impact assessment pursuant to Section 37; at request of the Office, the controlling authority shall provide also other related information.

(3) The Office may issue a register of personal data processing operations in relation to which the controlling authority is obliged to consult the Office. The controlling authority shall inform the Office of any such processing.

(4) If the Office considers that the provisions of this Title or provisions of any other legal regulation on personal data processing would be breached by the envisaged personal data processing, it shall advise the controlling authority of this fact within 6 weeks of the date of lodging the request pursuant to paragraph 1 above, or, where appropriate, exercise its other powers. The Office may extend the above deadline by 1 month on grounds of complexity; the Office shall inform the controlling authority of the extension within 1 month of the date of lodging the request.

Section 39
Intervention Based on Automated Processing

The controlling authority may, on the basis of exclusively automated personal data processing, interfere with the rights and legally protected interests of the data subject or cause the data subject to face some other similarly serious consequence only if this is expressly laid down by another law.

Section 40
Security of Personal Data Processing

(1) The controlling authority shall implement such organisational and technical measures as to ensure a level of security of personal data appropriate to the nature, scope, circumstances, purpose and risk of their processing.

(2) If personal data are processed by automated means, the controlling authority shall implement necessary measures in order to

(a) secure the personal data against unauthorised access, transmission, alteration, destruction, loss, theft, abuse or other unauthorised processing;

(b) ensure recoverability of the personal data;

(c) ensure the possibility to determine and verify the person who entered the personal data or to whom they have been transferred or disclosed using data communication equipment;

(d) ensure security and reliability of the information system containing the personal data, including reporting of errors; and

(e) prevent unauthorised access to the personal data carrier or equipment used for their processing.

(3) The obligations of the controlling authority laid down in paragraphs 1 and 2 above shall apply to the processors *mutatis mutandis*.

Section 41
Notification of Personal Data Breach to the Office

(1) The controlling authority shall notify without undue delay any personal data breach to the Office unless the risk of unauthorised interference with the rights and freedoms of the data subject is low.
(2) If the controlling authority gives the notification more than 72 hours after becoming aware of the breach, it shall enclose reasoning of the delay.
(3) In the notification pursuant to paragraph 1 above, the controlling authority shall indicate at least the following, as far as it possesses such information:
(a) description of the nature of the personal data breach;
(b) categories and approximate number of data subjects and personal data records concerned;
(c) name and contact details of the officer or some other workplace where more information on the personal data breach can be obtained;
(d) description of the likely consequences of the personal data breach; and
(e) description of the measures taken or proposed to be taken by the controlling authority to remedy or mitigate the damage caused by the personal data breach.
(4) The controlling authority shall supplement any facts pursuant to paragraph 3 above that were not known to the controlling authority at the time of the notification without undue delay after becoming aware thereof.
(5) The controlling authority shall communicate the facts pursuant to paragraph 3 above also to a person or authority of some other Member State of the European Union that provided or obtained the personal data.
(6) The controlling authority shall document each case of personal data breach, its consequences and remedial measures implemented and retain the documentation for at least 3 years.

Section 42
Communication of Personal Data Breach to the Data Subject

(1) The controlling authority shall communicate without undue delay any personal data breach to the data subject if the ensuing risk of unauthorised interference with the rights and freedoms of the data subject is high.
(2) In the communication, the controlling authority shall provide at least the data set out in Section 41 (3)(a) and (c) to (e).
(3) If the communication to the data subject pursuant to paragraph 1 above involves disproportionate effort, the controlling authority shall publish the communication by way of appropriate means.
(4) The controlling authority is not obliged to communicate a personal data breach if
(a) the technical and organisational measures taken ensure that it is impossible to misuse the personal data concerned; or
(b) subsequent measures of the controlling authority have significantly reduced the risk of unauthorised interference with the rights and freedoms of the data subject.
(5) The Office may also decide that there is a high risk of unauthorised interference with the rights and freedoms of the data subject or that the conditions pursuant to paragraph 4 above have been met.
(6) The controlling authority shall not communicate a personal data breach, or communicate it only partly if the communication would result in a danger pursuant to Section 28 (2).

TITLE IV
PERSONAL DATA PROTECTION IN ENSURING DEFENCE AND SECURITY INTERESTS OF THE CZECH REPUBLIC

Section 43

(1) Unless other legal regulations[6]) lay down otherwise, the provisions of this Title shall apply to personal data processing for the purpose of ensuring defence and security interests of the Czech Republic.

(2) For the purposes of this Title, Art. 4 (1), (2), (6) to (8), (9) and (11) of Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply *mutatis mutandis*.

(3) The controller may only process personal data with the consent of the relevant data subject. Without such consent, the controller may process the personal data if

(a) processing is necessary for compliance with the controller's obligation;

(b) processing is necessary for the performance of a contract to which the data subject is party or for the purposes of negotiations aimed at entering into or amending a contract initiated by the data subject;

(c) processing is necessary in order to protect the vital interests of the data subject; in such a case, consent of the data subject shall be obtained without undue delay, otherwise the controller shall discontinue the processing and erase the data;

(d) processing concerns legitimately published personal data;

(e) processing is necessary for the protection of rights or legally protected interests of the controller, recipient or other person concerned; however, such processing of personal data may not be at variance with the right of the data subject to protection of his or her private and personal life;

(f) provides personal data on a public person, official or employee of a public authority that reveal his or her public or official activities, function or job; or

(g) processing is carried out solely for archiving purposes.

(4) Prior to granting his or her consent, the data subject shall be informed of the purpose of processing and for what personal data is the consent being granted, to which controller and for what period of time. The controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data throughout the entire term of the processing.

(5) The obligations laid down in paragraphs 3 and 4 above shall apply to the processors *mutatis mutandis*.

Section 44

If the mandate does not follow from another legal regulation, the controller shall enter into a contract for personal data processing with the processor. The contract shall be made in writing. The contract shall explicitly specify in particular the scope, purpose and term of processing and contain the processor's warranties on taking of, and compliance with, technical and organisational measures aimed at ensuring security and protection of personal data.

Section 45

Should the processor ascertain that the controller is in breach of obligations laid down by this Act or another legal regulation[6]), the processor shall immediately notify the controller or such a fact and discontinue personal data processing. Should the processor fail to do so, it shall be liable for the resulting damage together with the controller jointly and severally.

Obligations of Persons in Securing Personal Data

Section 46

(1) The controller is obliged to take technical and organisational measures preventing unlawful or accidental access to personal data, their alteration, destruction, loss, unauthorised transmission or other unauthorised processing or abuse. This obligation shall survive discontinuation of personal data processing.

(2) The controller is obliged to take technical and organisational measures aimed at protection of

personal data in accordance with this Act and other legal regulations. The controller shall document the technical and organisational measures taken and retain the documentation during the period of personal data processing.

(3) Within the measures pursuant to paragraph 1 above, the controller shall assess risks associated with the following areas

(a) fulfilment of instructions for personal data processing by persons who have direct access to personal data;

(b) preventing unauthorised persons from accessing personal data and means for their processing;

(c) preventing unauthorised reading, creation, copying, transmission, alteration or deletion of records containing personal data and

(d) measures for determining and verifying to whom the personal data were transferred.

(4) In automated personal data processing, the controller's obligations under the measures provided for in paragraph 1 above shall also include

(a) ensuring that the automated personal data processing system is used only by an authorised natural person;

(b) ensuring that the authorised natural person only has access to personal data corresponding to the scope of his or her authorisation based on special user rights established exclusively for him or her;

(c) making of electronic records allowing tracing and verification of when, by whom and for what reason the personal data were recorded or otherwise processed; and

(d) preventing unauthorised access to data carriers.

(5) The obligations laid down in paragraphs 1 to 4 above shall apply to the processors *mutatis mutandis*.

Section 47

Employees of the controller or processor, other persons processing personal data based on a contract with the controller or processor or persons who come into contact with personal data at the controller or processor in exercise of their authorisation and performance of their obligations following from law are obliged to maintain confidentiality of the personal data, as well as of the organisational and technical measures the publication of which would endanger the security of the personal data. The confidentiality obligation shall survive termination of employment or the relevant work.

Section 48
Erasure of Personal Data

The controller or, on the controller's instruction, the processor, is obliged to erase personal data once the purpose for which the personal data were processed ceases to exist or based on a request of the data subject pursuant to Section 49.

Section 49
Protection of Rights of Data Subjects

(1) Every data subject who believes that the controller or processor processes his or her personal data at variance with the protection of private and personal life of the data subject or at variance with this Title, especially where the personal data are inaccurate with regard to the purpose of their processing, he or she may

(a) request explanation from the controller or processor; or

(b) request that the controller or processor remedy the state of affairs, in particular by means of rectification, completion or erasure of the personal data.

(2) If the request of the data subject pursuant to paragraph 1(b) above is found justified, the controller or the processor shall remedy the defective state of affairs without undue delay.

(3) Should the obligations imposed by law be breached at the controller or the processor during personal data processing, the controller and the processor shall be liable for the resulting damage jointly and severally.

(4) The controller is obliged to inform the recipient without undue delay of request of a data subject pursuant to paragraph 1 above and on the rectification, completion or erasure of personal data. The above shall not apply if informing the recipient is impossible or involves a disproportionate effort.

TITLE V
OFFICE
Section 50

(1) The Office is the central administrative authority in the field of personal data protection within the scope laid down by this Act, other legal regulations[5]), international treaties that form part of the national laws, and directly applicable regulations of the European Union.

(2) The seat of the Office is in Prague.

Section 51

(1) Activities of the Office may only be interfered with on the basis of a law. In exercising its competence in the area of personal data protection, the Office shall act independently and follow only the legal regulations and directly applicable regulations of the European Union.

(2) Activities of the Office shall be paid for from a separate chapter of the State budget of the Czech Republic.

(3) The Deputy Minister of the Interior for the Civil Service shall not be the superior service body for the President of the Office. Decisions of the President of the Office concerning civil service matters and decisions of a first-instance disciplinary committee established in the Office shall not be subject to appeal.

President and Vice-president of the Office
Section 52

(1) The Office shall be headed by the President of the Office appointed and removed by the President of the Republic on the proposal of the Senate. President of the Office shall be deemed to be a member of the supervisory authority pursuant to Section 53 of Regulation (EU) 2016/679 of the European Parliament and of the Council. President of the Office may permanently entrust some of his or her tasks to the Vice-president of the Office. President of the Office shall be deemed to be a service body pursuant to the Civil Service Act and shall be authorised to instruct civil servants on the performance of the civil service.

(2) The term of office of the President of the Office shall be 5 years. President of the Office may be appointed for 2 consecutive terms at maximum.

(3) President of the Office may only be appointed from among Czech citizens who

(a) enjoy full legal capacity;

(b) have reached at least 40 years of age;

(c) have clear criminal record, comply with the conditions laid down by other legal regulations[7]) and their knowledge, experience and morals indicate that they will discharge the office properly; and

(d) have obtained university education by completing a Master's programme with specialisation in law or informatics, are sufficiently fluent in English, German or French and have at least 5 years of experience in the area of protection of personal data or human rights and basic freedoms; education in other fields is permissible for candidates with over 10 years of experience

in the above areas.

(4) For the purposes of this Act, clear criminal record shall mean lack of valid conviction of a criminal offence related to personal data processing committed intentionally or by negligence.

(5) The discharge of office of the President of the Office is incompatible with the discharge of the office of member of the Chamber of Deputies or Senate, judge, public prosecutor or any public administration office or a membership in a political party or a political movement.

(6) President of the Office may not discharge another paid office, be in another employment relationship or perform gainful activities except for management of his or her own property and scientific, educational, literary, journalistic or artistic activities, unless such activities impair the dignity of the Office or endanger the trust in its independence and impartiality.

(7) President of the Office may be removed if he or she no longer complies with any of the conditions for appointment.

Section 53

(1) The Office shall have two Vice-presidents, who shall be elected and removed by the Senate at the proposal of the President of the Office. Vice-president of the Office shall be a section director. Vice-president of the Office shall be deemed to be a member of the supervisory authority pursuant to Section 53 of Regulation (EU) 2016/679 of the European Parliament and of the Council.

(2) Vice-president of the Office shall represent the President of the Office in his or her absence; the order of precedence in representing the President shall be based on the order in which the Vice-presidents of the Office were elected, including any immediately preceding term of office.

(3) Section 52 (2) to (7) shall apply *mutatis mutandis*.

Section 54
Activities of the Office

(1) In relation to personal data processing pursuant to Title II, the Office

(a) shall perform audits pursuant to Art. 58 (1)(b) of Regulation (EU) 2016/679 of the European Parliament and of the Council in compliance with the inspection rules;

(b) may invite the controller to explain or remedy the state of affairs in procedure pursuant to Art. 58 (1)(d) of Regulation (EU) 2016/679 of the European Parliament and of the Council;

(c) shall notify the controller or processor that the intended personal data processing would probably result in breach of their obligations;

(d) may determine the criteria or requirements pursuant to Art. 41 (3), Art. 42 (5) or Art. 43 (1)(b) of Regulation (EU) 2016/679 of the European Parliament and of the Council by means of a Decree;

(e) may order a certification body to withdraw certification issued by the body pursuant to Art. 42 and 43 of Regulation (EU) 2016/679 of the European Parliament and of the Council;

(f) shall approve codes of conduct; if a code of conduct is at variance with Regulation (EU) 2016/679 of the European Parliament and of the Council, the Office shall refuse to approve it; and

(g) shall publish standard contractual clauses adopted pursuant to Art. 28 (8) or Art. 46 (2)(d) of Regulation (EU) 2016/679 of the European Parliament and of the Council in a manner enabling remote access.

(2) In relation to personal data processing pursuant to Title III other than personal data processing carried out by courts and public prosecutors' offices, the Office shall

(a) supervise compliance with obligations laid down by law in personal data processing;

(b) verify the lawfulness of personal data processing at instigation of data subject pursuant to

Section 31;
(c) accept instigations and complaints regarding a breach of obligations laid down by law in personal data processing and provide information on the manner in which they were addressed;
(d) hear infractions and impose fines;
(e) provide consultations in the field of personal data protection;
(f) inform the public of the risks, rules, safeguards and rights in relation to personal data processing;
(g) inform controllers and processors of their obligations in the area of personal data protection and
(h) exercise other competences entrusted to the Office by this Act.
(3) Furthermore, the Office shall
(a) prepare and make available to the public annual reports on its activities;
(b) provide for the fulfilment of requirements following from international treaties binding on the Czech Republic and from directly applicable regulations of the European Union;
(c) even without a request provide the Parliament with opinions on draft regulations governing personal data processing;
(d) participate in the activities of the European Data Protection Board; co-operate with similar authorities in other countries, with institutions of the European Union and with bodies of international organisations operating in the area of personal data protection;
(4) The supervision over personal data processing carried out by courts or public prosecutors' offices under Title III of this Act or by intelligence services, shall be governed by another legal regulation[8]).

Section 55
Use of Information from Public Administration Information Systems

(1) In exercising its competence pursuant to this Act or another legal regulation, the Office shall use the following data from the basic population register
(a) surname(s);
(b) name(s);
(c) address of residence and
(d) date of birth.
(2) In exercising its competence pursuant to this Act or another legal regulation, the Office shall use the following data from the information system of population records
(a) name(s); surname(s); surname at birth, if applicable;
(b) date of birth;
(c) address of permanent residence, including former addresses of permanent residence;
(d) date of commencement of permanent residence or date of cancellation of permanent residence or date of termination of permanent residence in the territory of the Czech Republic; and
(e) birth identification number.
(3) In exercising its competence pursuant to this Act or another legal regulation, the Office shall use the following data from the information system for foreign nationals
(a) name(s); surname(s); surname at birth, if applicable;
(b) date of birth;
(c) type of residence and address of residence;
(d) number and date of expiry of residence permit and
(e) date of commencement of residence; date of termination of residence, if applicable.

(4) Data kept as reference data in the basic population register shall be taken from the information system for population records or the information system for foreign nationals only if they are in a form preceding the current state.

(5) In each specific case, only the data necessary for carrying out a given task may be taken from the accessible records.

Section 56
International Co-operation

(1) In the area of personal data protection under Title III, the Office shall provide assistance, including investigation, checks and provision of information, to supervisory authorities of other Member States of the European Union and states that apply regulations transposing Directive (EU) 2016/680 of the European Parliament and of the Council.

(2) The Office shall respond to requests from supervisory authorities of other Member States of the European Union or states that apply regulations transposing Directive (EU) 2016/680 of the European Parliament and of the Council under paragraph 1 above without undue delay, but not later than 1 month of the receipt of the request, unless the Office is not authorised to provide assistance or this would lead to violation of the law.

(3) The Office shall inform the requesting supervisory authority of the manner in which the request was addressed pursuant to paragraph 2 above or of reasons for not addressing the request.

(4) Assistance pursuant to paragraph 1 above shall be provided at the expense of the Office; should addressing a request require unreasonable expenses, the Office shall postpone addressing of the request until an agreement is reached with the requesting supervisory authority on the manner of paying the expenses.

(5) If addressing a request of the Office abroad would require unreasonable expenses, the request may be addressed at the expense of the Office, with its consent.

Section 57
Annual Report

(1) The Office's annual report shall comprise, in particular, information on its supervisory activities and their evaluation, information and evaluation of the situation in the area of personal data processing and protection in the Czech Republic, and evaluation of other activities of the Office, including supervision over processing under Title II of this Act.

(2) The President of the Office shall submit the annual report to the Parliament and the Government within 3 months of the end of the budgetary year.

Section 58
Authorisation of the Office to Access Information

(1) The Office may become acquainted with all information necessary for the fulfilment of a specific task. This also applies to information subject to a confidentiality obligation under another legal regulation unless another legal regulation[9]) lays down other conditions for access to such data by the Office.

(2) The Office may become acquainted with information subject to a confidentiality obligation under the Legal Profession Act only in the presence and with the consent of a representative of the Czech Bar Association (hereinafter the "Bar") appointed by the President of the Bar from among its employees or attorneys. Should the representative of the Bar refuse the consent, he or she shall, at written request of the Office, ensure confidentiality and integrity of the data pursuant to the first sentence and submit without delay to the Bar's Supervisory Council the Office's written request for replacement of the consent of the Bar's representative by a decision of the Bar's Supervisory Council. If the Bar's Supervisory Council does not decide to replace the consent of

the Bar's representative based on the Office's request within 30 days of delivery of the request by the Bar's representative, the consent of the Bar's representative may be replaced by a court decision pursuant to the Special Court Proceedings Act at the Office's request.

(3) The Office may become acquainted with information subject to a confidentiality obligation pursuant to the Tax Consultancy Act and the Chamber of Tax Advisors of the Czech Republic only in the presence and with the consent of a representative of the Chamber of Tax Advisors of the Czech Republic appointed by the President of the Chamber of Tax Advisors of the Czech Republic from among its employees or tax advisors. Should the representative of the Chamber of Tax Advisors of the Czech Republic refuse the consent, he or she shall, at written request of the Office, ensure confidentiality and integrity of the data pursuant to the first sentence and submit without delay to the Supervisory Committee of the Chamber of Tax Advisors of the Czech Republic the Office's written request for replacement of the consent of the representative of the Chamber of Tax Advisors of the Czech Republic by a decision of the Supervisory Committee of the Chamber of Tax Advisors of the Czech Republic. If the Supervisory Committee of the Chamber of Tax Advisors of the Czech Republic does not decide to replace the consent of the representative of the Chamber of Tax Advisors of the Czech Republic based on the Office's request within 30 days of delivery of the request by the representative of the Chamber of Tax Advisors of the Czech Republic, the consent of the representative of the Chamber of Tax Advisors of the Czech Republic may be replaced by a court decision pursuant to the Special Court Proceedings Act at the Office's request.

(4) If the Office enables a person other than the person from which the relevant information has been obtained to inspect files, it shall exclude from inspection of files information that constitutes business secrets, banking secrets or other secrets protected by similar laws, information protected by copyright and information pursuant to the second sentence of paragraph 1 or paragraph 2 above. In proceedings on imposing of an obligation, the Office shall make available to the party to the proceedings information excluded under the first sentence, if it has served or will serve as evidence. Prior to disclosing the information, the party to the proceedings or its representative must be advised on the manner in which the information is protected; a record shall be drawn up on the advice. The authorisation to access such information shall not include authorisation to make excerpts from or copies of the information.

(5) Paragraph 1 above shall in no way prejudice the obligation of the relevant inspector to prove his or her authorisation to access classified information.

Section 59
Confidentiality Obligation of Employees of the Office

(1) The Vice-president and employees of the Office are obliged to maintain confidentiality of personal data, in particular information pursuant to Section 58 (4), as well as organisational and technical measures the publication of which would endanger the security of the personal data that they learned in the discharge of the competences of the Office or in connection therewith. This obligation shall survive termination of service or employment relationship.

(2) The confidentiality obligation pursuant to paragraph 1 above may not be invoked *vis-à-vis* the Office. The confidentiality obligation pursuant to paragraph 1 above may be invoked *vis-à-vis* prosecuting bodies or courts only if the confidentiality obligation could be invoked *vis-à-vis* a prosecuting body or a court by the person on whom the confidentiality obligation was imposed by law and from whom the information subject to the confidentiality obligation was obtained. Personal data may only be disclosed to a data subject if such disclosure does not endanger a protected interest provided for in Section 6 (2).

(3) The Vice-president and employees of the Office may be relieved from confidentiality obligation by the President of the Office or a person authorised by the President.

Section 60
Measures to Remedy Shortcomings

In the event of breach of an obligation laid down by the Act or imposed on its basis in personal data processing under Title II or III or under Regulation (EU) 2016/679 of the European Parliament and of the Council, the Office may impose a measure to remedy the determined shortcomings and set a reasonable deadline for remedy.

TITLE VI
INFRACTIONS
Section 61

(1) A natural person, legal person or natural person operating a business commits an infraction by breaching the ban on disclosure of personal data imposed by another legal regulation[10]).

(2) Infraction pursuant to paragraph 1 above may be subject to a fine of up to

(a) CZK 1,000,000; or

(b) CZK 5,000,000 if the infraction is committed through press, film, radio, television, publicly accessible computer network or in some other similarly effective manner.

(3) The Office shall waive administrative punishment also with respect to entities set out in Art. 83 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

Section 62

(1) The controller or processor pursuant to Title II commits an infraction by

(a) breaching either of the obligations pursuant to Art. 8, 11, 25 to 39, 42 to 49 of Regulation (EU) 2016/679 of the European Parliament and of the Council or Title II;

(b) breaching either of the basic principles of personal data processing pursuant to Art. 5 to 7 or 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council;

(c) breaching either of the rights of data subjects pursuant to Art. 12 to 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council or Title II;

(d) failing to comply with an order or limitation on personal data processing or the suspension of data flows imposed by the Office pursuant to Art. 58 (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council; or

(e) failing to provide to the Office access to data, information and premises pursuant to Art. 58 (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

(2) A certification body commits an infraction by breaching either of the obligations pursuant to Art. 42 and 43 of Regulation (EU) 2016/679 of the European Parliament and of the Council or Title II.

(3) Body monitoring compliance commits an infraction by breaching either of the obligations pursuant to Art. 41 (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

(4) The Office may waive administrative punishment also if it imposes measures pursuant to Section 54 (1)(e) or Section 60.

(5) The Office shall waive administrative punishment also with respect to controllers and processors set out in Art. 83 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

Section 63

(1) Legal person commits an infraction during processing of personal data by

(a) failing to determine the purpose of personal data processing at variance with Section 25

(1)(a) or if the determined purpose of personal data processing is in breach of an obligation or in excess of authorisation following from another law;

(b) failing to implement measures ensuring that personal data are accurate in relation to the nature and purpose of their processing at variance with Section 25 (1)(b);

(c) keeping personal data longer than for the period necessary for achieving the purpose of their processing at variance with Section 25 (1)(a);

(d) failing to provide to data subjects information within the scope or in the manner laid down by the Act at variance with Section 27;

(e) failing to comply with a request of a data subject provided for in Section 28 (1) at variance with Section 28 (2);

(f) failing to comply with a request of a data subject provided for in Section 29 (1) or (2) at variance with Section 29 (5);

(g) failing to take technical and organisational measures or to keep records thereof at variance with Section 32 (1) to (3);

(h) failing to keep written overviews of all typified activities of personal data processing at variance with Section 32 (4);

(i) failing to make logs at variance with Section 36 (1);

(j) using the logs for another purpose at variance with Section 36 (3);

(k) failing to perform data protection impact assessment at variance with Section 37;

(l) failing to consult with the Office the envisaged personal data processing at variance with Section 38 (1);

(m) interfering with the rights and legally protected interests of the data subject or causing the data subject to face some other similarly serious consequence at variance with Section 39;

(n) failing to take organisational and technical measures to ensure adequate level of personal data protection at variance with Section 40 (1);

(o) failing to take the necessary measures at variance with Section 40 (2);

(p) failing to notify the Office of a personal data breach at variance with Section 41 (1);

(q) failing to communicate personal data breach to the relevant data subject at variance with Section 42 (1);

(r) failing to perform the imposed remedial measures by the deadline set by the Office;

(s) failing to comply with limitation on processing of special categories of personal data under another legal regulation[5]);

(t) breaching the obligation to appoint the officer under another legal regulation[5]);

(u) failing to comply with the obligation to provide information on incorrect transfer or transfer of inaccurate personal data pursuant to Section 32 (5) or under another legal regulation[5]);

(v) breaching any condition laid down by another legal regulation[5]) for transfer of personal data to an international organisation or a state that does not apply regulations transposing Directive (EU) 2016/680 of the European Parliament and of the Council; or

(w) breaching the obligation to verify the necessity for further processing or erase personal data under another legal regulation[5]).

(2) A person commits an infraction during processing of personal data by

(a) failing to keep overviews of all typified activities of personal data processing at variance with Section 34 (4);

(b) failing to notify the controlling authority of personal data breach at variance with Section 34 (5);

(c) failing to process personal data only according to instructions of the controlling authority or

based on law at variance with Section 35;

(d) failing to make logs at variance with Section 36 (1);

(e) using the logs for another purpose at variance with Section 36 (3);

(f) failing to take organisational and technical measures to ensure adequate level of personal data protection at variance with Section 40 (1);

(g) failing to take the necessary measures at variance with Section 40 (2);

(h) failing to perform the imposed remedial measures by the deadline set by the Office;

(i) failing to comply with limitation on processing of special categories of personal data under another legal regulation[5]);

(j) breaching the obligation to appoint the officer under another legal regulation[5]);

(k) failing to comply with the obligation to provide information on incorrect transfer or transfer of inaccurate personal data pursuant to Section 32 (5) or under another legal regulation[5]);

(l) breaching any condition laid down by another legal regulation[5]) for transfer of personal data to an international organisation or a state that does not apply regulations transposing Directive (EU) 2016/680 of the European Parliament and of the Council; or

(m) breaching the obligation to verify the necessity for further processing or erase personal data under another legal regulation[5]).

(3) Infraction pursuant to paragraphs 1 and 2 may be subject to a fine of up to CZK 10,000,000.

Section 64

(1) Infractions under this Act shall be heard by the Office.

(2) Fines shall be collected by the Office.

Section 65
Special Provisions on Discontinuation of Proceedings

Without initiating proceedings concerning an infraction pursuant to this Act and breach of Regulation (EU) 2016/679 of the European Parliament and of the Council, the Office may also discontinue proceedings by its resolution if it is clear, given the significance and degree of violation of or danger to the protected interest affected, the manner of committing the act, its consequences, the circumstances under which the act was committed, and given the conduct of the accused after committing the offence, that the purpose of the proceedings on the infraction has been achieved or could be achieved in another manner. Resolution on discontinuation pursuant to the first sentence shall only be recorded in the file; in such a case, the provisions of the Act on Liability for Infractions and Proceedings Concerning Infractions pertaining to notices of discontinuation of proceedings shall not apply.

PART TWO

TRANSITORY, REPEALING AND FINAL PROVISIONS

Section 66

Transitory Provisions

(1) From the effective date of this Act until 31 December 2020, the Office shall only have 1 Vice-president. A second Vice-president of the Office may be elected with effect from 1 January 2021 at the earliest.

(2) The person who is the acting President of the Office as of the effective date of this Act shall complete his or her term of office pursuant to former legal regulations.

(3) The person who is the acting inspector of the Office as of the effective date of this Act shall complete his or her term of office pursuant to former legal regulations. From the effective date of this Act up until the end of his or her term of office, the Office's inspector shall be an employee of the Office authorised to carry out management and inspection activities under an employment

relationship concluded for a fixed term. The entitlement of the Office's inspector to salary, compensation of expenses and performances in kind shall be governed by the former legal regulations.

(4) Information processed prior to the effective date of this Act in the register of personal data processing pursuant to Act No. 101/2000 Coll., on protection of personal data and amendment to certain laws, shall be publicly accessible for a period of 18 months from the effective date of this Act.

(5) Proceedings initiated pursuant to Act No. 101/2000 Coll., which have not been closed by a final decision before the effective date of this Act shall be closed pursuant to Act No. 101/2000 Coll.

(6) From the effective date of this Act, the terms sensitive data or sensitive personal data used in the former legal regulations shall mean personal data, which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of unique identification of a natural person, data concerning health or data concerning sex life, sexual orientation, and data relating to criminal convictions and offences or related security measures.

(7) Consent granted by a data subject pursuant to Act No. 101/2000 Coll. shall be deemed consent pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council unless the manner of granting of the consent has been at variance with the Regulation.

Section 67

Repealing Provisions

The following are hereby repealed:

1. Act No. 101/2000 Coll., on the protection of personal data and amendment to certain laws.

2. Act No. 177/2001 Coll., amending Act No. 101/2000 Coll., on the protection of personal data and amendment to certain laws, as amended by Act No. 227/2000 Coll. and Act No. 65/1965 Coll., the Labour Code, as amended.

3. Part Six of Act No. 450/2001 Coll., amending Act No. 128/2000 Coll., on municipalities (the Municipal Order), as amended; Act No. 129/2000 Coll., on regions (the Regional Order), as amended; Act No. 131/2000 Coll., on the Capital City of Prague, as amended; Act No. 250/2000 Coll., on budgetary rules for territorial budgets, as amended by Act No. 320/2001 Coll.; Act No. 218/2000 Coll., on budgetary rules and amendment to certain related laws (the Budgetary Rules), as amended; and Act No. 101/2000 Coll., on the protection of personal data and amendment to certain laws, as amended.

4. Part Four of Act No. 107/2002 Coll., amending Act No. 140/1996 Coll., on access to the files of the former State Security, and certain other laws.

5. Part Two of Act No. 310/2002 Coll., amending Act No. 148/1998 Coll., on the protection of confidential facts and amendment to certain laws, as amended; Act No. 101/2000 Coll., on the protection of persona data and amendment to certain laws, as amended; Act No. 18/1997 Coll., on peaceful utilisation of nuclear energy and ionising radiation (the Atomic Act) and amending and supplementing certain laws, as amended; Act No. 38/1994 Coll., on foreign trade in military material and supplementing Act No. 455/1991 Coll., on business in trade (the Trade Act), as amended; and Act No. 140/1961 Coll., the Criminal Code, as amended; Act No. 283/1993 Coll., on Public Prosecutor's Office, as amended; and Act No. 42/1992, on arrangement of property relations and settlement of property claims in co-operatives, as amended.

6. Part Nine of Act No. 517/2002 Coll., implementing certain measures in the system of central governmental authorities and amending certain laws.
7. Part One of Act No. 439/2004 Coll., amending Act No. 101/2000 Coll., on the protection of personal data and amendment to certain laws, as amended.
8. Part Four of Act No. 480/2004 Coll., on certain services of the information society and amendment to certain laws (the Act on Certain Services of Information Society).
9. Part Six of Act No. 626/2004 Coll., on amendment to certain laws in connection with the implementation of a reform of public finances in terms of remuneration.
10. Part Forty of Act No. 413/2005 Coll., on amendment to laws with connection to adoption of the Act on Protection of Classified Information and Security Qualification.
11. Part Eleven of Act No. 109/2006 Coll., amending certain laws in connection with adoption of the Act on Social Services.
12. Part Twenty of Act No. 264/2006 Coll., amending certain laws in connection with adoption of the Labour Code.
13. Part Thirty-six of Act No. 342/2006 Coll., amending certain laws in connection with populations records and certain other laws.
14. Part Thirteen of Act No. 170/2007 Coll., amending certain laws in connection with Czech Republic joining the Schengen Area.
15. Part Sixty-five of Act No. 41/2009 Coll., amending certain laws in connection with adoption of the Criminal Code.
16. Part Three of Act No. 52/2009 Coll., amending Act No. 141/1961 Coll., on criminal court proceedings (the Criminal Code), as amended, and certain other laws.
17. Part Eighty-eight of Act No. 227/2009 Coll., amending certain laws in connection with adoption of the Act on Basic Registries.
18. Part Sixty-five of Act No. 281/2009 Coll., amending certain laws in connection with adoption of the Tax Code.
19. Part Forty-six of Act No. 375/2011 Coll., amending certain laws in connection with adoption of the Act on Healthcare Services, Act on Specific Healthcare Services and Act on Medical Emergency Service.
20. Part Four of Act No. 468/2011 Coll., amending Act No. 127/2005 Coll., on electronic communications and amendment to certain related laws (the Electronic Communications Act), as amended, and certain other laws.
21. Part Twenty-nine of Act No. 64/2014 Coll., amending certain laws in connection with adoption of the Inspection Rules.
22. Part Twenty-nine of Act No. 250/2014 Coll., on amendment to laws in connection with adoption of the Civil Service Act.
23. Part Six of Act No. 301/2016 Coll., amending certain laws in connection with adoption of the Central Bank Account Registry Act.
24. Part Eighty-two of Act No. 183/2017 Coll., amending certain laws in connection with adoption of the Act on Liability for Infractions and Proceedings Concerning Infractions and the Act on Certain Infractions.
25. Government Regulation No. 277/2011 Coll., on the form identity card for inspectors of the Office for Personal Data Protection.

Section 68

Effect

This Act enters into effect on the date of its publication.

Vondráček, signed
Zeman, signed
Babiš, signed

Footnotes

[1)] Directive (EU) 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.

[2)] 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).

[3)] Act No. 22/1997 Coll., on technical requirements for products and amendment and supplementation to certain laws, as amended.

[4)] Section 82 of Act No. 89/2012 Coll., the Civil Code, as amended.
Section 10 *et seq.* of Act No. 46/2000 Coll., on the rights and obligations in publishing of periodical press and amendment to certain other laws (the Press Act), as amended.
Section 35 *et seq.* of Act No. 231/2001 Coll., on operation of radio and television broadcasting and amendment to other laws, as amended.

[5)] E.g. Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended; Act No. 341/2011 Coll., on the General Inspectorate of Security Forces and amendment to related laws, as amended; Act No. 300/2013 Coll., on the Military Police and amendment to certain laws, as amended; Act No. 257/2000 Coll., on the Probation and Mediation Service and amendment to Act No. 2/1969 Coll., on establishment of ministries and other central governmental authorities of the Czech Republic, as amended; Act No. 269/1994 Coll., on the Criminal Records, as amended; Act No. 555/1992 Coll., on the Prison Service and judicial guard of the Czech Republic, as amended; Act No. 141/1961 Coll., on criminal court proceedings (the Criminal Code), as amended; Act No. 104/2013 Coll., on international judicial co-operation in criminal matters, as amended; and Act No. 17/2012 Coll., on the Customs Administration of the Czech Republic, as amended.

[6)] E.g. Act No. 153/1994 Coll., on the intelligence services of the Czech Republic, as amended; Act No. 154/1994 Coll., on the Security Intelligence Service of the Czech Republic, as amended; Act No. 219/1999 Coll., on armed forces of the Czech Republic, as amended; Act No. 221/1999 Coll., on professional soldiers, as amended; Act No. 222/1999 Coll., on defence of the Czech Republic, as amended; Act No. 240/2000 Coll., on crisis management and amendment to certain laws (the Crisis Act), as amended; Act No. 241/2000 Coll., on economic measures in emergency situations and amendment to certain related laws, as amended; Act No. 585/2004 Coll., on conscription and its ensuring (the Military Service Act), as amended; Act No. 289/2005 Coll., on the Military Intelligence, as amended; Act No. 412/2005 Coll., on protection of classified information and security qualification, as amended; Act No. 320/2015 Coll., on the Fire Rescue Service of the Czech Republic and amendment to certain laws (the Fire Rescue Service Act), as amended; and Act No. 45/2016 Coll., on the service of military reservists, as amended.

[7)] Act No. 451/1991 Coll., laying down some other requirements for discharge of certain offices in governmental authorities and organisations of the Czech and Slovak Federative Republic, the Czech Republic and the Slovak Republic, as amended.

[8)] E.g. Act No. 6/2002 Coll., on courts and judges, as amended; Act No. 283/1993 Coll., on Public Prosecutor's Office, as amended; Act No. 153/1994 Coll., on the intelligence services of the Czech Republic, as amended.

[9)] E.g. Section 16 of Act No. 89/1995 Coll., on the State statistical service, as amended.

[10)] E.g. Section 8a, Section 8b (1) to (4) and Section 8c of Act No. 141/1961 Coll., Section 52 to 54 of Act No. 218/2003 Coll., on juvenile justice, as amended.