*Unofficial translation*

# 30 JULY 2018 - Act on the protection of natural persons with regard to the processing of personal data

(Belgian Official Journal - 05 September 2018) - Consolidated version (05/09/2018)

## PRELIMINARY TITLE. - Introductory provisions

**Art. 1.** This Act regulates the matter referred to in article 74 of the Constitution.

**Art. 2.** This Act applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

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, hereinafter "the Regulation" also applies to the processing of personal data referred to in articles 2.2.a) and 2.2.b) of the Regulation.

**Art. 3.** The free movement of personal data is neither restricted nor prohibited for reasons related to the protection of natural persons with regard to the processing of personal data.

In particular, the exchange of personal data between controllers, the competent authorities, administrations, bodies and recipients as referred to in Titles 1 to 3 of this Act and acting in the context of the purposes referred to in article 23.1.a) to h) of the Regulation cannot be restricted or prohibited for such reasons.

However, a restriction or prohibition may be imposed in cases where there is a high risk that the exchange of the data may lead to a circumvention of this Act.

**Art. 4.** § 1. This Act shall apply to the processing of personal data in the context of the activities of an establishment of a controller or processor established on Belgian territory, whether or not the processing is performed on Belgian territory.

§ 2. This Act shall apply to the processing of personal data of data subjects who are on Belgian territory, by a controller or processor not established in the European Union, where the processing activities are related to:

1° the offering of goods or services to such data subjects on Belgian territory, irrespective of whether a payment of the data subject is required; or

2° the monitoring of their behaviour as far as their behaviour takes place on Belgian territory.

§ 3. By way of derogation from paragraph 1, when the controller is established in a Member State of the European Union and resorts to a processor established on the Belgian territory, the law of the Member State in question applies to the processor, provided that the processing activities take place on the territory of that Member State.

§ 4. This Act shall apply to the processing of personal data by a controller which is not established on Belgian territory, but in a place where Belgian law applies under public international law.

**Art. 5.** The definitions of the Regulation apply.

For the purposes of this Act "public authority" means:

1° the Federal State, the federated entities and the local authorities;

2° the legal persons under public law subordinate to the Federal State, the federated entities or the local authorities;

3° the persons, whatever their form or nature:

- established for the specific purpose of meeting needs of general interest, without any industrial or commercial character; and

- having legal personality; and

- either whose activities are mainly financed by the public authorities or bodies referred to in the provisions sub 1 or 2°, either whose management is subject to supervision of those authorities or bodies, or having an administrative, management or supervisory body of which more than half of the members are appointed by these authorities or bodies;

4° associations composed of one or more public authorities as referred to in the provisions sub 1°, 2° or 3°.

## TITLE 1. - The protection of natural persons with regard to the processing of personal data

### CHAPTER I. – General provision

**Art. 6.** Without prejudice to specific provisions, this title enforces the Regulation.

### CHAPTER II. - Principles relating to the processing

**Art. 7.** In implementation of article 8.1 of the Regulation, the processing of personal data related to children in relation to the offer of information society services directly to a child is lawful where the consent has been given by children who are at least 13 years old.

Where the processing concerns personal data of a child below the age of 13 years, such processing shall be lawful only if that consent is given by the child's legal representative.

**Art. 8.** § 1. In implementation of article 9.2.g) of the Regulation, the processing activities listed hereafter shall be regarded as necessary for reasons of substantial public interest:

1° the processing by associations with legal personality or foundations whose principal legal objective is to defend and promote human rights and fundamental freedoms, carried out to achieve that objective, provided that the processing in question was authorised by the King, by decree deliberated in the Council of Ministers, after advice of the competent supervisory authority. The King can lay down further terms for that processing;

2° the processing managed by the public utility foundation "Fondation pour Enfants Disparus et Sexuellement Exploités (Foundation for Missing and Sexually Exploited Children)" for the receipt, transmission to the judicial authorities and follow-up of data on persons suspected of having committed a criminal act or an offence in a particular file of missing persons or sexual exploitation;

3° the processing of personal data about the sexual life, carried out by associations with legal personality or foundations whose principal legal objective is to assess, supervise and treat persons whose sexual behaviour can be qualified as an offence and which, for the purpose of achieving that objective, are approved and subsidized by the competent authority. For processing activities such as these, which must be intended to assess, supervise and treat persons referred to in this paragraph and exclusively concern personal data which, as far as they relate to the sexual life, concern the persons referred to in this paragraph, a special individual authorisation must be granted by the King, by decree deliberated in the Council of Ministers, after advice of the competent supervisory authority.

The decree referred to in the first subparagraph, 3°, shall specify the validity period of the authorisation, the data processing methods , the methods of supervision of the association or foundation by the competent authority and the manner in which this authority reports to the competent supervisory authority on the processing of personal data in the context of the granted authorization.

Except specific legal provisions, the processing of genetic and biometric data by these associations and foundations, for the purpose of identifying a natural person in a unique manner, is prohibited.

§ 2. The controller and, where applicable, the processor, shall compile a list of the categories of persons who have access to the personal data, with a description of their capacity with respect to the processing of the data in question. This list shall be kept at the disposal of the competent supervisory authority.

The controller and, where applicable, the processor, shall ensure that the designated persons are bound by a legal or legal obligation, or by an equivalent contractual provision, to respect the confidential nature of the data concerned.

§ 3. The foundation referred to in paragraph 1, first subparagraph, 2°, can't keep any file on persons suspected of having committed a criminal act or an offence or on sentenced persons. It shall appoint a data protection officer.

**Art. 9.** In implementation of article 9.4 of the Regulation, any controller processing genetic data, biometric data or data concerning health, shall also take the following additional measures:

1° the controller or, as appropriate, the processor, shall designate the categories of persons who have access to the personal data, and shall meticulously describe their capacity with regard to the processing of the data concerned;

2° the controller or, as appropriate, the processor, shall keep the list of the as so designated categories of persons at the disposal of the competent supervisory authority;

3° the controller shall ensure that the designated persons are bound by a legal or legal obligation or by an equivalent contractual provision to respect the confidential nature of the data concerned.

**Art. 10.** § 1. In implementation of article 10 of the Regulation, the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out:

1° by natural persons or legal persons governed by private or public law as far as necessary for the management of their own disputes; or

2° by lawyers or other legal advisers in so far as relevant to the defence of their clients' interests; or

3° by other persons, if the processing is necessary for reasons of substantial public interest for the performance of general interest tasks assigned by or under a law, a decree, an ordinance or European Union law; or

4° for the requirements of scientific, historical or statistical research or for archiving purposes; or

5° in cases where the data subject has given his explicit consent in writing that the personal data in question can be processed for one or more specific purposes and if the processing is strictly limited to those purposes; or

6° if the processing relates to personal data the data subject clearly disclosed on his own initiative for one or more specific purposes and if the processing of these data is limited to those purposes.

§ 2. The controller and, where applicable, the processor, shall compile a list of the categories of persons who have access to the personal data, with a description of their capacity with respect to the processing of the data in question. This list shall be kept at the disposal of the competent supervisory authority.

The controller and, where applicable, the processor, shall ensure that the designated persons are bound by a legal or legal obligation, or by an equivalent contractual provision, to respect the confidential nature of the data concerned.

## SECTION III. - Restrictions of the rights of the data subject

**Art. 11.** § 1. Pursuant to article 23 of the Regulation, articles 12 to 22 and 34 of the Regulation, as well as the principle of transparency of the processing referred to in article 5 of the Regulation, do not apply to the processing of personal data directly or indirectly originating from the authorities referred to in Title 3, with respect to:

1° the authorities and persons referred to in articles 14, 16 and 19 of the organic Act of 30 November 1998 of the intelligence and security services to which these data are transferred by the authorities referred to in Title 3, whether directly or indirectly;

2° the authorities and persons referred to in article 2, first subparagraph, 2°, of the Threat Assessment Act of 10 July 2006 and in article 44/11/3ter, §§ 2 and 3, and article 44/11/3quater of the Act of 5 August 1992 on the Police Function, and which fall within the scope of application of Title 1, and to which these data were transferred.

§ 2. The controller referred to in this Title who is in possession of such data shall not disclose them to the data subject concerned unless:

1° it is compelled to do so by law in the context of litigation process; or

2° the authority referred to in Title 3 authorizes it to do so.

The controller or the competent authority shall not mention that it is in possession of data originating from the authorities referred to in Title 3.

§ 3. The restrictions referred to in paragraph 1 also apply to the log files of the processing activities carried out by an authority referred to in Title 3 in the databases of the controllers referred to in this Title to which the authorities have direct access.

§ 4. The controller referred to in this Title who processes data originating from the authorities referred to in Title 3, whether directly or indirectly, shall as a minimum meet the following requirements:

1° it shall take the appropriate technical or organisational measures to ensure that access to the data and the processing opportunities are limited to what the persons concerned need to perform their duties or to what is necessary for the operational requirements.

2° it shall take the appropriate technical or organisational measures to protect the personal data against accidental or unauthorised destruction, against accidental loss, alteration or against any other form of unauthorised processing of the personal data concerned.

Furthermore, the members of the controller's staff processing the data referred to in the first subparagraph shall also be bound by the duty of discretion.

§ 5. Where a request or complaint is submitted to the supervisory authority referred to in the Act of 3 December 2017 establishing the Data Protection Authority, and the controller invokes the application of this article, the supervisory authority shall first consult with the Standing Committee I to allow it to carry out the necessary verifications with the authority referred to in Title 3.

After receipt of the reply from the Standing Committee I, the Data Protection Authority shall merely notify the data subject of the results of its verification relating to the personal data that did not originate from the authorities referred to in Title 3, which the supervisory authority is legally compelled to disclose.

If the request or complaint only relates to personal data originating from an authority referred to in Title 3, the Data Protection Authority shall, after receipt of the reply from Standing Committee I, reply that the relevant verifications have been carried out.

**Art. 12.** Pursuant to article 23 of the Regulation, any controller who discloses personal data to an authority referred to in Subtitles 2 and 4 of Title 3 of this Act does not come within the scope of application of articles 14.1.e and 15.1.c of the Regulation or of article 20, § 1, 6° of this Act and is not entitled to notify the data subject of any such transfer.

**Art. 13.** Where an authority referred to in Subtitles 1 and 6 of Title 3 has direct access to a public or private sector database or can search directly in that database, its processing activities of personal data in that database shall be protected by technical, organisational and individual security measures to ensure that only the following actors can have access to the content of these processing activities for the purpose of carrying out their legal supervisory tasks:

1° the data protection officer of the controller of the database;

2° the data protection officer of the authority referred to in Subtitles 1 and 6 of Title 3;

3° the controller of the database or its authorized representative;

4° the controller of the authority referred to in Subtitles 1 and 6 of Title 3;

5° any other person specified in a protocol between the controllers in so far as such access is part of the legal supervisory tasks of the data protection officers and the controllers.

The security measures referred to in the first subparagraph are intended to safeguard the legal obligations about protection of sources, protection of the identity of their officers or the discretion of the investigations by the authorities referred to in Subtitles 1 and 6 of Title 3. They shall be made available to the competent supervisory authority.

These processing operations shall only be accessible for purposes other than those relating to said supervision, provided the concerned controllers set out these purposes in a protocol agreement within the purposes defined by or under a law.

The protocol agreement shall list the person or persons who need to have access to the log files in order to meet each purpose authorized under the third subparagraph.

The log files and the security measures referred to in the first subparagraph shall be made available to of the Standing Committee I.

The authority referred to in Title 3 can depart from the first subparagraph in cases where access to its processing activities in a database and to the log files is unlikely to be damaging to the interests referred to in the second subparagraph.

**Art. 14.** § 1. Pursuant to article 23 of the Regulation, the rights referred to in articles 12 to 22 and 34 of the Regulation and the principle of transparency of the processing referred to in article 5 of the Regulation do not apply to the processing of data originating, whether directly or indirectly, from the judicial authorities, the police services, the General Inspectorate of the Federal and Local Police, the Financial Intelligence Processing Unit, the General Administration of Customs and Excise Duties and the Passenger Information Unit as referred to in Title 2, with respect to:

1° the public authorities, within the meaning of article 5 of this Act, to which the data were transferred by or under a law, decree or ordinance;

2° other institutions and bodies to which the data were transferred by or by virtue of a law, decree or ordinance.

§ 2. Any controller referred to in this Title in possession of data as referred to in paragraph 1 shall not disclose these data to the data subject unless:

1° it is compelled to do so by law in the context of legal proceedings; or

2° the judicial authorities, the police services, the General Inspectorate of the Federal and Local Police, the Financial Intelligence Processing Unit, the General Administration of Customs and Excise Duties and the Passenger Information Unit as referred to in paragraph 1, authorize it to do so, each in respect of the data relevant to them.

The controller or the competent authority shall not mention that it is in possession of data originating from them.

§ 3. The restrictions referred to in paragraph 1 also apply to the log files of the processing operations by the judicial authorities, the police services, the General Inspectorate of the Federal and Local Police, the Financial Intelligence Processing Unit, the General Administration of Customs and Excise Duties and the Passenger Information Unit in the databases of the controllers referred to in this Title to which they have direct access.

These restrictions only apply to data that were initially processed for the purposes referred to in article 27 of this Act.

§ 4. The legal safeguards referred to in article 23.2 of the Regulation that the authorities, bodies or institutions must meet are determined by or under the law.

The authorities, bodies or institutions which process data originating from the judicial authorities, the police services, the General Inspectorate of the Federal and Local police, the Financial Intelligence Processing Unit, the General Administration of Customs and Excise Duties and the Passenger Information Unit, whether directly or indirectly, shall as a minimum meet the following requirements:

1° they shall take the appropriate technical or organisational measures to ensure that access to the data and the processing opportunities are limited to what the persons concerned need to perform their duties or to what is necessary for the operational requirements.

2° they shall take the appropriate technical or organisational measures to protect the personal data against accidental or unauthorised destruction, against accidental loss and alteration, and against any other form of unauthorised processing of the personal data concerned.

Furthermore, any members of staff of the public authorities, bodies or institutions processing the data referred to in § 1 shall also be bound by the duty of discretion.

§ 5. Any request relating to the exercise of the rights referred to in articles 12 to 22 of the Regulation and addressed to a public authority, body or institution referred to in § 1, 1° and 2°, shall be transmitted without undue delay to the Data Protection Authority referred to in the Act of 3 December 2017 establishing the Data Protection Authority.

Where the Data Protection Authority is approached by the data subject directly or by the controller invoking the application of this article, it shall carry out the necessary verifications with the relevant authorities, bodies or institutions.

Where the Data Protection Authority was approached by the data subject, it shall inform this data subject in accordance with the further terms laid down by law.

§ 6. Where the processing relates to data that were initially processed by the police services or the General Inspectorate of the Federal and Local Police, the Data Protection Authority directly approached by the data subject, or by the controller invoking the application of this article, shall contact the supervisory authority referred to in article 71 so that it carries out the necessary verifications with the competent authorities, bodies or institutions.

Where the Data Protection Authority was approached by the data subject, the Data Protection Authority shall, after receipt of the reply from the authority referred to in article 71, notify the data subject in accordance with the further terms laid down by law.

§ 7. Where the processing relates to data that were initially processed by the judicial authorities, the Data Protection Authority directly approached by the data subject, or by the controller invoking the application of this article, shall contact the competent supervisory authority for the judicial authorities so that it carries out the necessary verifications with the competent authorities, bodies or institutions, referred to in § 1, 1° and 2°.

Where the Data Protection Authority was approached by the data subject, the Data Protection Authority shall, after receipt of the reply from the competent supervisory authority for the

judicial authorities, notify the data subject in accordance with the further terms laid down by law.

**Art. 15.** Pursuant to article 23 of the Regulation, articles 12 to 22 and 34 of the Regulation, as well as the principle of transparency of the processing referred to in article 5 of the Regulation, shall not apply to the processing of personal data by the Passenger Information Unit as referred to in Chapter 7 of the Act of 25 December 2016 on the processing of passenger data.

Controllers shall not disclose the data referred to in the first subparagraph to the data subject unless compelled to do so by law in the context of legal proceedings.

On no account shall controllers notify the data subjects that they are in possession of data relating to them.

The restrictions referred to in the first subparagraph also apply to the log files of the processing operations by the Passenger Information Unit in the databases of the controllers referred to in this Title.

Where a request or complaint is submitted to the competent supervisory authority and the controller invokes the application of this article, the supervisory authority shall merely reply that the necessary verifications have been carried out.

**Art. 16.** Where the personal data are mentioned in a judgment or a judicial file, or are processed in the context of criminal investigations and proceedings, the rights referred to in articles 12 to 22 and 34 of the Regulation shall be exercised in accordance with the Judicial Code, the Code of Criminal Procedure, the special laws governing criminal procedure and their implementing decrees.

**Art. 17.** Pursuant to article 23 of the Regulation, controllers referred to in this Title, who provide personal data to a common database, are not allowed to notify the data subject of any such transfer.

By "Common database" is meant the joint exercise of the tasks exercised in the context of Title 1 and Titles 2 or 3 by several authorities, structured by means of automated processes and applied to personal data

## CHAPTER IV. - Controller and processor

### Section 1. - General provision

**Art. 18.** In implementation of article 43 of the Regulation, certification bodies shall be accredited by the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, in accordance with Standard EN-ISO/IEC 17065 and with the additional requirements established by the competent supervisory authority.

### Section 2. - Public sector

**Art. 19.** This Section is applicable to the police services within the meaning of article 2, 2°, of the Act of 7 December 1998 organising an integrated police service structured at two levels, which are regarded as one public authority.

**Art. 20.** § 1. Unless otherwise provided for in specific laws, the federal public authority shall, in implementation of article 6.2 of the Regulation, in cases where it transfers personal data to any other public authority or private body on the basis of article 6.1.c) and e) of the Regulation, formalize this transfer for each processing activity by means of a protocol negotiated between the initial controller and the recipient controller.

This protocol may in particular provide for:

1° the identification of the federal public authority that transfers the personal data and the identification of the recipient;

2° the identification of the controller within the public authority that transfers the data and within the recipient;

3° the contact details of the data protection officers within the public authority that transfers the data and those of the recipient;

4° the purposes for which the personal data are transferred;

5° the categories of personal data transferred, including their format;

6° the categories of recipients;

7° the legal basis for the data transfer;

8° the methods for the communication used;

9° any specific measure that provides a framework to the transfer in accordance with the principle of proportionality and the data protection requirements by design and by default;

10° the applicable legal restrictions relating to the rights of the data subject;

11° the specific rules on the exercise of the rights of the data subject with the recipient;

12° the periodicity of the data transfer;

13° the duration of the protocol;

14° the penalties for infringements of the protocol without prejudice to Title 6.

§ 2. The protocol shall be concluded after receipt of the respective opinions of the data protection officer of the federal public authority, in possession of the personal data, and of the recipient. These opinions shall be appended to the protocol. Where the controllers disregard at least one of these opinions, the protocol shall mention in its introductory provisions the reason or reasons why the opinion or opinions has/have been disregarded.

§ 3. The protocol shall be published on the website of the controllers concerned.

**Art. 21.** In implementation of article 37.4 of the Regulation, any private body processing personal data for the account of a federal public authority, or to which a federal public authority has transferred personal data, shall appoint a data protection officer if the processing of these data is likely to result in a high risk as referred to in article 35 of the Regulation.

**Art. 22.** Where the processing of personal data is likely to result in a high risk as referred to in article 35 of the Regulation, the federal public authority shall consult the data protection officer prior to the processing.

If the federal public authority continues the implementation of the processing against the opinion and the recommendations of the data protection officer, it shall give reasons for its decision.

The statement of reasons shall specify why the opinion or recommendations have been disregarded.

**Art. 23.** In implementation of article 35.10 of the Regulation, a specific data protection impact assessment shall be carried out prior to the processing operation even if a general data protection impact assessment has already been carried out in the context of the adoption of the legal basis.

## CHAPTER V. - Processing for journalistic purposes and the purposes of academic, artistic or literary expression

**Art. 24.** § 1. By "processing of personal data for journalistic purposes" is meant the preparation, collection, drafting, production, dissemination or archiving with a view to informing the public, via any medium, and where the controller imposes on itself rules of journalistic deontology.

§ 2. Articles 7 to 10, 11.2, 13 to 16, 18 to 20 and 21.1 of the Regulation do not apply to the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.

§ 3. Articles 30.4, 31, 33 and 36 of the Regulation do not apply to the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression if their application would compromise a planned publication or would constitute a control measure prior to the publication of an article.

§ 4. Articles 44 to 50 of the Regulation do not apply to the transfers of personal data carried out for journalistic purposes or the purposes of academic, artistic or literary expression to third countries or international organisations in so far as necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information.

§ 5. Article 58 of the Regulation does not apply to the processing of personal data for journalistic purposes or the purposes of academic, artistic or literary expression if its application would provide indications as to the information sources or would constitute a control measure prior to the publication of an article.

# TITLE 2. - 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, including the safeguarding against and the prevention of threats to public security

## CHAPTER I. – General provisions

**Art. 25.** This Title provides for the transposition of 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.

**Art. 26.** For the purposes of this Title:

1° "personal data" means any information relating to an identified or identifiable natural person (hereinafter referred to as "the data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2° "processing" means 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;

3° "restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

4° "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to 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;

5° "pseudonymisation" means 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;

6° "filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

7° "competent authorities" means

a) the police services within the meaning of article 2, 2° of the Act of 7 December 1998 organising an integrated police service structured at two levels;

b) the judicial authorities, meaning the common law courts and the Public Prosecutor's Office;

c) the Investigation Department of the Standing Police Monitoring Committee in the context of its judicial mandates as referred to in article 16, 3rd paragraph of the Organic Law of 18 July 1991 governing the review of the police and intelligence services and of the Coordination Unit for Threat Assessment;

d) the General Inspectorate of the Federal and Local Police referred to in article 2 of the Act of 15 May 2007 on the General Inspectorate and laying down various provisions on the legal status of some members of the police services;

e) the General Administration of Customs and Excise Duties, in the context of its mandate to detect, establish and prosecute offences as defined in the Belgian General Customs and

Excise Act of 18 July 1977, and in the Act of 22 April 2003 conferring the status of judicial police officer on certain officers of the administration of customs and excise duties;

f) the Passenger Information Unit referred to in Chapter 7 of the Act of 25 December 2016 on the processing of passenger data;

g) the Financial Intelligence Processing Unit referred to in article 76 of the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and the restriction on the use of cash;

h) the Investigation Department of the General Inspectorate of the Standing Intelligence Agencies in the context of its judicial mandates as referred to in article 40, 3rd paragraph of the Act of 18 July 1991 governing the review of the police and intelligence services and of the Coordination Unit for Threat Assessment;

8° "controller" means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by law, decree or ordinance, the controller is the entity nominated by or by virtue of the law, decree or ordinance;

9° "processor" means a natural or legal person, a public authority, an agency or other body which processes personal data on behalf of the controller or another processor;

10° "recipient" means a natural or legal person, a public authority, an agency or other body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry pursuant to the law, decree or ordinance shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

11° "security breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

12° "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

13° "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

14° "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

15° "supervisory authority" means an independent public authority set up by law and responsible for monitoring the application of this Title;

16° "international organisation" means 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;

17° "international agreement" means any bilateral or multilateral international agreement in force between Member States of the European Union and third countries relating to judicial cooperation and/or police cooperation.

**Art. 27.** This Title applies to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

**CHAPTER II. - Principles relating to processing**

**Art. 28.** Personal data shall be:

1° processed lawfully and fairly;

2° collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3° adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4° accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

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

6° processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Art. 29.** § 1. Further processing by the same or another controller for a purpose listed in article 27, other than the purpose for which the personal data were collected, is permitted insofar as:

1° the controller is authorised by law, decree, ordinance, European law or international agreement to process these personal data for such purpose; and

2° the processing is necessary and proportionate by law, decree, ordinance, European law or international agreement.

§ 2. Personal data cannot be further processed by the same or another controller for a purpose other than the one the personal data were originally collected for if that purpose cannot be qualified as one of the purposes listed in article 27, unless that further processing is authorised by law, decree, ordinance, European law or international agreement.

§ 3. Where the processing is subject to specific conditions laid down by law, decree, ordinance, European law or international agreement, the transmitting competent authority shall inform the recipient of such personal data of those conditions and the requirement to respect them.

§ 4. The competent authorities transmitting data to recipients in the other Member States of the European Union are not entitled to impose any specific conditions additional to those applicable to national data transfers.

§ 5. The controller shall be responsible for and be able to demonstrate compliance with this article.

**Art. 30.** Except where the maximum storage period is laid down by European law or international agreement which forms the basis for the concerned storage, the maximum storage period shall be specified by law, decree or ordinance. After that period the data shall be erased.

By derogation from the first paragraph, the law, decree or ordinance can provide that, on expiry of a first storage period, an analysis must be performed on the basis of the various necessity and proportionality criteria to establish whether the data need to be retained and, where appropriate, define the new storage period.

In that case, the maximum storage period shall be laid down by law, decree or ordinance.

**Art. 31.** Where appropriate and insofar as possible, the controller shall clearly differentiate between the various categories of data subjects, such as:

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

2° persons who have been convicted of a criminal offence;

3° victims of a criminal offence, or persons in respect of whom certain facts give cause for suspicion that they could become the victim of a criminal offence;

4° third parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or persons who can provide information on criminal offences, or contacts or associates of one of the persons mentioned sub 1° and 2°.

**Art. 32.** § 1. Insofar as possible, fact-based personal data shall be differentiated from personal data based on personal judgment.

§ 2. The competent authorities shall take all reasonable measures to ensure that any personal data that are incorrect, incomplete or no longer up to date are not transmitted or made available. To do so, each competent authority shall, insofar as possible, check the quality of the personal data before the data are transmitted or made available.

Insofar as possible, personal data shall at all times be transmitted together with the relevant additional information on the basis of which the receiving competent authority can assess the accuracy, completeness and reliability of the personal data, including the extent to which they are current.

§ 3. If it turns out that incorrect personal data were transmitted or personal data were transmitted unlawfully, the recipient shall be notified without delay. In that case the personal data shall be corrected or erased, or their processing restricted in accordance with article 39.

**Art. 33.** § 1. The processing is lawful if:

1° it is necessary for the performance of a contract executed by a competent authority for the purposes referred to in article 27; and

2° it is based on a legal or regulatory obligation.

§ 2. The legal or regulatory obligation shall as a minimum regulate the categories of personal data that must be processed and the purposes of that processing.

**Art. 34.** § 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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 is permitted only if the processing is strictly necessary and is carried out subject to appropriate guarantees for the rights and freedoms of data subjects, and only in the following cases:

1° if the processing is authorised by law, decree, ordinance, European law or international agreement;

2° if the processing is necessary in order to protect the vital interests of the data subject or of another natural person;

3° if the processing relates to personal data manifestly made public by the data subject.

§ 2. Appropriate safeguards as referred to in paragraph 1 shall as a minimum entail that the competent authority or the controller compiles a list of the categories of persons who have access to the personal data, with a description of their capacity with respect to the processing of the data in question. This list shall be kept at the disposal of the competent supervisory authority.

The competent authority shall ensure that the designated persons are bound by a legal or legal obligation, or an equivalent contractual provision, to observe the confidential nature of the data concerned.

**Art. 35.** Decisions solely based on automated processing, including profiling, which have adverse legal consequences for data subjects or may significantly affect them are permitted if the law, the decree, the ordinance, the EU legislation or the international agreement provides for appropriate safeguards for the rights and freedoms of the data subject, including at least the right to human intervention on the part of the controller.

Profiling leading to discrimination between natural persons on the basis of the categories of personal data referred to in article 34 is prohibited.

## CHAPTER III. - Rights of the data subject

**Art. 36.** § 1. The controller shall take appropriate measures to provide any information referred to in article 37 and any communications referred to in articles 35, 38 to 41 and article 62 in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, by electronic means included. As a general rule, the controller shall provide the information in the same form as the request.

§ 2. The controller shall facilitate the exercise of the data subject’s rights by virtue of articles 35 and 38 to 41.

§ 3. The controller or the supervisory authority, in the case referred to in article 41, shall inform the data subject in writing, without undue delay, about the follow up to his request.

§ 4. Anyone is entitled to obtain the information referred to in article 37 free of charge and to request that the measures under articles 35, 38 to 41 and 62 are taken. Where requests

from a data subject are manifestly unfounded or excessive, in particular because of their repetitive nature, the controller may either:

1° charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

2° refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

§ 5. Where the controller has reasonable doubts about the identity of the natural person making the request referred to in article 38 or 39, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

**Art. 37.** § 1. To allow the data subject to exercise his right to information, the controller shall provide the data subject with the following information:

1° the identity and the contact details of the controller;

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

3° the purposes of the processing;

4° the existence of the right to lodge a complaint with the supervisory authority, and the contact details of the aforementioned authority;

5° the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject;

6° the legal basis for the processing;

7° the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

8° where applicable, the categories of recipients of the personal data;

9° where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

§ 2. The information referred to in paragraph 1 can be delayed, restricted or omitted by law, provided this constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

1° avoid obstructing inquiries, investigations, criminal procedures or other regulated procedures;

2° avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties;

3° protect public security;

4° protect national security;

5° protect the rights and freedoms of others.

§ 3. Except where provided under European legislation or the international agreement, the law, the decree or the ordinance can specify which processing categories can qualify as one of the points listed in paragraph 2, whether in full or in part.

§ 4. As far as the processing operations by the common law courts and the Public Prosecutor's Office are concerned, the rights under this Chapter shall exclusively be exercised within the limits and in accordance with the rules and detailed rules of the Judicial Code, the Code of Criminal Procedure, the specific laws governing criminal justice and their implementing decrees.

**Art. 38.** § 1. To offer the data subject the opportunity to exercise his right to access to the personal data relating to him, the controller shall provide the data subject with the following information:

1° confirmation as to whether or not the personal data relating to him are processed and access to those data;

2° the purposes of and legal basis for the processing;

3° the categories of personal data concerned;

4° the recipients or categories of recipients to whom the personal data have been disclosed;

5° the storage period, or if that is not possible, the criteria used to determine that period;

6° the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

7° the right to lodge a complaint with the supervisory authority, and the contact details of that authority;

8° the personal data undergoing processing and any available information as to their origin.

§ 2. The right of access of the data subject can be restricted in whole or in part by law, decree or ordinance insofar and as long as this complete or partial restriction constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of the natural person concerned, to:

1° avoid obstructing inquiries, investigations, criminal procedures or other regulated procedures;

2° avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties;

3° protect public security;

4° protect national security;

5° protect the rights and freedoms of others.

§ 3. In the cases referred to in paragraph 2, the controller is obliged to notify the data subject in writing and without undue delay that access has been refused or restricted and list the reasons for that refusal or restriction. The information can be omitted if there is a risk that its provision might undermine one of the purposes under paragraph 2. The controller shall notify the data subject of the option to lodge a complaint with the competent supervisory authority or to seek judicial redress.

§ 4. The controller shall document the factual or legal reasons for its decision. That information shall be put at the disposal of the competent supervisory authority.

**Art. 39.** § 1. The data subject shall have the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him or, as appropriate, to have the data concerning him completed.

§ 2. The controller shall erase the personal data without undue delay in cases where the processing is inconsistent with the provisions approved under articles 28, 29, 33 or 34 or where the personal data must be erased to comply with a legal obligation the controller is bound by.

§ 3. Instead of erasing the personal data, the controller may restrict their processing in cases where:

1° the accuracy of the personal data is disputed by the data subject and there is no way of establishing whether or not the data are accurate; or

2° the personal data must be stored as evidence.

When the processing is restricted on the basis of the first paragraph, 1°, the controller shall notify the data subject before lifting the processing restriction.

§ 4. The controller shall notify the data subject in writing where the request for rectification, erasure or restriction of processing of the personal data has been refused and communicate the reasons for that refusal. The information can be restricted by law, decree or ordinance insofar as, in a democratic society, such restriction of processing constitutes a necessary and proportionate measure, with due regard for the fundamental rights and legitimate interests of the data subject concerned, to:

1° avoid obstructing inquiries, investigations, criminal procedures or other regulated procedures;

2° avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties;

3° protect public security;

4° protect national security;

5° protect the rights and freedoms of others.

The controller shall notify the data subject of the option to lodge a complaint with the competent supervisory authority or to seek judicial redress.

§ 5. The controller shall communicate the rectification of the incorrect personal data to the authority that transferred the incorrect personal data.

§ 6. In the event of rectification, erasure or restriction of processing as referred to in paragraphs 1 to 3, the controller shall notify the recipients whereupon the recipients shall rectify or erase the personal data or restrict the processing of personal data within their competence.

**Art. 40.** The controller who receives a request to exercise a right referred to in articles 36 to 39 shall supply the applicant with a dated acknowledgement of receipt without delay and in any event within one month of receipt of the request.

**Art. 41.** In the cases referred to in articles 37, § 2, 38, § 2, 39, § 4, and 62, § 1, the law, the decree or the ordinance can stipulate that the rights of the data subject shall be exercised by the competent supervisory authority, with due regard for the principles of necessity and proportionality in a democratic society.

Without prejudice to article 44, in the case referred to in the first paragraph, the controller shall inform the data subject that he should exercise his rights via the competent supervisory authority.

In the case referred to in the first paragraph, the data subject shall lodge his request to exercise his rights with the competent supervisory authority.

**Art. 42.** The request to exercise the rights referred to in this Chapter in respect of the police service within the meaning of article 2, 2° of the Act of 7 December 1998 organising an integrated police service structured at two levels or the General Inspectorate of the Federal and Local Police, shall be addressed to the supervisory authority referred to in article 71.

In the cases referred to in articles 37, § 2, 38, § 2, 39, § 4, and 62, § 1, the supervisory authority referred to in article 71 shall exclusively inform the data subject that the necessary verifications were performed.

Notwithstanding the second paragraph, the supervisory authority referred to in article 71 may furnish the data subject with certain contextual information.

The King, on the advice of the supervisory authority referred to in article 71, defines the categories of contextual information the supervisory authority in question can communicate to the data subject.

**Art. 43.** As regards the processing of personal data by the customs administration referred to in article 26, 7°, e), and the Financial Intelligence Processing Unit referred to in article 26, 7°, g), the rights of the data subject under this chapter shall be exercised by the competent supervisory authority.

The competent supervisory authority shall merely inform the data subject that the necessary verifications were performed.

By derogation from the second paragraph, the competent supervisory authority may communicate certain contextual information to the data subject.

The King, on the advice of the competent supervisory authority, defines the categories of contextual information the supervisory authority can communicate to the data subject.

**Art. 44.** Where the personal data feature in a judgment or a judicial file or are processed in the context of criminal investigations and proceedings, the rights referred to in articles 37, 38, § 1, 39 and 41, second paragraph, shall be exercised in accordance with the Judicial Code, the Code of Criminal Procedure, the specific laws governing criminal justice and their implementing decrees.

**Art. 45.** § 1. Articles 36 to 44 and 62 are not applicable to the processing of personal data originating, whether directly or indirectly, from the authorities referred to in Title 3 of this Act, in respect of the controllers and competent authorities referred to in this Title to whom the data in question were transferred.

§ 2. The controller or the competent authority referred to in this Title holding such data shall not disclose them to the data subject unless:

1° it is obliged to do so by law in the context of legal proceedings; or

2° the authority referred to in Title 3 authorises it to do so.

§ 3. The controller or the competent authority shall not disclose that it is holding data originating from the authorities referred to in Title 3.

§ 4. The controller referred to in this Title, who processes data originating from the authorities referred to in Title 3, whether directly or indirectly, shall as a minimum meet the following requirements:

1° it shall take the appropriate technical or organisational measures to ensure that access to the data and the processing opportunities is limited to what the persons concerned need to perform their duties or to what is required to meet the needs of the authority referred to in Title 3;

2° it shall take the appropriate technical or organisational measures to protect the personal data against accidental or unauthorised destruction, against accidental loss, alteration or against any other form of unauthorised processing of the personal data concerned.

Members of staff of the controller processing data referred to in the first paragraph are bound by professional secrecy.

§ 5. The restrictions referred to in paragraph 1 also apply to the log files of the processing activities carried out by an authority referred to in Title 3 in the databases of the controllers and competent authorities referred to in this Title which the authority referred to in Title 3 has direct access to.

§ 6. Where a request or complaint is filed with the competent supervisory authority and the controller invokes the application of this article, the supervisory authority in question shall contact Standing Committee I to get it to perform the necessary verifications with the authority referred to in Title 3.

On receipt of the reply from Standing Committee I, the competent supervisory authority shall merely notify the data subject of the results of its verifications relating to the personal data that did not originate from the authority referred to in Title 3, which it is legally obliged to communicate.

If the request or complaint only relates to personal data originating from an authority referred to in Title 3, the competent supervisory authority shall, on receipt of the reply from Standing Committee I, reply that the relevant verifications were performed.

**Art. 46.** Any controller or competent authority referred to in this Title, who communicates personal data to an authority referred to in Subtitles 2 and 4 of Title 3 of this Act, shall not be subject to articles 37, § 1, 8° and 38 § 1, 4° and is not entitled to notify the data subject of that transfer.

**Art. 47.** Where an authority referred to in Subtitles 1 and 6 of Title 3 of this Act has direct access to or received a direct enquiry from a public or private sector database, its processing of personal data shall be protected by technical, organisational and personal security

measures to ensure that only the following actors can have access to the content of these processing activities in the context of the purposes referred to in article 56, § 2:

1° the data protection officer of the database controller or the person the latter has authorised to that effect;

2° the data protection officer of the authority referred to in Subtitles 1 and 6 of Title 3;

3° the database controller or the person the latter has authorised to that effect;

4° the controller of the authority referred to in Subtitles 1 and 6 of Title 3;

5° any other person designated in a protocol between controllers, who need such access to allow them to execute their legal supervisory duties.

The security measures referred to in the first paragraph are intended to safeguard the legal obligations to protect sources, to protect the identity of the officers or the secrecy of the investigations by the authorities referred to in Title 3, Subtitles 1 and 6.

The processing operations referred to in the first paragraph can only be accessed for purposes other than those relating to supervision on condition that these purposes, duly established by or by virtue of a law, are laid down in a protocol agreement between the controllers concerned.

The protocol agreement referred to in the third paragraph shall list the person or persons who need to have access to the log files to meet each objective set out in the third paragraph.

The log files and associated technical, organisational and personal security measures shall be put at the disposal of Standing Committee I

.

The authority referred to in Subtitles 1 and 6 of Title 3 can deviate from the first paragraph in cases where access to its processing activities in a database and to the log files cannot prejudice the interests referred to in the second paragraph.

**Art. 48.** Controllers covered by this Title, who share personal data with a common database, are not permitted to notify the data subject of such transfers.

"Common database" means the joint exercise of the functions carried out in the context of Titles 2 and 3 by several authorities, structured by means of automated processes and applied to personal data.

**Art. 49.** Articles 36 to 44 and 62 do not apply to the processing of personal data by the Passenger Information Unit.

Controllers shall not disclose the data referred to in the first paragraph to the data subject unless compelled to do so by law in the context of legal proceedings.

On no account shall controllers notify data subjects that they are holding data relating to them.

The restrictions referred to in the first paragraph also apply to the log files of the processing operations by the Passenger Information Unit in the databases of the controllers referred to in this Title.

Where a request or complaint is filed with the competent supervisory authority and the controller invokes the application of this article, the former shall merely reply that the necessary verifications were performed.

## CHAPTER IV. - Controller and processor

### Section 1. - Organisational and technical measures

**Art. 50.** Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures. Where proportionate in relation to processing activities, these measures shall include the implementation of appropriate data protection policies by the controller.

The controller shall be able to demonstrate that the processing is performed in accordance with the law.

Those measures shall be reviewed and updated where necessary.

**Art. 51.** § 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, the technical and organisational measures referred to in article 50 shall be designed so as to ensure the effective implementation of the data protection principles and the integration of the necessary safeguards to protect the rights of data subjects, both when defining the means for processing and at the time of the processing itself.

§ 2. The technical and organisational measures referred to in article 50 shall ensure that, in principle, only personal data which are necessary for each specific purpose of the processing are processed.

In particular, such measures shall ensure that, in principle, personal data are not made accessible without human intervention to an indefinite number of natural persons.

### Section 2. - Joint controllers

**Art. 52.** Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

On the basis of an agreement between them, they shall, in a transparent manner, determine the respective responsibilities of the joint controllers, in particular as regards the exercising of the rights of the data subject and their duty to provide the information referred to in articles 37 and 38, unless their respective responsibilities are determined by law, decree, ordinance, European law or international agreement.

In the agreement one single contact point for data subjects may be designated.

### Section 3. - Processor

**Art. 53.** § 1. Where processing is entrusted to a processor, the controller shall use only a processor who provides sufficient guarantees in terms of the technical and organisational security measures implemented with regard to the processing operations.

§ 2. The processor shall not engage another processor without prior specific or general written authorisation of the controller.

In the case of a general written authorisation, the processor shall inform the controller of any intended changes with regard to the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

§ 3. Processing by a processor shall be governed by a contract or other legal act that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the rights and obligations of the controller.

That contract or other legal act shall stipulate, in particular, that the processor:

1° only acts on the instructions of the controller;

2° ensures that any persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality;

3° assists the controller by appropriate means in ensuring compliance with the provisions governing the rights of the data subject;

4° deletes or returns all the personal data to the controller once the processing services have come to an end and deletes any existing copies, unless storage of the personal data is required by law, decree, ordinance, European law or international agreement;

5° makes available to the controller all information necessary to demonstrate compliance with this article;

6° meets the requirements set out under paragraphs 2 and 3 to recruit another processor.

§ 4. The contract or other legal act referred to in paragraph 3 shall be drawn up in writing, including in electronic form.

§ 5. Where, in contravention of this Title, the processor determines the purposes and means of processing, the processor shall be considered to be the controller in respect of that processing.

**Art. 54.** The processor and any person acting under the authority of the controller, or the processor, who has access to personal data, shall exclusively process those data on the instructions of the controller, unless required to do so by law, decree, ordinance, European law or international agreement.

### Section 4. - Obligations

**Art. 55.** § 1. Each controller and processor shall keep a register of the categories of processing activities carried out under its responsibility. That register shall contain the following information:

1° the name and contact details of the controller or the processor and of its deputy or representative;

2° the name and contact details of the data protection officer;

3° the purposes of the processing;

4° the categories of data subjects;

5° the categories of personal data;

6° the categories of recipients;

7° the transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where applicable, the documentation attesting that suitable safeguards are in place;

8° the envisaged time limits for erasure of the various categories of data;

9° a general description of the technical and organisational security measures referred to in article 50;

10° the use of profiling;

11° the legal basis;

12° the category of external sources;

13° the protocol referred to in article 20, including the opinion of the data protection officer and the reasons referred to in article 22.

§ 2. The data protection officer shall be involved in the elaboration and maintenance of the register.

§ 3. The register shall be put at the disposal of the competent supervisory authority.

**Art. 56.** § 1. The log files of at least the following processing operations shall be kept in automated processing systems: the collection, alteration, consultation, disclosure, including transfers, combination and erasure.

The log files relating to consultation and disclosure shall allow the following to be established:

1° the reasons, date and time of the processing activities;

2° the categories of persons who consulted personal data and, where possible, the identity of the person who consulted the personal data;

3° the systems that disclosed these personal data;

4° and the categories of recipients who received the personal data, and where possible, the identity of the recipients of the personal data.

The King can, by decree deliberated on in the Council of Ministers and upon the advice of the supervisory authority, determine other types of processing activities log files must be compiled for.

§ 2. The log files shall be used exclusively to establish whether the processing is lawful, for internal control purposes, to guarantee the integrity and security of the personal data and for the purposes referred to in article 27.

§ 3. The controller and the processor shall make the log files available to the competent supervisory authority on request.

**Art. 57.** On request, the controller and the processor shall cooperate with the supervisory authority in the performance of its tasks.

**Art. 58.** Where a type of processing, in particular a processing operation using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The assessment referred to in the first paragraph shall as a minimum contain a general description of the envisaged processing operations, an assessment of the risk to the rights and freedoms of the data subjects, the measures envisaged to mitigate the risks, the precautionary measures, security measures and mechanisms that have been implemented to safeguard the personal data and demonstrate compliance with this Title, taking into account the rights and legitimate interests of the data subjects and other relevant stakeholders.

**Art. 59.** § 1. The controller or its processor shall consult the competent supervisory authority of the controller prior to processing of personal data which will form part of a new filing system to be created:

1° where a data protection impact assessment as referred to in article 58 shows that the processing is likely to result in a high risk if the controller takes no measures to mitigate the risk; or

2° if the nature of the processing, in particular involving the use of new technologies, mechanisms or procedures is likely to result in a high risk to the rights and freedoms of the data subjects.

The competent supervisory authority shall be consulted when a law, decree, ordinance or a relevant regulatory measure with regard to the processing is drafted.

§ 2. The competent supervisory authority can compile a list of the processing operations in respect of which prior consultation in accordance with paragraph 1 shall take place.

§ 3. The controller shall furnish the competent supervisory authority with the data protection impact assessment pursuant to article 58 and, on request, with any other information on the basis of which the competent supervisory authority can assess the conformity of the processing and, in particular, the risks to the protection of personal data of the data subject and the relevant safeguards.

§ 4. Where the competent supervisory authority is of the opinion that the intended processing referred to in paragraph 1 conflicts with this Title, in particular if the controller has insufficiently identified or mitigated the risk, the competent supervisory authority shall, within six weeks of receipt of the request for consultation, provide the controller and, where applicable, the processor, with a non-binding written opinion and may use any of its powers conferred on it by law. That period may, taking into account the complexity of the intended processing, be extended by one month. The competent supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay.

**Art. 60.** § 1. The controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular with regard to the processing of personal data as referred to in article 34 of this Act and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons.

§ 2. With respect to the automated processing, the controller or processor shall, based on the assessment of the risk, implement measures to:

1° deny unauthorised persons access to processing equipment used for processing;

2° prevent the unauthorised reading, copying, modification or removal of data media;

3° prevent the unauthorised input of personal data in the filling system and the unauthorised consultation, modification or deletion of stored personal data;

4° prevent the use of automated processing systems by unauthorised persons using data communication equipment;

5° ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation;

6° ensure 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;

7° ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input;

8° prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media;

9° ensure that installed systems may, in the case of interruption, be restored;

10° ensure that the functions of the system perform, that the appearance of any faults in the functions is reported and that stored personal data cannot be corrupted by means of a malfunctioning of the system.

**Art. 61.** § 1. The controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the breach of security to the competent supervisory authority. This obligation of notification does not apply if it the breach of security is unlikely to result in a risk to the rights and freedoms of natural persons.

If the notification to the competent supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

§ 2. The processor shall, without undue delay and not later than 72 hours after having become aware of it, notify the breach of security to the controller.

§ 3. The notification referred to in paragraph 1 shall in particular describe or communicate:

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

2° the name and contact details of the data protection officer or other contact point where more information can be obtained;

3° the likely consequences of the breach of security;

4° the measures proposed or taken by the controller to address the breach of security, including, where appropriate, measures to mitigate its possible adverse effects.

§ 4. Where, and in so far as it is not possible to provide all the information at the same time, the information may be provided in phases without undue further delay.

§ 5. Where the breach of security relates to personal data transmitted by or to the controller of another Member State of the European Union, the information referred to in paragraph 3 shall be communicated to the controller of that Member State without undue delay.

§ 6. The controller shall document any breaches of security referred to in paragraph 1, including the facts, its effects and the remedial action taken. That documentation shall enable the competent supervisory authority to verify compliance with this article.

**Art. 62.** § 1. When the breach of security is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the breach of security to the data subject without delay.

§ 2. The communication to the data subject referred to in paragraph 1 shall contain a description of the nature of the security breach and, as a minimum, the information and measures referred to in article 61, § 3, 2° to 4°.

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

1° the controller has implemented appropriate technical and organisational protection measures and those measures were applied to the personal data affected by the breach of security, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as encryption;

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

3° the communication would involve disproportionate effort.

In the case referred to in the first paragraph, 3°, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

§ 4. If the controller has not already communicated the breach of security to the data subject, the competent supervisory authority, having considered the likelihood of the breach of security resulting in a high risk, may compel it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

§ 5. The communication to the data subject referred to in paragraph 1 can be delayed, restricted or omitted under the conditions and for the reasons set out in article 37, § 2.

**Section 5. - Data protection officer**

**Art. 63.** The controller shall designate one or more data protection officers.

The data protection officer shall be designated on the basis of his professional qualities and, in particular, his expert knowledge of data protection law and practices and his ability to fulfil the tasks referred to in article 65.

It is possible to designate one single data protection officer for several authorities or controllers, taking account of their organisational structure and size.

The controller shall publish the contact details of the data protection officer and communicate them to the competent supervisory authority.

The further rules on the functioning, designation and relevant competences are established by the King.

**Art. 64.** The controller shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues relating to the protection of personal data.

The controller shall provide the data protection officer with the resources necessary to carry out those tasks and with access to the personal data and processing operations, and offer him the opportunity to maintain his expert knowledge.

The controller shall ensure that the data protection officer does not receive any instructions in relation to the performance of these tasks. The data protection officer shall directly report to the highest management level of the controller.

Except in pursuance of articles 41 and 44, data subjects can contact the data protection officer about any matters relating to the processing of the information relating to them and the exercise of their rights.

The data protection officer shall be bound by secrecy or confidentiality with regard to the performance of his tasks.

The data protection officer may fulfil other tasks and duties. The controller shall ensure that any such tasks and duties do not result in a conflict of interests.

**Art. 65.** The data protection officer shall in particular have the following tasks:

1° to inform and advise the controller and the employees who carry out processing of their obligations in relation to the protection of personal data;

2° to monitor compliance with the legislation and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and the related audits;

3° to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to article 58;

4° to cooperate with the competent supervisory authority;

5° to act as the contact point for the competent supervisory authority on issues relating to processing, including the prior consultation referred to in article 59, and, where appropriate, engage in consultation with regard to any other matter.

## CHAPTER V. - Transfers of personal data to third countries or international organisations

**Art. 66.** § 1. Without prejudice to the provisions in this Title, the competent authorities can only facilitate the transfer of personal data to countries outside the European Union or to an international organisation, including the onward transfer to another country outside the European Union or international organisation, subject to the following conditions being met:

1° the transfer is necessary for the purposes of article 27;

2° the personal data are transmitted to a controller in a country outside the European Union or at an international organisation which is a competent authority for the purposes referred to in article 27;

3° where personal data are transmitted or made available from another Member State of the European Union, that Member State has given its prior authorisation to the transfer in accordance with its national law;

4° the European Commission has adopted an adequacy decision as referred to in article 67 or, in the absence thereof, appropriate safeguards have been offered or derogations for specific situations under article 69 apply;

5° in the case of an onward transfer to a county outside the European Union or to another international organisation, the controller, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

§ 2. Transfers without prior authorisation by a Member State of the European Union as referred to in paragraph 1, 3°, is permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

**Art. 67.** Transfers of personal data to a country outside the European Union or an international organisation may take place if the European Commission has decided, by adequacy decision, that the country, a region or one or more specific sectors in that country or the international organisation concerned guarantee(s) a suitable level of protection. No specific authorisation is required for transfers such as these.

**Art. 68.** § 1. In the absence of an adequacy decision as referred to in article 67, or where that decision was revoked, amended or suspended, a transfer of personal data to a country outside the European Union or an international organisation can only take place provided:

1° appropriate safeguards for the protection of personal data have been set out in a legally binding instrument; or

2° the controller has assessed all the circumstances surrounding the transfer of personal data and has concluded that the appropriate safeguards with regard to the protection of personal data are in place.

§ 2. The controller informs the competent supervisory authority about the categories of transfers under paragraph 1, 2°.

§ 3. Transfers based on paragraph 1, 2°, shall be documented and contain:

1° the date and time of transfer;

2° information about the competent receiving authority;

3° the reason for the transfer and the personal data transferred.

On request, the documentation shall be made available to the competent supervisory authority.

**Art. 69.** § 1. In the absence of an adequacy decision as referred to in article 67, or of appropriate safeguards as referred in article 68, a transfer or a category of transfers of personal data to a country outside the European Union or an international organisation is permitted only if the transfer is necessary:

1° to protect the vital interests of the data subject or of another natural person;

2° to protect the legitimate interests of the data subject where provided by law;

3° to prevent an immediate and serious threat to public security;

4° in individual cases for the purposes set out in article 27;

5° in individual cases for the establishment, exercise or defence of legal claims relating to the purposes set out in article 27.

§ 2. Personal data shall not be transferred where the transferring competent authority determines that the fundamental rights and freedoms of the data subject override the public interest in the transfer set out in paragraph 1, 4° and 5°.

§ 3. The transfer referred to in paragraph 1, 2°, shall be documented and contain:

1° the date and time of transfer;

2° information about the competent receiving authority;

3° the reason for the transfer and the personal data transferred.

On request, the documentation shall be made available to the competent supervisory authority.

**Art. 70.** § 1. By derogation from article 66, § 1, 2°, and without prejudice to the international agreements and provisions of this Title, the competent authorities may, in specific cases, directly transmit personal data to recipients in countries outside the European Union not qualified as a competent authority for the purposes of article 27, provided all of the following requirements are met:

1° the transfer is strictly necessary for the performance of a task of the transferring competent authority;

2° the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

3° the transferring competent authority considers that the transfer to a competent authority in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

4° the competent authority in the country in question is informed without undue delay, unless this is ineffective or inappropriate;

5° the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

§ 2. The transferring competent authority informs the supervisory authority of the transfers under this article.

§ 3. Where a transfer is based on paragraph 1, such a transfer shall be documented.

**CHAPTER VI: - Independent supervisory authorities**

**Art. 71.** § 1. At Chamber of Representatives level, an independent supervisory authority for police information is set up, known by the name of Supervisory Body for Police Information Management.

It is the legal successor of the Supervisory Body for Police Information Management as set up by article 36ter, § 1, first paragraph of the Privacy Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data.

Towards the competent authorities referred to in article 26, § 1, 7°, a), d) and f), it is responsible for:

1° monitoring the application of this Title, as provided under article 26, 15°;

2° monitoring the processing of the information and personal data referred to in articles 44/1 to 44/11/13 of the Act of 5 August 1992 on the Police Service, including those entered into the databases referred to in article 44/2 of that same Act;

3° any other mandate it is vested with by or by virtue of other laws.

§ 2. The headquarters of the Supervisory Body for Police Information Management is based in the administrative district Brussels-Capital.

With regard to the performance of its tasks and the exercise of its powers pursuant to this Act and other acts, the Supervisory Body for Police Information Management shall act in complete independence.

**TITLE 3. - The protection of natural persons with regard to the processing of personal data by authorities other than those referred to in Titles 1 and 2**

**SUBTITLE 1. - The protection of natural persons with regard to the processing of personal data by the intelligence and security services**

**CHAPTER I. - Definitions**

**Art. 72.** § 1. The definitions referred to in articles 26, 1° to 6°, 9°, 11° to 14°, 16° and 17°, are applicable to this Subtitle.

§ 2. For the purposes of this Subtitle:

1° "the intelligence and security services" means State Security and the General Intelligence and Security Service referred to in the Act of 30 November 1998 governing the intelligence and security services;

2° "the controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

3° "the Act of 30 November 1998" means the Act of 30 November 1998 governing the intelligence and security services;

4° "the Act of 18 July 1991" means the Act of 18 July 1991 governing the review of the police and intelligence services and of the Coordination Unit for Threat Assessment;

5° "the Act of 11 December 1998" means the Act of 11 December 1998 on classification and security clearances, security certificates and security recommendations;

6° "supervisory authority" means an independent public authority mandated by law to monitor the application of this Act;

7° "Standing Committee I" means the Standing Intelligence Agencies Review Committee referred to in the Act of 18 July 1991 tasked with monitoring the application of this Subtitle in application of article 95.

**CHAPTER II. - Scope**

**Art. 73.** This subtitle shall apply to any processing of personal data by the intelligence and security services and their processors, carried out in the context of the mandate of these services as referred to in articles 7 and 11 of the Act of 30 November 1998 and by or by virtue of special laws.

Titles 1, 2, 4, 5 and 7 of this Act are not applicable to the processing operations referred to in the first paragraph. In Title 6 only articles 226, 227 and 230 are applicable.

**CHAPTER III. - General conditions of processing**

**Art. 74.** Personal data shall only be processed in one of the following cases:

1° if the data subject has unambiguously given his consent;

2° if the processing is necessary for the performance of a contract the data subject is party to or for the implementation of measures that precede the conclusion of the contract and which were taken at the request of the data subject;

3° if the processing is useful in terms of the intelligence and security service carrying out its legal duties;

4° if the processing is necessary for the performance of a task carried out in the public interest or which forms part of the exercise of the official authority vested in the controller or the public authority to whom the personal data are disclosed.

**Art. 75.** Personal data shall be:

1° processed lawfully and fairly;

2° collected for specific, explicitly described and legitimate purposes and not further processed in a manner that, taking account of all the relevant factors, in particular the applicable legal and regulatory provisions, is incompatible with those purposes. In accordance with the conditions laid down in articles 99 to 104, further processing for historical, scientific or statistical purposes shall not be regarded as incompatible;

3° adequate, relevant and not excessive in terms of the purposes for which they were collected or are further processed;

4° accurate and, where necessary, updated. All reasonable measures shall be taken to erase or rectify any personal data which, based on the purposes for which they were collected or are further processed, prove to be inaccurate or incomplete.

**CHAPTER IV. - Nature of the personal data**

**Art. 76.** In the interest of the performance of their duties, the intelligence and security services process personal data of any nature, including those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic and biometric data, data concerning health or data concerning sexual behaviour or sexual orientation and data relating to criminal prosecutions and associated offences or security measures.

**CHAPTER V. - Retention of personal data**

**Art. 77.** Personal data shall not be kept longer than necessary for the purposes they are stored and in accordance with the detailed rules set in the context of article 21 of the Act of 30 November 1998.

**CHAPTER VI: - Rights of the data subject**

**Art. 78.** In the context of the processing of personal data relating to a natural person, every natural person has the right to the protection of his fundamental rights and freedoms, in particular to the protection of personal data relating to him.

**Art. 79.** The data subject is entitled to ask that:

1° incorrect personal data relating to him are corrected or erased;

2° Standing Committee I verifies compliance with the provisions of this Subtitle.

**Art. 80.** The rights referred to in article 79 shall be exercised free of charge via Standing Committee I on the initiative of the data subject who shall furnish proof of identity.

Standing Committee I shall perform the verification and shall merely inform the data subject that the necessary verifications were carried out.

The specific rules governing the exercise of these rights are laid down by law.

**Art. 81.** Standing Committee I and the intelligence and security services shall keep a log file of all the requests from data subjects to exercise their rights.

**Art. 82.** Decisions that give rise to legal consequences for a person cannot be taken purely on the basis of an automated processing of personal data designed to assess certain aspects of that person's personality.

The ban under the first paragraph shall not apply if the decision is based on a legal provision or when necessary for reasons of substantial public interest.

**CHAPTER VII. - Obligations of the controller and the processor**

**Section 1. - General obligations**

**Art. 83.** The controller:

1° shall see to it that the personal data are updated; that incorrect, incomplete or irrelevant data, including data that were collected or further processed in contravention of this subtitle, are corrected or erased;

2° shall ensure that access to the data and the processing opportunities is limited to what the persons acting under its authority need to perform their duties or to what is required to provide the service;

3° shall inform all persons acting under its authority about all the provisions of this Subtitle and about all the relevant provisions governing the protection of privacy in the context of the processing of personal data.

Art. 84. Where processing is entrusted to a processor, the controller shall:

1° use only a processor providing sufficient guarantees in terms of the technical and organisational security measures with regard to the processing activities;

2° ensure compliance with these measures, in particular, via contractual provisions;

3° define the responsibility of the processor in the contract;

4° agree with the processor that the latter acts on the instructions of the controller only and that it is subject to the same obligations the controller is bound by in virtue of this Subtitle;

5° set out the elements of the contract relating to the protection of personal data and the requirements relating to the measures referred to in the provisions sub 3° and 4° in a written document or on an electronic device.

**Art. 85.** The processor shall be subject to the same obligations as the controller is bound by.

Unless expressly authorised by the controller, the processor is not entitled to entrust the processing of personal data to another processor.

**Art. 86.** Except pursuant to a legal obligation, anyone acting under the authority of the controller or the processor, including the processor, who has access to personal data, can only process them on the instructions of the controller.

**Section 2. - Joint controllers**

**Art. 87.** Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

The contract sets out the respective responsibilities of the joint controllers, in particular as regards the exercise of the rights of the data subject and the communication of personal data, unless their respective obligations are defined by or by virtue of a law.

The contract shall designate one contact point for data subjects. The joint controllers shall list this point of contact in the register referred to in article 90.

**Section 3. - Security of personal data**

**Art. 88.** The controller, as well as the processor, shall take the appropriate technical and organisational measures to protect personal data against accidental or unauthorised destruction, accidental loss, including against any unauthorised alteration of or access to, and against any other unauthorised processing of personal data.

These measures shall ensure an appropriate level of security, taking account, on the one hand, of the state of the art and the costs of implementation and, on the other hand, of the nature of the personal data to be protected and the potential risks.

**Art. 89.** § 1. Where a security breach is likely to result in a high risk for the rights and freedoms of natural persons, the controller shall communicate this breach to Standing Committee I without delay and, where feasible, not later than 72 hours after having become aware of it.

§ 2. The processor shall notify the controller of any security breach without delay.

§ 3. The notification referred to in paragraphs 1 and 2 shall, as a minimum, describe or communicate:

1° the nature of the security breach including, where possible, the approximate number of data subjects and personal data concerned;

2° the name and contact details of the data protection officer or other contact point where more information can be obtained;

3° the likely consequences of the security breach;

4° the measures taken or proposed by the controller or the processor to address the breach of security, including, where appropriate, measures to mitigate its possible adverse effects.

**Section 4. - Registers**

**Art. 90.** § 1. The controller shall keep a register, classified within the meaning of the Act of 11 December 1998, of the databases of the intelligence and security services and of those made available to it.

This register shall contain the following information:

1° as regards the databases of the intelligence and security services:

a) the contact details of the controller and, where appropriate, of the joint controllers, and of the data protection officer;

b) the purposes of the processing;

c) the categories of recipients the personal data may be communicated to;

d) insofar as possible, the envisaged time limits for erasure of the personal data;

e) insofar as possible, a general description of the technical and organisational security measures referred to in article 88;

2° as regards the databases made available to the intelligence and security services:

a) the contact details of the controller and, where possible, for the countries outside the European Union, the agency managing the database, and, where appropriate, of the joint controllers and of the data protection officer;

b) the purposes of the processing of the intelligence and security services.

§ 2. Each processor shall keep a register, classified within the meaning of the Act of 11 December 1998, of all the categories of processing activities it carried out on behalf of the controller.

This register shall contain the following information:

1° the contact details of the processor and of the controller on behalf of whom the processor is acting, and, where appropriate, of the data protection officer;

2° the categories of processing operations carried out on behalf of the controller;

3° where possible, a general description of the technical and organisational security measures referred to in article 88;

§ 3. The registers referred to in paragraphs 1 and 2 shall be compiled in writing, including in electronic form.

§ 4. The controller shall make the register available to Standing Committee I at its request.

On request, the processor shall make the register available to the controller and to Standing Committee I.

**Section 5. - Data protection officer**

**Art. 91.** § 1. The controller, and, where appropriate, the processor, shall designate a data protection officer. This decision shall be communicated to Standing Committee I.

The data protection officer shall be the holder of a "top secret" security clearance, within the meaning of the Act of 11 December 1998.

§ 2. The data protection officer cannot be penalised for performing his tasks. Neither can he be dismissed for carrying out his duties, except if he is found guilty of serious misconduct or no longer meets the requirements necessary for the exercise of his mandate.

The data protection officer can appeal any such decision to Standing Committee I.

§ 3. He is, in an independent manner, tasked with:

1° monitoring compliance with this Subtitle throughout the processing of personal data;

2° providing advice on any useful measures designed to guarantee the security of the data stored;

3° informing and advising the controller, and, where applicable, the processor, the head of department and the staff of the department carrying out the processing of their obligations under this Subtitle;

4° issuing opinions and recommendations to the controller, and, where applicable, to the processor or the head of department;

5° performing other duties entrusted to him by the controller, and, where applicable, by the processor or the head of department.

The data protection officer is the contact person for Standing Committee I with regard to the application of this Subtitle.

§ 4. The controller and, where appropriate, the processor, shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues relating to the protection of personal data.

The controller, and, where applicable, the processor, shall see to it that the data protection officer has all the resources necessary to carry out his tasks.

The data protection officer may be assisted by one or several deputies.

§ 5. Where appropriate, the King can establish further rules on the functioning, the designation and the relevant competences.

## CHAPTER VIII. - Communication and transfer of personal data

### Section 1. - Communication of personal data to the public sector and to the private sector

**Art. 92.** By way of derogation from articles 20, 22, 23, 58 and 59 of this Act and from articles 35 en 36 of the Regulation and in the interest of the performance of the mandate of the intelligence and security services, neither a protocol, nor an opinion of the data protection officer, nor a data protection impact assessment, nor the opinion issued following consultation with the competent supervisory authority can be a prerequisite for the communication of personal data between an intelligence and security service and any public or private body.

This notification shall be made in accordance with articles 14, 16 and 19 of the Act of 30 November 1998.

Where the parties decide to sign a protocol, the protocol shall, by way of derogation from article 20, § 1, second paragraph, contain the following:

1° the identity of the intelligence and security service and of the public or private body exchanging personal data;

2° the identity of the controllers;

3° the contact details of the relevant data protection officers;

4° the purposes for which the personal data are transferred;

5° the legal basis;

6° the restrictions to the rights of the data subject.

The protocol referred to in the third paragraph shall be marked "RESTRICTED" within the meaning of the Royal Decree of 24 March 2000 implementing the Act of 11 December 1998, where a classification within the meaning of the Act of 11 December 1998 is unjustified.

### Section 2. - Transfer of personal data to countries that are not a member of the European Union or to international organisations

**Art. 93.** Personal data can only be transferred to a country that is not a member of the European Union or to an international organisation if that country or that organisation

ensures an appropriate level of protection and compliance with the other provisions of this Subtitle.

The question whether the level of protection is appropriate shall be assessed taking account of all the circumstances relating to the transfer of personal data or to a category of transfers of personal data. More specifically, account shall be taken of the nature of the data, the purpose and the duration of the intended processing, the country of origin and the country of final destination, the general and sectoral rules of law prevailing in the country in question or within the organisation, including the ethics and security measures adhered to in these countries or organisations.

An appropriate level of protection can be assured by means of security clauses between the controller and the recipient of the personal data.

**Art. 94.** By way of derogation from article 93, transfers of personal data to a country that is not a member of the European Union or to an international organisation which does not offer any guarantees in terms of an appropriate level of protection can take place only if:

1° the data subject has unambiguously given his consent to the envisaged transfer; or

2° the transfer is mandatory in the context of international relations; or

3° the transfer is essential to safeguard the vital interest of the persons; or

4° the transfer is essential or required by law to safeguard a substantial public interest or to establish, exercise or defend a right in law.

**CHAPTER IX. - Supervisory authority**

**Art. 95.** By way of derogation from the Act of 3 December 2017 establishing the Data Protection Authority, Standing Committee I, in its capacity of independent public authority, has been designated as data protection authority tasked with monitoring the processing of personal data by the intelligence and security services and their processors pursuant to the detailed rules laid down in the Act of 18 July 1991.

Standing Committee I monitors the application of this Subtitle to safeguard the fundamental rights and freedoms of natural persons in respect of that processing.

**Art. 96.** Where necessary, Standing Committee I shall cooperate with other Belgian supervisory authorities, without prejudice to the physical integrity of persons, or the mandate of the intelligence and security services or the Act of 11 December 1998.

In the context of the exercise of the supervision referred to in article 95, Standing Committee I shall share the result thereof with the other competent supervisory authorities. These shall not disclose the results to the data subject.

**Art. 97.** The intelligence and security services and their processors shall cooperate with Standing Committee I.

**Art. 98.** The supervisory authorities shall notify Standing Committee I of any infringements of the regulations on the processing of personal data by the intelligence and security services as soon as they become aware of it.

Each supervisory authority shall consult Standing Committee I when seized of a file that may have consequences for the processing of personal data by the intelligence and security services.

## CHAPTER X. - Processing of personal data for historical, scientific or statistical purposes

**Art. 99.** By way of derogation from Title 4, consultation for historical, scientific or statistical purposes, by a subsequent controller, of personal data of the intelligence and security services and their staff shall be authorised by the intelligence and security service concerned if it does not prejudice its mandate, its obligations referred to in articles 13, third paragraph, and 13/4, second paragraph, of the Act of 30 November 1998, an ongoing preliminary or judicial investigation, or the relations between Belgium and foreign States or international organisations and in accordance with the Act of 11 December 1998.

Each request to the State archives to further process personal data of the intelligence and security services and their staff for purposes other than those referred to in the first paragraph shall be refused unless the purpose is legitimate and the intelligence and security service concerned is of the opinion that the processing cannot prejudice the interests referred to in the first paragraph.

**Art. 100.** Prior to the consultation referred to in article 99, the personal data shall be marked "Protection of personal data - articles 99 to 104 of the Act of 30 July 2018".

**Art. 101.** The personal data referred to in article 99 shall be anonymised before they are consulted.

Where the further processing of anonymous data does not allow the historical, scientific or statistical purposes to be realised, the intelligence and security service may authorise the consultation of pseudonymised data.

Where anonimysation or pseudonymisation does not prevent the identification of the data, the intelligence and security service shall refuse consultation in cases where this would lead to a disproportionate prejudice to privacy.

Where the further processing of pseudonymised data does not allow the historical, scientific or statistical purposes to be realised, the intelligence and security service may authorise the consultation of non-pseudonymised data in cases where this would not lead to a disproportionate prejudice to privacy.

**Art. 102.** By way of derogation from Title 4, the communication or publication of non-anonymised or non-pseudonymised personal data referred to in article 99, consulted by a subsequent controller, shall invariably require the consent of the intelligence and security service concerned and be subject to the conditions laid down by the latter.

**Art. 103.** The subsequent controller of personal data referred to in article 99 shall keep a log file of its further processing activities for historical, scientific or statistical purposes.

This log file shall be classified within the meaning of the Act of 11 December 1998 if the processing relates to classified data.

This log file shall contain the following information:

1° the contact details of the first controller, the subsequent controller and of the latter's data protection officer;

2° the purposes of the further processing;

3° the data, object of the further processing;

4° the conditions governing the further processing, if any, as defined by the intelligence and security service concerned;

5° the recipients, if any, authorised by the intelligence and security service concerned.

**Art. 104.** Each public authority, natural person or legal person processing personal data as referred to in article 99 for historical, scientific or statistical purposes shall be regarded as data controller.

He or she may not engage in activities designed to convert the anonymous or pseudonymised data into non-anonymous or non-pseudonymised data.

**SUBTITLE 2. - The protection of natural persons with regard to the processing of personal data by the armed forces**

**Art. 105.** When deploying the armed forces, and during the preparations with a view to the deployment of the armed forces, as referred to in article 3 of the Act of 20 May 1994 on the periods and positions of the military of the reserve forces and the deployment and preparations of the armed forces with a view to fulfilling their constitutional mandate, the following regime applies:

1° insofar as necessary for the exercise of their functions, the armed forces process personal data of any nature, including those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic and biometric data, data concerning health or data concerning sexual behaviour or sexual orientation and data relating to criminal prosecutions and associated offences or security measures;

2° the personal data can be processed only if their processing is necessary for the deployment or preparations with a view to the deployment of the armed forces and shall not be processed in a manner that is incompatible with these purposes;

3° the personal data shall be processed lawfully and fairly;

4° the personal data shall be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

5° the personal data shall be adequate, relevant and not excessive in terms of the purposes for which they were collected or are further processed;

6° the personal data shall be accurate and, where necessary, updated. All reasonable measures shall be taken to erase or rectify any personal data which, based on the purposes for which they were collected or are further processed, prove to be inaccurate or incomplete.

7° the personal data may be transmitted to a country that is not a member of the European Union or to an international organisation if such transfer is necessary for operational reasons;

8° with the exception of the definitions under article 26, 1° to 6°, 8° to 14°, 16° and 17°, and of articles 2, 78 and 83 to 89, the provisions of the other Titles do not apply;

9° with regard to the processing of personal data, the following rights shall be restricted only if this constitutes a necessary and proportionate measure within the constraints of applicable international law on the deployment of the armed forces or their preparations with a view to the deployment of the armed forces:

a) the right to take cognisance of the existence of an automated file of personal data, its main purposes, including the identity and regular place of business or headquarters of the file holder;

b) the right, where necessary, to have the data rectified or erased if they were processed in contravention of the law;

c) the right to legal remedy in cases where a request for confirmation or, as appropriate, communication, rectification or exchange of personal data is disregarded.

10° insofar as it does not pose a risk to the deployment and the preparations of the armed forces, the processing of personal data is subject to control by the competent supervisory authority.

## SUBTITLE 3. - The protection of natural persons with regard to the processing of personal data in the context of the Act of 11 December 1998 on classification and security clearances, security certificates and security recommendations

### CHAPTER I. - Definitions

**Art. 106.** § 1. The definitions set out in articles 26, 1° to 6°, 9°, 11° to 14°, 16° and 17°, are applicable to this Subtitle.

§ 2. For the purposes of this Subtitle:

1° "the Act of 11 December 1998" means the Act of 11 December 1998 on classification and security clearances, security certificates and security recommendations;

2° "the Act of 11 December 1998 creating an appeal board" means the Act of 11 December 1998 creating an appeal board in respect of security authorisations, security certificates and security recommendations;

3° "appeal board" means the appeal board referred to in article 3 of the Act of 11 December 1998 creating an appeal board;

4° "the controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

5° "supervisory authority" means the independent public authority mandated by law to monitor the application of this Subtitle;

6° "Standing Committee I" means the Standing Intelligence Agencies Review Committee on the Intelligence and Security Services referred to in the Act of 18 July 1991 tasked with monitoring the application of this Subtitle pursuant to article 95.

### CHAPTER II. - Scope

**Art. 107.** This Subtitle applies to all processing operations of personal data in the context of security clearances, security certificates and security recommendations referred to in the Act of 11 December 1998 by:

1° the security authority referred to in article 15, first paragraph, of the Act of 11 December 1998;

2° any member of the government referred to in the provision sub 1°;

3° the authorities referred to in articles 15, second paragraph and 22ter of the Act of 11 December 1998;

4° the security officers referred to in article 13, 1°, of the Act of 11 December 1998;

5° the processors of authorities and persons referred to in the provisions sub 1° to 4°.

This Subtitle also applies to any processing operations of personal data by the appeal board in the context of the redress procedures referred to in the Act of 11 December 1998 creating an appeal board.

Titles 1, 2, 4, 5 and 7 of this Act are not applicable to the processing operations referred to in the first paragraph. For the purpose of Title 6, only articles 226, 227 and 230 are applicable.

**CHAPTER III. - General conditions of processing**

**Art. 108.** Personal data can be processed in one of the following cases only:

1° if the data subject has unambiguously given his consent;

2° if the processing is necessary for the performance of a contract the data subject is party to or for the implementation of measures that precede the conclusion of the contract and which were taken at the request of the data subject;

3° if the processing is necessary in terms of an obligation the controller is subject to by or by virtue of a law;

4° if the processing is necessary for the performance of a task carried out in the public interest or forms part of the exercise of the official authority vested in the controller or the third party to whom the personal data are disclosed.

**Art. 109.** Personal data shall be:

1° processed in a manner that is lawful and appropriate in respect of the data subject;

2° collected for specific, explicitly described and legitimate purposes and not further processed in a manner that, taking account of all the relevant factors, in particular the applicable legal and regulatory provisions, is incompatible with those purposes. In accordance with the conditions laid down in articles 132 to 137, further processing for historical, scientific or statistical purposes shall not be regarded as incompatible;

3° adequate, relevant and not excessive in terms of the purposes for which they were collected or are further processed;

4° accurate and, where necessary, updated. All reasonable measures shall be taken to erase or rectify any personal data which, based on the purposes for which they were collected or are further processed, prove to be inaccurate or incomplete.

**CHAPTER IV. - Nature of the personal data**

**Art. 110.** In the interest of the performance of their duties, the authorities, bodies and persons referred to in article 107 process personal data of any nature, including those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic and biometric data, data concerning health or data concerning sexual behaviour or sexual orientation and data relating to criminal prosecutions and associated offences or security measures.

**CHAPTER V. - Retention of personal data**

**Art. 111.** Personal data shall not be kept longer than necessary for the purposes they are stored and in accordance with the specific rules set out under article 25 of the Act of 11 December 1998.

**CHAPTER VI: - Rights of the data subject**

**Art. 112.** In the context of the processing of personal data relating to a natural person, every natural person has the right to the protection of his fundamental rights and freedoms, in particular to the protection of personal data relating to him/her.

**Art. 113.** The data subject is entitled to ask that:

1° incorrect personal data relating to him/her are corrected or erased;

2° the competent supervisory authority verifies compliance with the provisions of this Subtitle.

**Art. 114.** § 1. To safeguard the confidentiality and effectiveness of the processing activities, access by the data subject to personal data relating to him/her being processed by the authorities, bodies and persons referred to in article 107, first paragraph, shall be limited to the information the data subject disclosed to them.

The rights referred to in article 113, 1° and 2° with regard to the processing activities referred to in article 107, first paragraph, shall be exercised by Standing Committee I free of charge on the initiative of the data subject who shall furnish proof of identity. Standing Committee I shall perform the verification and shall only inform the data subject that the necessary verifications were carried out.

§ 2. The data subject's access to his personal data processed by the appeal board shall be facilitated in accordance with article 6 of the Act of 11 December 1998 creating an appeal board.

To exercise his rights referred to in article 113, 1°, and with regard to the processing operations referred to in article 107, second paragraph, the data subject shall contact the appeal board in accordance with the specific rules set out under the Act of 11 December 1998 creating an appeal board.

**Art. 115.** Decisions that give rise to adverse legal consequences for a person cannot be taken purely on the basis of an automated processing of personal data designed to assess certain aspects of that person's personality.

The ban under the first paragraph shall not apply if the decision is based on a legal provision or is necessary for reasons of substantial public interest.

## CHAPTER VII. - Obligations of the controller and the processor

### Section 1. - General obligations

**Art. 116.** The controller:

1° shall ensure that personal data are updated; that incorrect, incomplete or irrelevant data, including data that were collected or further processed in contravention of this subtitle, are corrected or erased;

2° shall ensure that access to the data and the processing opportunities is limited to what the persons acting under its authority need to perform their duties or to what is required to perform the service;

3° shall inform all persons acting under its authority about all the provisions of this Subtitle and about all the relevant provisions governing the protection of privacy in the context of the processing of personal data.

**Art. 117.** Where processing is entrusted to a processor, the controller shall:

1° use only a processor providing sufficient guarantees in terms of the technical and organisational security measures with regard to the processing activities;

2° ensure compliance with these measures, in particular, via contractual provisions;

3° define the responsibility of the processor in the contract;

4° agree with the processor that the latter acts on the instructions of the controller only and that it is subject to the same obligations the controller is bound by under this Subtitle.

**Art. 118.** The processor shall be subject to the same obligations as the controller is bound by.

Unless expressly authorised by the controller, the processor is not entitled to entrust the processing of personal data to another processor.

**Art. 119.** Except pursuant to a legal obligation, anyone acting under the authority of the controller or the processor, including the processor, who has access to personal data, can only process them on the instructions of the controller.

### Section 2. - Joint controllers

**Art. 120.** Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

The contract sets out the respective obligations of the joint controllers, in particular as regards the exercise of the rights of the data subject and the communication of personal data, unless their respective obligations are defined by or by virtue of a law.

The contract shall designate one contact point for data subjects. The joint controllers shall list this point of contact in the register referred to in article 123.

## Section 3. - Security of personal data

**Art. 121.** To safeguard the security of the personal data, the controller, and the processor, shall take the appropriate technical and organisational measures to protect the personal data against accidental or unauthorised destruction, accidental loss, including against any unauthorised alteration of or access to, and against any other unauthorised processing of personal data.

These measures shall ensure an appropriate level of security, taking account, on the one hand, of the state of the art and the costs of implementation and, on the other hand, of the nature of the personal data to be protected and the potential risks.

**Art. 122.** § 1. Where security breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate this breach to Standing Committee I without delay and, where feasible, not later than 72 hours after having become aware of it.

§ 2. The processor shall notify the controller of any security breach without delay.

§ 3. The notification referred to in paragraphs 1 and 2 shall, as a minimum, describe or communicate:

1° the nature of the security breach including, where possible, the approximate number of data subjects and personal data concerned;

2° the name and contact details of the data protection officer or other contact point where more information can be obtained;

3° the likely consequences of the security breach;

4° the measures taken or proposed by the controller or the processor to address the security breach, including, where appropriate, measures to mitigate its possible adverse effects.

## Section 4. - Registers

**Art. 123.** § 1. The controller and, where appropriate, its processor, shall keep a register of the personal data processing activities.

This register shall, where appropriate and insofar as possible, contain the following processing-related details:

1° the contact details of the controller and, where appropriate, of the joint controllers, and of the data protection officer;

2° the purposes of the processing;

3° the categories of data subjects;

4° the categories of personal data;

5° the categories of the main recipients personal data may be communicated to;

6° the transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where applicable, the documentation attesting that suitable safeguards are in place;

7° the envisaged time limits for erasure of the personal data;

8° the use of profiling;

9° the legal basis;

10° a general description of the technical and organisational security measures referred to in article 121.

§ 2. The registers referred to in paragraph 1 shall be compiled in writing, including in electronic form.

§ 3. The controller shall make the register available to the competent supervisory authority, at its request.

On request, the processor shall make the register available to the controller and also to the competent supervisory authority.

**Section 5. - Data protection officer**

**Art. 124.** § 1. The controller, and, where appropriate, the processor, shall designate a data protection officer. This decision shall be communicated to the competent supervisory authority.

The data protection officer shall be the holder of a "top secret" security clearance, within the meaning of the Act of 11 December 1998.

§ 2. The data protection officer cannot be penalised for performing his tasks. Neither can he be dismissed for carrying out his duties, except if he is found guilty of serious misconduct or no longer meets the requirements necessary for the exercise of his mandate.

The data protection officer can appeal any such decision to Standing Committee I.

§ 3. He is, in an independent manner, tasked with:

1° monitoring compliance with this Subtitle throughout the processing of personal data;

2° issuing recommendations on any useful measures to ensure the security of the personal data stored;

3° informing and advising the controller, and, where applicable, the processor, and the members of staff carrying out the processing of their obligations under this Subtitle;

4° issuing opinions and recommendations to the controller, and, where applicable, to the processor;

5° performing other duties entrusted to him by the controller, and, where applicable, by the processor.

The data protection officer is the contact person for the competent supervisory authority with regard to the application of this Subtitle.

§ 4. The controller and, where appropriate, the processor, shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues relating to the protection of personal data.

The controller, and, where applicable, the processor, shall see to it that the data protection officer has all the resources necessary to carry out his tasks.

The data protection officer may be assisted by one or several deputies.

§ 5. Where appropriate, the King can establish further rules on the functioning, the designation and the relevant competences.

## CHAPTER VIII. - Communication and transfer of personal data

### Section 1. - Communication of personal data to the public sector and to the private sector

**Art. 125.** § 1. By way of derogation from articles 20, 22, 23, 58 and 59 of this Act and from articles 35 and 36 of the Regulation, neither a protocol, nor an opinion of the data protection officer, nor a data protection impact assessment, nor the opinion issued following consultation with the competent supervisory authority can be a prerequisite for the communication of personal data between the authorities or persons referred to in article 107 and any public or private body.

This notification shall be made in accordance with the Act of 11 December 1998.

§ 2. Where the parties decide to sign a protocol, the protocol shall, by way of derogation from article 20, § 1, second paragraph, contain the following:

1° the identity of the federal government body or the federal public body transmitting personal data;

2° the identity of the controllers;

3° the contact details of the relevant data protection officers;

4° the purposes for which the personal data are transferred;

5° the legal basis;

6° the specific rules on the communication method used;

7° the restrictions to the rights of the data subject;

8° the periodicity of the data transfer;

9° the duration of the protocol.

### Section 2. - Transfer of personal data to countries that are not a member of the European Union or to international organisations

**Art. 126.** Personal data can only be transferred to a country that is not a member of the European Union or to an international organisation if that country or that organisation ensures an appropriate level of protection and compliance with the other provisions of this Subtitle.

The question whether the level of protection is appropriate shall be assessed taking account of all the circumstances related to the transfer of personal data or to a category of transfers of personal data. More specifically, account shall be taken of the nature of the data, the purpose and the duration of the intended processing, the country of origin and the country of final destination, the general and sectoral rules of law prevailing in the country in question or within the organisation, including the ethics and security measures adhered to in these countries or organisations.

An appropriate level of protection can be assured by means of security clauses between the controller and the recipient of the personal data.

**Art. 127.** By way of derogation from article 126, transfers of personal data to a country that is not a member of the European Union or to an international organisation which do not ensure an appropriate level of protection can take place only if:

1° the data subject has unambiguously given his consent to the envisaged transfer; or

2° the transfer is mandatory in the context of international relations; or

3° the transfer is essential to safeguard the vital interest of the persons; or

4° the transfer is essential or required by law to safeguard a substantial public interest or to establish, exercise or defend a right in law.

## CHAPTER IX. - Supervisory authority

**Art. 128.** § 1. By way of derogation from the Act of 3 December 2017 establishing the Data Protection Authority, Standing Committee I, in its capacity of independent public authority, has been designated as supervisory authority tasked with monitoring the processing of personal data carried out in the context of article 107, first paragraph, by the authorities and persons referred to in that same paragraph.

Standing Committee I monitors the application of this Subtitle to safeguard the fundamental rights and freedoms of natural persons in respect of that processing.

§ 2. In its capacity of judicial authority, the appeal board is not subject to control by a data protection supervisory authority.

**Art. 129.** Where necessary, Standing Committee I shall, with due regard for the Act of 11 December 1998, cooperate with other Belgian supervisory authorities, and this without prejudice to the interests referred to in article 5 of the Act of 11 December 1998 creating an appeal board.

In the context of the exercise of the supervision referred to in article 128, Standing Committee I shall share the result thereof with other competent supervisory authorities.

**Art. 130.** The authorities and persons referred to in article 107, first paragraph, shall cooperate with Standing Committee I.

**Art. 131.** The supervisory authorities shall notify Standing Committee I of any infringements of the regulations on the processing of personal data in the context of article 107 as soon as they become aware of it.

Each supervisory authority shall consult Standing Committee I when seized of a file that may have consequences for the processing of personal data in the context of article 107.

## CHAPTER X. - Processing of personal data for historical, scientific or statistical purposes

**Art. 132.** By way of derogation from Title 4, the consultation of personal data for historical, scientific or statistical purposes held by the authorities, the appeal board or the persons referred to in article 107 and their staff by a subsequent controller is authorised, provided it does not prejudice the interests referred to in article 12, first paragraph, of the Act of 11 December 1998.

**Art. 133.** Prior to the consultation referred to in article 132, the personal data shall be marked "Protection of personal data - articles 132 to 137 of the Act of 30 July 2018".

**Art. 134.** The personal data referred to in article 132 shall be anonymised before they are consulted.

Where a further processing of anonymous data does not allow the historical, scientific or statistical purposes to be realised, the controller may, in the context of article 107, authorise the consultation of pseudonymised data.

Where anonimysation or pseudonymisation does not prevent the identification of the data, the controller shall, in the context of article 107, refuse consultation in cases where this privacy would be disproportionately prejudiced.

Where a further processing of pseudonymised data does not allow the historical, scientific or statistical purposes to be realised, the controller may, in the context of article 107, authorise the consultation of non-pseudonymised data in cases where privacy will not be disproportionately prejudiced.

**Art. 135.** By way of derogation from Title 4, the communication or publication of non-anonymised or non-pseudonymised personal data referred to in article 132, consulted by a subsequent controller, shall invariably require the consent of the controller in the context of article 107 and be subject to the conditions laid down by the latter.

**Art. 136.** The subsequent controller of personal data referred to in article 132 shall keep a log file of its further processing activities for historical, scientific or statistical purposes.

This log file shall be classified within the meaning of the Act of 11 December 1998 if the processing relates to classified data.

This log file shall contain the following information:

1° the contact details of the first controller, the subsequent controller and of the latter's data protection officer;

2° the purposes of the further processing;

3° the conditions for the further processing, if any, as defined by the controller in the context of article 107;

4° the recipients, if any, authorised by the controller in the context of article 107.

**Art. 137.** Each public authority, natural person or legal person processing personal data as referred to in article 132 for historical, scientific or statistical purposes shall be regarded as data controller.

He or she may not engage in activities designed to convert the anonymous or pseudonymised data into non-anonymous or non-pseudonymised data.

## SUBTITLE 4. - The protection of natural persons with regard to the processing of personal data by the Coordination Unit for Threat Assessment

### CHAPTER I. - Definitions

**Art. 138.** § 1. The definitions referred to in articles 26, 1° to 6°, 9°, 11° to 14° and 16° to 17° are applicable to this Subtitle.

§ 2. For the purposes of this Subtitle:

1° "CUTA" means the Coordination Unit for Threat Assessment referred to in the Threat Assessment Act of 10 July 2006;

2° "the controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

3° "the Act of 18 July 1991" means the Act of 18 July 1991 governing the review of the police and intelligence services and of the Coordination Unit for Threat Assessment;

4° "the Act of 11 December 1998" means the Act of 11 December 1998 on classification and security clearances, security certificates and security recommendations;

5° "supervisory authority" means an independent public authority mandated by law to monitor the application of this Act;

6° "the Act of 10 July 2006" means the Threat Assessment Act of 10 July 2006;

7° "the CUTA information system" means the information system referred to in article 9 of the Act of 10 July 2006.

**CHAPTER II. - Scope**

**Art. 139.** This Subtitle shall apply to any processing of personal data by CUTA, carried out in the context of its mandate as referred to in the Act of 10 July 2006 and by or by virtue of special acts.

Titles 1, 2, 4, 5 and 7 of this Act are not applicable to the processing operations referred to in the first paragraph. For the purpose of Title 6, only articles 226, 227 and 230 shall be applicable.

**CHAPTER III. - General conditions of processing**

**Art. 140.** Personal data can be processed in one of the following cases only:

1° if the data subject has unambiguously given his consent;

2° if the processing is necessary for the performance of a contract the data subject is party to or for the implementation of measures that precede the conclusion of the contract and which were taken at the request of the data subject;

3° if the processing is useful in terms of an obligation CUTA is subject to by or by virtue of a law;

4° if the processing is necessary for the performance of a task carried out in the public interest or forms part of the exercise of the official authority vested in the controller or the public authority to whom the personal data are disclosed.

**Art. 141.** Personal data shall be:

1° processed lawfully and fairly;

2° collected for specific, explicitly described and legitimate purposes and not further processed in a manner that, taking account of all the relevant factors, in particular the applicable legal and regulatory provisions, is incompatible with those purposes. In

accordance with the conditions laid down in articles 162 to 167, further processing for historical, scientific or statistical purposes shall not be regarded as incompatible;

3° adequate, relevant and not excessive in terms of the purposes for which they were collected or are further processed;

4° accurate and, where necessary, updated. All reasonable measures shall be taken to erase or rectify any personal data which, based on the purposes for which they were collected or are further processed, prove to be inaccurate or incomplete.

**CHAPTER IV. - Nature of the personal data**

**Art. 142.** Insofar as necessary in the interest of the exercise of its mandate, CUTA processes personal data of any nature, including those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic and biometric data, data concerning health or data concerning sexual behaviour or sexual orientation and data relating to criminal prosecutions and associated offences or security measures.

**CHAPTER V. - Retention of personal data**

**Art. 143.** Personal data shall not be kept longer than necessary for the purposes they are stored and in accordance with the detailed rules set out under article 9 of the Act of 10 July 2006 as far as the CUTA information system is concerned and article 44/11/3bis of the Act of 5 August 1992 on the Police Service as regards the common databases CUTA is the operational administrator of.

**CHAPTER VI. - Rights of the data subject**

**Art. 144.** In the context of the processing of personal data relating to a natural person, every natural person has the right to the protection of his fundamental rights and freedoms, in particular to the protection of personal data relating to him.

**Art. 145.** The data subject is entitled to ask that:

1° incorrect personal data relating to him/her are corrected or erased;

2° the competent supervisory authority verifies compliance with the provisions of this Subtitle.

**Art. 146.** The rights referred to in article 145 shall be exercised free of charge via the competent supervisory authority on the initiative of the data subject who shall furnish proof of identity.

The competent supervisory authority shall perform the verification and shall only inform the data subject that the necessary verifications were carried out.

The specific rules governing the exercise of these rights are laid down by law.

**Art. 147.** The supervisory authorities referred to in article 161 and CUTA shall keep a log file of all the requests from data subjects to exercise their rights.

**Art. 148.** Decisions that give rise to legal consequences for a person cannot be taken purely on the basis of an automated processing of personal data designed to assess certain aspects of that person’s personality.

The ban under the first paragraph shall not apply if the decision is based on a legal provision or when the decision is necessary for reasons of substantial public interest.

## CHAPTER VII. - Obligations of the controller and the processor

### Section 1. - General obligations

**Art. 149.** The controller:

1° shall see to it that the personal data are updated; that incorrect, incomplete or irrelevant data, including data that were collected or further processed in contravention of this subtitle, are corrected or erased;

2° shall ensure that access to the data and the processing opportunities is limited to what the persons acting under its authority need to perform their duties or to meet the CUTA requirements;

3° shall inform all persons acting under its authority about all the provisions of this Subtitle and about all the relevant provisions governing the protection of privacy in the context of the processing of personal data.

**Art. 150.** Where processing is entrusted to a processor, the controller shall:

1° use only a processor providing sufficient guarantees in terms of the technical and organisational security measures with regard to the processing activities;

2° ensure compliance with these measures, in particular, via contractual provisions;

3° define the responsibility of the processor in the contract;

4° agree with the processor that the latter acts on the instructions of the controller only and that the processor is subject to the same obligations the controller is bound by under this Subtitle.

5° set out the elements of the contract relating to the protection of personal data and the requirements relating to the measures referred to in the provisions sub 3° and 4° in a written document or on an electronic device.

**Art. 151.** The processor is subject to the same obligations as the controller is bound by.

Unless expressly authorised by the controller, the processor is not entitled to entrust the processing of personal data to another processor.

**Art. 152.** Except pursuant to a legal obligation, anyone acting under the authority of the controller or the processor, including the processor, who has access to personal data, can only process them on the instructions of the controller.

### Section 2. - Joint controllers

**Art. 153.** Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

The contract sets out the respective responsibilities of the joint controllers, in particular as regards the exercise of the rights of the data subject and the communication of personal data, unless their respective obligations are defined by or by virtue of a law.

The contract between the parties shall designate one contact point for data subjects. The joint controllers shall list this point of contact in the register referred to in article 156.

**Section 3. - Security of personal data**

**Art. 154.** The controller, as well as the processor, shall take the appropriate technical and organisational measures to protect personal data against accidental or unauthorised destruction, accidental loss, including against any unauthorised alteration of or access to, and against any other unauthorised processing of personal data.

These measures shall ensure an appropriate level of security, taking account, on the one hand, of the state of the art and the costs of implementation and, on the other hand, of the nature of the personal data to be protected and the potential risks.

**Art. 155.** § 1. Where a security breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate this breach to the competent supervisory authority without delay and, where feasible, not later than 72 hours after having become aware of it.

§ 2. The processor shall notify the controller of any security breach without delay.

§ 3. The notification referred to in paragraphs 1 and 2 shall, as a minimum, describe or communicate:

1° the nature of the security breach including, where possible, the approximate number of data subjects and personal data concerned;

2° the name and contact details of the data protection officer or other contact point where more information can be obtained;

3° the likely consequences of the security breach;

4° the measures taken or proposed by the controller or the processor to address the security breach, including, where appropriate, measures to mitigate its possible adverse effects.

**Section 4. - Registers**

**Art. 156.** § 1. The controller shall keep a register, classified within the meaning of the Act of 11 December 1998, of the CUTA databases and of those the controller is given access to.

This register shall contain the following information:

1° as regards the CUTA databases:

a) the contact details of the controller and, where appropriate, of the joint controllers, and of the data protection officer;

b) the purposes of the processing;

c) the categories of recipients the personal data may be communicated to;

d) insofar as possible, the envisaged time limits for erasure of the personal data;

e) insofar as possible, a general description of the technical and organisational security measures referred to in article 154;

2° as regards the databases made available to CUTA:

a) the contact details of the controller and, where possible, for the countries outside the European Union, of the agency managing the database, and, where appropriate, of the joint controllers and of the data protection officer;

b) the purposes of the processing by CUTA.

§ 2. Each processor shall keep a register, classified within the meaning of the Act of 11 December 1998, of all the categories of processing activities it carried out on behalf of the controller.

This register shall contain the following information:

1° the contact details of the processor and of the controller on behalf of whom the processor is acting, and, where appropriate, of the data protection officer;

2° the categories of processing operations carried out on behalf of the controller;

3° where possible, a general description of the technical and organisational security measures referred to in article 154;

§ 3. The registers referred to in paragraphs 1 and 2 shall be compiled in writing, including in electronic form.

§ 4. The controller shall make the register available to the competent supervisory authority, at its request.

On request, the processor shall make the register available to the controller and also to the competent supervisory authority.

**Section 5. - Data protection officer**

**Art. 157.** § 1. The controller, and, where appropriate, the processor, shall designate a data protection officer. This decision shall be communicated to the competent supervisory authority.

The data protection officer shall be the holder of a "top secret" security clearance, within the meaning of the Act of 11 December 1998.

§ 2. The data protection officer cannot be penalised for performing his tasks. Neither can he be dismissed for carrying out his duties, except if he is found guilty of serious misconduct or no longer meets the requirements necessary for the exercise of his mandate.

The data protection officer can appeal any such decision to Standing Committee I.

§ 3. He is, in an independent manner, tasked with:

1° monitoring compliance with this Subtitle throughout the processing of personal data;

2° providing advice on any useful measures designed to guarantee the security of the data stored;

3° informing and advising the controller, and, where applicable, the processor, the head of department and the staff of the department carrying out the processing of their obligations under this Subtitle;

4° issuing opinions or recommendations to the controller, and, where applicable, to the processor or the head of CUTA;

5° performing other duties entrusted to him by the controller, and, where applicable, by the processor or the head of CUTA.

The data protection officer is the contact person for the competent supervisory authority with regard to the application of this Subtitle.

§ 4. The controller and, where appropriate, the processor, shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues relating to the protection of personal data.

The controller, and, where applicable, the processor, shall see to it that the data protection officer has all the resources necessary to carry out his tasks.

The data protection officer may be assisted by one or several deputies.

§ 5. Where appropriate, the King can establish further rules on the functioning, the designation and the relevant competences.

## CHAPTER VIII. - Communication and transfer of personal data

### Section 1. - Communication of personal data to the public sector and to the private sector

**Art. 158.** By way of derogation from articles 20, 22, 23, 58 and 59 of this Act and from articles 35 and 36 of the Regulation and in the interest of the performance of the CUTA mandate, neither a protocol, nor an opinion from the data protection officer, nor a data protection impact assessment, nor the opinion following consultation with the competent supervisory authority can be a prerequisite for the exchange of personal data between CUTA and any public or private body.

This notification shall be made in accordance with articles 8 to 12 of the Act of 10 July 2006 and Chapter IV, Section 12, Subsection 7bis, of the Act of 5 August 1992 on the Police Service.

Where the parties decide to sign a protocol, the protocol shall, by way of derogation from article 20, § 1, second paragraph, contain the following:

1° the identity of CUTA and of the public or private body exchanging personal data;

2° the identity of the controllers;

3° the contact details of the relevant data protection officers;

4° the purposes for which the personal data are transferred;

5° the legal basis;

6° the restrictions to the rights of the data subject.

The protocol referred to in the third paragraph shall be marked "RESTRICTED" within the meaning of the Royal Decree of 24 March 2000 implementing the Act of 11 December 1998, where a classification within the meaning of the Act of 11 December 1998 is unjustified.

## Section 2. - Transfer of personal data to countries that are not a member of the European Union or to international organisations

**Art. 159.** Personal data can only be transferred to a country that is not a member of the European Union or to an international organisation if that country or that organisation ensures an appropriate level of protection and compliance with the other provisions of this Subtitle.

The question whether the level of protection is appropriate shall be assessed taking account of all the circumstances relating to the transfer of personal data or to a category of transfers of personal data. More specifically, account shall be taken of the nature of the data, the purpose and the duration of the intended processing, the country of origin and the country of final destination, the general and sectoral rules of law prevailing in the country in question or within the organisation, including the ethics and security measures adhered to in these countries or organisations.

An appropriate level of protection can be assured by means of security clauses between the controller and the recipient of the personal data.

**Art. 160.** By way of derogation from article 159, transfers of personal data to a country that is not a member of the European Union or to an international organisation which does not offer any guarantees in terms of an appropriate level of protection can take place only if:

1° the data subject has unambiguously given his consent to the envisaged transfer; or

2° the transfer is mandatory in the context of international relations; or

3° the transfer is essential to safeguard the vital interest of the persons; or

4° the transfer is essential or required by law to safeguard a substantial public interest or to establish, exercise or defend a right in law.

## CHAPTER IX. - Supervisory authority

**Art. 161.** Standing Committee I, in its capacity of independent public authority, and the Standing Police Monitoring Committee, shall be appointed as data protection authorities tasked with monitoring the processing of personal data by CUTA and its processors in accordance with the specific rules laid down in the Act of 18 July 1991.

## CHAPTER X. - Processing of personal data for historical, scientific or statistical purposes

**Art. 162.** By way of derogation from Title 4, consultation for historical, scientific or statistical purposes, by a subsequent controller, of personal data of CUTA and its staff shall be authorised by CUTA if it does not prejudice its mandate as referred to in the Act of 10 July 2006, an ongoing preliminary or judicial investigation, or the relations between Belgium and foreign States or international organisations and in accordance with the Act of 10 July 2006.

Each request to the State archives to further process personal data of CUTA and its members of staff for purposes other than those referred to in the first paragraph shall be refused unless the purpose is legitimate and CUTA is of the opinion that the processing cannot prejudice the interests referred to in the first paragraph.

**Art. 163.** Prior to the consultation referred to in article 162, the personal data shall be marked "Protection of personal data - Chapter X, Subtitle 4 of Title 3 of the Act of 30 July 2018".

**Art. 164.** The personal data referred to in article 162 shall be anonymised before they are consulted.

Where a further processing of anonymous data does not allow the historical, scientific or statistical purposes to be realised, CUTA may authorise the consultation of pseudonymised data.

Where anonimysation or pseudonymisation does not prevent the identification of the data, CUTA shall refuse consultation in cases where this would result in a disproportionate prejudice to privacy.

Where a further processing of pseudonymised data does not allow the historical, scientific or statistical purposes to be realised, CUTA may authorise the consultation of non-pseudonymised data in cases where this would not result in a disproportionate prejudice to privacy.

**Art. 165.** By way of derogation from Title 4, the communication or publication of non-anonymised or non-pseudonymised personal data referred to in article 162, consulted by a subsequent controller, shall invariably require the consent of CUTA and be subject to the conditions laid down by the latter.

**Art. 166.** The subsequent controller of personal data referred to in article 162 shall keep a log file of its further processing activities for historical, scientific or statistical purposes.

This log file shall be classified within the meaning of the Act of 11 December 1998 if the processing relates to classified data.

This log file shall contain the following information:

1° the contact details of the first controller, the subsequent controller and of the latter's data protection officer;

2° the purposes of the further processing;

3° the data, object of the further processing;

4° the conditions governing the further processing, if any, as defined by CUTA;

5° the recipients, if any, authorised by CUTA.

**Art. 167.** Each public authority, natural person or legal person processing personal data as referred to in article 162 for historical, scientific or statistical purposes shall be regarded as data controller.

It may not engage in activities designed to convert the anonymous or pseudonymised data into non-anonymous or non-pseudonymised data.

## SUBTITLE 5. - The protection of natural persons with regard to the processing of personal data by the Passenger Information Unit

### CHAPTER I. - Definitions

**Art. 168.** § 1. The definitions referred to in articles 26, 1° to 3°, 8°, 10° and 11°, and in article 72, § 2, 6° and 7° are applicable to this Subtitle.

§ 2. For the purposes of this Subtitle:

1° "the Act of 25 December 2016" means the Act of 25 December 2016 on the processing of passenger data;

2° "the PIUE" means the Passenger Information Unit referred to in Chapter 7 of the Act of 25 December 2016.

**CHAPTER II. - Scope**

**Art. 169.** This Subtitle applies to any processing of personal data by the PIU in the context of the purposes referred to in article 8, § 1, 4°, of the Act of 25 December 2016.

Titles 1, 2, 4, 5 and 7 of this Act are not applicable to the processing operations referred to in the first paragraph. For the purpose of Title 6, only articles 226, 227 and 230 are applicable.

**CHAPTER III. - General conditions of processing**

**Art. 170.** Personal data shall be:

1° processed lawfully and fairly;

2° collected for specific, explicitly described and legitimate purposes and not further processed in a manner that, taking account of all the relevant factors, in particular the applicable legal and regulatory provisions, is incompatible with those purposes;

3° adequate, relevant and not excessive in terms of the purposes for which they were collected or are further processed;

4° accurate and, where necessary, updated. All reasonable measures shall be taken to erase or rectify any personal data which, based on the purposes for which they were collected or are further processed, prove to be inaccurate or incomplete.

**CHAPTER IV. - Retention of personal data**

**Art. 171.** Personal data shall not be kept longer than necessary for the purposes they are stored and in accordance with the specific rules set out under Chapter 9 of the Act of 25 December 2016.

**CHAPTER V. - Rights of the data subject**

**Art. 172.** In the context of the processing of personal data relating to a natural person, every natural person has the right to the protection of his fundamental rights and freedoms, in particular to the protection of personal data relating to him.

**Art. 173.** The data subject is entitled to ask that:

1° incorrect personal data relating to him/her are corrected or erased;

2° Standing Committee I verifies compliance with the provisions of this Subtitle.

**Art. 174.** The rights referred to in article 173 shall be exercised free of charge via Standing Committee I on the initiative of the data subject who shall furnish proof of identity.

Standing Committee I shall perform the verification and shall merely inform the data subject that the necessary verifications were carried out.

The specific rules under which these rights shall be exercised are set out in the Act of 18 July 1991 governing the review of the police and intelligence services and of the Coordination Unit for Threat Assessment.

**Art. 175.** Standing Committee I and the PIU shall keep a log file of all the requests from data subjects to exercise their rights.

**Art. 176.** Decisions that give rise to legal consequences for a person cannot be taken purely on the basis of an automated processing of personal data designed to assess certain aspects of that person's personality.

## CHAPTER VI. - Obligations of the controller

### Section 1. - General obligations

**Art. 177.** The controller:

1° shall see to it that the personal data are updated; that incorrect, incomplete or irrelevant data, including data that were collected or further processed in contravention of this Subtitle, are corrected or erased;

2° shall ensure that access to the data and the processing opportunities is limited to what the persons acting under its authority need to perform their duties or to what is required to provide the service;

3° shall inform all persons acting under its authority about all the provisions of this Subtitle and about all the relevant provisions governing the protection of privacy in the context of the processing of personal data.

**Art. 178**. Except pursuant to a legal obligation, anyone acting under the authority of the controller who has access to personal data can only process them on the instructions of the controller.

### Section 2. - Security of personal data

**Art. 179.** The controller shall take the appropriate technical and organisational measures to protect personal data against accidental or unauthorised destruction, accidental loss, including against any unauthorised alteration of or access to, and against any other unauthorised processing of personal data.

These measures shall ensure an appropriate level of security, taking account, on the one hand, of the state of the art and the costs of implementation and, on the other hand, of the nature of the personal data to be protected and the potential risks.

**Art. 180.** § 1. Where a security breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate this breach to Standing Committee I without delay and, where feasible, not later than 72 hours after having become aware of it.

§ 2. The notification referred to in paragraph 1 shall, as a minimum, describe or communicate:

1° the nature of the security breach including, where possible, the approximate number of data subjects and personal data concerned;

2° the name and contact details of the data protection officer or other contact point where more information can be obtained;

3° the likely consequences of the security breach;

4° the measures proposed or taken by the controller to address the security breach, including, where appropriate, measures to mitigate its possible adverse effects.

**Section 3. - Register**

**Art. 181.** § 1. The controller shall keep a register of the passenger database referred to in Chapter 8 of the Act of 25 December 2016, on the one hand, and of the databases it has access to, on the other hand.

This register shall contain the following information:

1° as regards the aforementioned passenger database:

a) the contact details of the controller and of the data protection officer;

b) the purposes of the processing;

c) the categories of recipients the personal data may be communicated to;

d) insofar as possible, the envisaged time limits for erasure of the personal data;

e) insofar as possible, a general description of the technical and organisational security measures referred to in article 179;

2° as regards the databases made available to the PIU:

a) the contact details of the controller and, where possible, for the countries outside the European Union, of the agency managing the database, and, where appropriate, of the joint controllers and of the data protection officer;

b) the purposes of the processing by the PIU.

§ 2. The register referred to in paragraph 1 shall be compiled in writing, including in electronic form.

§ 3. The controller shall make the register available to Standing Committee I at its request.

**CHAPTER VII. - Communication and transfer of personal data**

**Art. 182.** Personal data can only be transferred to a country that is not a member of the European Union or to an international organisation if that country or that organisation ensures an appropriate level of protection and compliance with the other provisions of Chapter 12 of the Act of 25 December 2016.

The question whether the level of protection is appropriate shall be assessed taking account of all the circumstances relating to the transfer of personal data or to a category of transfers of personal data. More specifically, account shall be taken of the nature of the data, the purpose and the duration of the intended processing, the country of origin and the country of final destination, the general and sectoral rules of law prevailing in the country in question

or within the organisation, including the ethics and security measures adhered to in these countries or organisations.

An appropriate level of protection can be assured by means of security clauses between the controller and the recipient of the personal data.

**Art. 183.** By way of derogation from article 182, transfers of personal data to a country that is not a member of the European Union or to an international organisation which does not offer any guarantees in terms of an appropriate level of protection can take place only if:

1° the data subject has unambiguously given his consent; or

2° the transfer is mandatory in the context of international relations; or

3° the transfer is essential to safeguard the vital interest of the persons; or

4° the transfer is essential or required by law to safeguard a substantial public interest or to establish, exercise or defend a right in law.

**CHAPTER VIII. - Supervisory authority**

**Art. 184.** The processing of personal data as referred to in this Subtitle is subject to control by the supervisory authority referred to in article 95.

**SUBTITLE 6. - Special provisions**

**Art. 185.** § 1. Insofar as necessary in the context of the performance of their duties, the following public authorities process personal data of any nature, including those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic and biometric data, data concerning health or data concerning sexual behaviour or sexual orientation and data relating to criminal prosecutions and associated offences or security measures:

1° the administrative commission tasked with monitoring specific and exceptional methods to collect data by the intelligence and security services in the context of their mandate referred to in the Act of 30 November 1998 governing the intelligence and security services;

2° Standing Committee I in the context of its mandate referred to in the Act of 18 July 1991 governing the review of the police and intelligence services and of the Coordination Unit for Threat Assessment and in the Act of 30 November 1998 governing the intelligence and security services and in special acts;

3° Standing Committee P in the context of its mandate referred to in the Act of 18 July 1991 governing the review of the police and intelligence services and of the Coordination Unit for Threat Assessment and in special acts;

4° the Supervisory Body for Police Information Management in the context of its mandate referred to in article 71, § 1.

§ 2. To safeguard the confidentiality and effectiveness of the performance of the mandates referred to in paragraph 1, the right of a data subject to access the personal data relating to him/her shall be limited as set out in special acts.

§ 3. The data subject is free to ask to have any inaccurate data relating to him/her and processed by the authorities listed in paragraph 1 rectified or erased.

§ 4. By way of derogation from the administrative commission referred to in paragraph 1, 1°, which comes under the authority of Standing Committee I, the processing of personal data by the authorities referred to in paragraph 1 in the context of their mandate as supervisory authority shall not be subject to control by the Data Protection Authority referred to in the Act of 3 December 2017 establishing the Data Protection Authority.

## TITLE 4. - Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes referred to in article 89, §§ 2 and 3, of the Regulation

### CHAPTER I. – General provisions

**Art. 186.** This Title sets out the exemption regime with respect to the rights of data subjects referred to in article 89, §§ 2 and 3 of the Regulation.

In so far as the exercise of the rights referred to in article 89, §§ 2 and 3 of the Regulation is likely to make the achievement of the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes impossible or to seriously hinder this achievement, and as derogations are required to achieve those purposes, the derogations in question shall apply in the conditions set out in this Title.

**Art. 187.** Articles 190 to 204 do not apply, provided that a code of conduct, approved in accordance with article 40 of the Regulation, is respected.

**Art. 188.** For the purposes of this Title:

1° "trusted third party" means the natural or legal person, the de facto association or the public administration other than the controller of the processing for archiving purposes or research or statistical purposes, that pseudonymises the data;

2° "communication of data" means communication of data to identified third parties;

3° "dissemination of data" means the disclosure of data without identifying the third parties.

**Art. 189.** This Title does not apply to processing operations carried out by the authorities referred to in Title 3.

### CHAPTER II. - General safeguards

**Art. 190.** The controller shall designate a data protection officer if the processing of the personal data is likely to result in a high risk as referred to in article 35 of the Regulation.

**Art. 191.** When processing data for scientific or historical research or statistical purposes, the controller shall, prior to collection, and without prejudice to articles 24 and 30 of the Regulation, add the following elements to the record of processing activities:

1° the justification for the use of the data, whether pseudonymised or not;

2° the reasons why the exercise of the rights by the data subject is likely to make the achievement of the purposes impossible or to seriously hinder it;

3° where appropriate, the data protection impact assessment if the controller processes sensitive data, within the meaning of article 9.1 of the Regulation, for scientific or historical research or statistical purposes.

**Art. 192.** When processing data for archiving purposes in the public interest, the controller shall, prior to collection, and without prejudice to articles 24 and 30 of the Regulation, add the following elements to the record of processing activities:

1° the justification for the public interest of the stored archives;

2° the reasons why the exercise of the rights by the data subject is likely to make the achievement of the purposes impossible or to seriously hinder it.

## CHAPTER III. - Data collection

### Section 1 - Data collected from the data subject

**Art. 193.** Without prejudice to article 13 of the Regulation, any controller collecting personal data from the data subject shall inform the data subject:

1° whether or not the data will be rendered anonymous;

2° the reasons why the exercise of the rights by the data subject is likely to make the achievement of the purposes impossible or to seriously hinder it.

### Section 2. - Further processing of data

**Art. 194.** Where personal data are not collected from the data subject, the controller shall conclude an agreement with the original controller.

The first subparagraph does not apply in cases where:

1° the processing relates to personal data that were made public;

2° European Union law, a law, a decree or an ordinance:

a) gives the controller as a mandate to process personal data for archiving purposes in the public interest, scientific or historical research or statistical purposes; and

b) prohibits the reuse of the data collected for other purposes.

Where exempted from concluding an agreement, the controller shall notify the original controller of the data collection.

**Art. 195.** The agreement or notification referred to in article 194 shall contain the following elements:

1° in the event of an agreement, the contact details of the original controller and of the controller of the further processing;

2° the reasons why the exercise of the rights by the data subject is likely to make the achievement of the purpose of the further processing impossible or to seriously hinder it.

**Art. 196.** The agreement or notification concerning the data collection shall be appended to the record of processing activities.

**Art. 197.** The controller processing data for research or statistical purposes shall use anonymous data.

If it is not possible to achieve the research or statistical purpose by processing anonymous data, the controller shall use pseudonymised data.

If it not possible to achieve the research or statistical purpose by processing pseudonymised data, the controller shall use non-pseudonymised data.

**Section 3. - Anonymisation or pseudonymisation of data processed for scientific or historical research purposes or statistical purposes**

**Art. 198.** When processing data for scientific or historical research purposes or statistical purposes, based on data collected from the data subject, the controller shall anonymise or pseudonymise the data once they have been collected.

**Art. 199.** When the processing of data for scientific or historical research purposes or statistical purposes is carried out by a controller of the further processing which is the same as the controller of the original processing, the controller shall anonymise or pseudonymise the data before the further processing.

**Art. 200.** The controller is only entitled to de-pseudonymise the data if it is necessary for the research or the statistical purposes, and, where applicable, after consulting the data protection officer.

**Art. 201.** Without prejudice to special provisions, when the processing of data for scientific or historical research purposes or statistical purposes is carried out by a controller other than the original controller, the original controller shall anonymise or pseudonymise the data before communicating them to the controller tasked with the further processing.

The controller of the further processing shall not have any access to the pseudonymisation keys.

**Art. 202.** § 1. Without prejudice to special provisions, when the processing of data for scientific or historical research purposes or statistical purposes combines several original processing activities, the controllers of the original processing activities shall have the data anonymised or pseudonymised by one of the controllers of the original processing or by a trusted third party before communicating them to the controller tasked with the further processing.

§ 2. Without prejudice to special provisions, when the processing of data for scientific or historical research purposes or statistical purposes combines several original processing activities, of which at least one concerns sensitive data, the controllers of the original processing activities shall have the data anonymised or pseudonymised by the controller of the original processing of sensitive data or by a trusted third party before communicating them to the controller tasked with the further processing.

Only the controller of the original processing who pseudonymised the data or the trusted third party shall have access to the pseudonymisation keys.

**Art. 203.** The trusted third party shall:

1° be bound by professional secrecy within the meaning of article 458 of the Penal Code, subject to other provisions of this Act and of the Regulation;

2° act independently from the controller of the original processing and of the further processing.

**Art. 204.** Where a data protection officer was designated in accordance with article 190, the latter shall issue opinions on the use of the various pseudonymisation and anonymisation methods, in particular on their effectiveness in terms of data protection.

### Section 4. - Dissemination of data processed for archiving purposes in the public interest, for scientific or historical research or statistical purposes

**Art. 205.** Without prejudice to European Union law, special acts, ordinances or decrees imposing more stringent conditions on the dissemination of data processed for archiving purposes in the public interest, for scientific or historical research or statistical purposes, the controller shall not disseminate any non-pseudonymised data, unless:

1° the data subject has given his consent; or

2° the data were made public by the data subject in person; or

3° the data are closely linked to the public or historical nature of the data subject; or

4° the data are closely linked to the public or historical nature of facts in which the data subject was involved.

**Art. 206.** Without prejudice to European Union law, special acts, ordinances or decrees imposing more stringent conditions on the dissemination of data processed for archiving purposes in the public interest, for scientific or historical research or statistical purposes, the controller can disseminate pseudonymised data, with the exception of the personal data referred to in article 9.1 of the Regulation.

### Section 5. - Communication of data processed for archiving purposes in the public interest, for scientific or historical research or statistical purposes

**Art. 207.** Without prejudice to European Union law, special acts, ordinances or decrees imposing more stringent conditions on communication, the controller, who communicates non-pseudonymised data to an identified third party for the purposes referred to in article 89 of the Regulation, shall ensure that the identified third party is unable to reproduce the data communicated, except in a handwritten form, in cases where:

1° it concerns personal data as referred to in articles 9.1 and 10 of the Regulation; or

2° the agreement between the controller of the original processing and the controller of the further processing forbids it; or

3° any such reproduction may compromise the safety of the data subject.

**Art. 208.** The obligation as referred to in article 207 does not apply when:

1° the data subject has given his consent; or

2° the data were made public by the data subject in person; or

3° the data are closely linked to the public or historical nature of the data subject; or

4° the data are closely linked to the public or historical nature of facts in which the data subject was involved.

## TITLE 5. - Remedies and representation of data subjects

### CHAPTER I. - Injunctions

**Art. 209.** Without prejudice to any other judicial, administrative or extra-judicial remedy, the president of the court of first instance, sitting as in proceedings for interim measures, shall establish the existence of a processing activity that infringes the legal and regulatory provisions on the protection of natural persons with regard to the processing of their personal data and impose an injunction.

The president of the court of first instance, sitting as in proceedings for interim measures, shall take cognizance of any request relating to the right of obtain communication of personal data, granted by or under the law, as well as of any request to have any inaccurate personal data rectified, deleted or to prohibit the use of inaccurate personal data or personal data which, given the purpose of the processing, are incomplete or irrelevant, or which cannot be registered, communicated or stored or in respect of which the data subject objected to their processing or which are kept beyond the authorised time limit.

**Art. 210.** However, once the processing referred to in article 209 concerns personal data processed in the course of a preliminary investigation, a judicial investigation, criminal proceedings before the judge ruling on the merits or proceedings to enforce a judgment under criminal law, the decision on the rectification, erasure of prohibition to use personal data, or the restriction of processing shall, depending on the stage of the proceedings, exclusively rest with the Public Prosecutor's Office or to the competent criminal judge.

**Art. 211.** § 1. The action for an injunction shall be lodged on the basis of contradictory request, in accordance with articles 1034ter to 1034sexies of the Judicial Code.

§ 2. By derogation from article 624 of that same Code, the action can, at the applicant's choice, be brought before the president of the court of first instance for:

1° the domicile or the place of residence of the applicant, if the applicant or at least one of the applicants is the data subject;

2° the domicile, place of residence, registered office or place of establishment of the defendant or one of the defendants;

3° the place or one of the places where all or part of the processing activities take place.

Where the defendant does not have his domicile, place of residence, registered office or place of establishment in Belgium, the action shall be brought before the president of the court of first instance in Brussels.

§ 3. Actions based on article 209 shall be filed by:

1° the data subject;

2° the competent supervisory authority.

**Art. 212.** Subject to the application of provisions to the contrary in international treaties in force in Belgium or under European Union law, and without prejudice to their international jurisdiction on the basis of the Code of Private International Law, the Belgian courts shall in any event have international jurisdiction with regard to the actions referred to in article 209 of this Act filed against:

1° a controller or processor established or with an establishment on the Belgian territory, as regards any processing of personal data in the context of the activities of that establishment, irrespective of where the processing takes place;

2° a controller or processor who is not established or does not have an establishment on the Belgian territory, as regards any processing activities that have an impact on or are wholly or partly directed at data subjects based on the Belgian territory.

**Art. 213.** The ruling shall be notified to the competent supervisory authority within eight days of its delivery.

Furthermore, the clerk of the court where an appeal was lodged against the ruling referred to in the first subparagraph shall notify the competent supervisory authority without undue delay.

**Art. 214.** If required by the nature of the infringement, the president of the court of first instance may grant a period of grace to put an end to the infringement. He can lift the injunction when the infringement has come to an end.

**Art. 215.** The president of the court of first instance may authorise that his judgment or his summary thereof is posted for a period determined by him, both inside and outside the premises concerned, and can order, in any way he deems suitable, that his ruling or the summary thereof is published in newspapers or publicised in any other way, the foregoing at the expense of the unsuccessful party.

However, the publication measures referred to in the first subparagraph shall be authorised only if they are likely to put an end to the challenged act or its effects.

**Art. 216.** Following the action referred to in article 209, the applicant may sue for damages in pursuance of contractual or extra-contractual liability law.

**Art. 217.** If the inaccurate, incomplete or irrelevant personal data or personal data whose retention was forbidden were communicated to third parties, or if the communication of personal data took place after their authorised retention period, the president of the court of first instance can order the controller, the processor, the recipient or their representative to notify the third parties in question of the restriction of processing or the rectification or erasure of the personal data concerned.

**Art. 218.** If there are compelling reasons to fear that evidence that can be used in support of an action provided for in this Chapter may be concealed, disappear or made inaccessible, the president of the court of first instance shall, on the basis of an ex parte application, impose any measure to prevent such concealment, disappearance or inaccessibility.

**Art. 219.** Without prejudice to article 210, the provisions of this Chapter do not limit the competence of the court of first instance or of the president of the court of first instance sitting in proceedings for interim measures.

**CHAPTER II. - Representation of data subjects**

**Art. 220.** § 1. The data subject is entitled to instruct a body, an organisation or a non-profit association to lodge a complaint on his behalf and to seek administrative or legal redress on his behalf, be it with the competent supervisory authority, the judiciary, as defined in the special acts, the Judicial Code and the Code of Criminal Procedure.

§ 2. In the case of litigation as referred to in paragraph 1, the body, organisation or non-profit association shall:

1° be validly set up in accordance with Belgian law;

2° have legal personality;

3° have legal objectives of public interest;

4° have been involved in the protection of the rights and freedoms of data subjects in the context of the protection of personal data for a minimum of three years.

§ 3. The body, organisation or non-profit association shall prove, on the basis of its activity reports or any other document, that it has been effectively involved in this activity for a minimum of three years, that this activity is consistent with its corporate purpose and that it relates to the protection of personal data.

## TITLE 6. - Penalties

### CHAPTER I. - Administrative penalties

**Art. 221.** § 1. The corrective powers of the supervisory authority by virtue of article 58.2 of the Regulation also apply to articles 7 to 10, 20 to 24, 28 to 70 of Title 2 and to Title 4 of this Act.

Without prejudice to specific provisions, the first paragraph does not apply to processing activities by the competent authorities referred to in article 26, 7°, b) carried out in the performance of their judicial capacity.

§ 2. Article 83 of the Regulation does not apply to the public authorities or their attendants or authorised representatives, unless it concerns legal persons governed by public law who offer products and services on a market.

### CHAPTER II. - Criminal penalties

**Art. 222**. The controller or the processor, its attendant or authorised representative, the competent authority, as referred to in Titles 1 and 2, shall be punishable by means of a fine of two hundred and fifty to fifteen thousand euro in cases where:

1° the personal data are processed without legal basis in accordance with article 6 of the Regulation and articles 29, § 1, and 33, § 1, of this Act, including the conditions for consent and further processing;

2° the personal data are processed in contravention of the conditions imposed by article 5 of the Regulation and article 28 of this Act, whether through gross negligence or maliciously;

3° the processing objected to pursuant to article 21.1 of the Regulation continues without compelling legal reasons;

4° the transfer of personal data to a recipient in a third country or to an international organisation is made in contravention of the safeguards, conditions or exceptions provided for in articles 44 to 49 of the Regulation or articles 66 to 70 of this Act, whether through gross negligence or maliciously;

5° the corrective measure to temporarily or definitively restrict flows in accordance with article 58.2.f) of the Regulation imposed by the supervisory authority is disregarded;

6° the corrective measure within the meaning of article 58.2.d) of the Regulation imposed by the supervisory authority is disregarded;

7° the legal mandate of verification and control of the competent supervisory authority, its members or experts were hampered;

8° rebellious acts, within the meaning of article 269 of the Criminal Code, were committed against the members of the supervisory authority;

9° certification, as referred to in article 42 of the Regulation, is claimed or data protection seals are used publicly, even though the certifications, seals or marks were not issued by an accredited body or are used after the validity of the certification, seal or mark has expired;

10° the certification referred to in article 42 of the Regulation was obtained on the basis of forged documents or incorrect documents;

11° tasks are carried out in the capacity of a certification body, even though that body was not accredited by the competent national accreditation body;

12° the certification body does not conform to the principles and tasks it is subject to, as referred to in articles 42 and 43 of the Regulation;

13° the tasks of the body referred to in article 41 of the Regulation are carried out without accreditation from the competent supervisory authority;

14° the accredited body referred to in article 41 of the Regulation did not take the appropriate measures in cases where the code of conduct, as referred to in article 41.4 of the Regulation, was infringed.

**Art. 223**. Shall be penalised by means of a fine of five hundred euro to thirty thousand euro, the controller referred to in Title 1, the processor or the person acting under their authority, who:

1° whether through personal negligence, provided it can be qualified as serious, or maliciously, failed to inform the data subject of the existence of personal data relating to him or her that originated from an authority referred to in Title 3 in contravention of article 11, while he was aware of the origin of the information and did not find himself in one of the situations referred to in article 11, § 2, first paragraph, 1° or 2°;

2° whether through personal negligence, provided it can be qualified as serious, or maliciously, informed the data subject that an authority referred to in Title 3 is the recipient of one of his personal data in contravention of article 12.

**Art. 224**. Shall be penalised by means of a fine of two hundred euro to ten thousand euro any member or member of staff of the competent supervisory authority or any expert who breached the confidentiality obligation incumbent on him.

**Art. 225**. When the court sentences on the grounds of an offence described in articles 222 or 223, it may order that the judgment is published, in full or by extract, in one or several newspapers as specified by the court, at the expense of the convicted party.

**Art. 226.** Any controller or person acting under the authority of the authority referred to in Title 3 or his processor, who, through personal negligence, provided it can be qualified as serious, or maliciously, failed to abide by one of the obligations concerning confidentiality and security referred to in articles 83 to 86, 116 to 119, 149 to 152, 177 and 178 shall be penalised by means of a fine of one hundred euro to ten thousand euro.

**Art. 227.** Shall be penalised by means of a fine of one hundred euro to twenty thousand euro:

1° any controller, processor, person acting under the authority of the authority referred to in Title 3 or of the processor or the attendant who, through personal own negligence, provided it can be qualified as serious, or maliciously, processes personal data in circumstances other than those referred to in articles 74, 108, 140 and 170;

2° any controller, processor or attendant processing personal data in contravention of the conditions for processing imposed by articles 75, 109, 141 and 170 and any person acting under the authority of the authority referred to in Title 3 or its processor, who through personal negligence, provided it can be qualified as serious, or maliciously, processes data in contravention of the conditions imposed by articles 75, 109, 141 and 170;

3° anyone who, with a view to extracting the data subject's consent to the processing of personal data relating to him or her, uses matters of fact, violence, threats, gifts or promises;

4° anyone who, through personal negligence, provided it can be qualified as serious, or maliciously, transfers, forces or facilitates the transfer of personal data to a country that is not a member of the European Union or to an international organisation without the requirements imposed by articles 93, 94, 126, 127, 159, 160, 182 and 183 having been met;

5° any person who, through personal negligence, provided it can be qualified as serious, or maliciously, gives access to the personal data referred to in articles 99, 132 and 162 for historical, scientific or statistical purposes and processes those data in contravention of articles 102, 104, 135, 137, 165 or 167.

**Art. 228.** Without prejudice to specific provisions, the controller, the processor, or its representative in Belgium shall be liable for the payment of the fines his attendant or authorised representative are ordered to pay.

**Art. 229.** § 1. With regard to the infringements referred to in articles 222 and 223, the competent supervisory authority and the Attorney-General's Office can sign a protocol setting out the working arrangements between the supervisory authority and the Public Prosecutor's Office with regard to files relating to facts where the law provides for both an administrative fine and a criminal penalty.

The King, by decree deliberated on in the Council of Ministers, establishes the further rules and the template for this protocol agreement.

This protocol shall be fully consistent with all the legal provisions and shall in particular deal with the procedures applicable to offenders without disregarding the rights of the offenders.

The protocol shall be published in the Belgian Official Journal and on the website of the competent supervisory authority.

§ 2. In the absence of a protocol and in respect of the infringements referred to in articles 222 and 223, the public prosecutor has a period of two months, as of the date the original report is received, to notify the competent supervisory authority that a preliminary investigation or judicial investigation has been launched or prosecutions were initiated. This notification removes the possibility for the supervisory authority to exercise its corrective powers.

The competent supervisory authority cannot impose any penalties until that term has passed. Failing notification by the public prosecutor within two months, the facts shall be subject to administrative penalties only.

**Art. 230.** All the provisions of Book I of the Criminal Code, including Chapter VII and article 85, are applicable to the infringements described in this Act or its implementing decrees.

## TITLE 7. - Supervisory Body for Police Information Management

### CHAPTER I. - Composition and status of the members and of the investigations unit

**Art. 231.** § 1. The Supervisory Body for Police Information Management, hereinafter referred to as the "Supervisory Body" is composed of three active members, one of whom the chairman, who carry out their functions on a full-time basis. Aside from the chairman, who shall be a magistrate, the supervisory authority is composed of a magistrate of the Public Prosecutor's Office and an expert.

Except for one of the members who is functionally bilingual, the Supervisory Body seats an equal number of Dutch-speaking and French-speaking members. The members have a functional knowledge of the second national language and of English. At least one of the members also has a functional knowledge of German. They are all appointed by the Chamber of Representatives who can also terminate their mandate when they no longer fulfil the conditions set out in article 232 or on serious grounds. Their mandate cannot be revoked for opinions expressed or actions taken in discharge of their duties.

§ 2. The members of the Supervisory Body are appointed by the Chamber of Representatives on the basis of their competence, their experience, their independence and their moral authority for a, one-time renewable, term of six years.

This term starts to run once they have been sworn in. At the end of this term, the members remain in office until their successor has been sworn in.

The members are not allowed to hold a public mandate conferred on them on the basis of the electoral process. They are not entitled to exercise a public or private function or role that could adversely reflect on the independence or the dignity of the office or that is incompatible with their office.

§ 3. Before taking up office, the members of the Supervisory Body shall take the oath prescribed under article 2 of the Decree of 20 July 1831 before the president of the Chamber of Representatives.

§ 4. Furthermore, the Supervisory Body is also composed of an investigations unit, hereinafter referred to as the "investigations unit", seating three active members who carry out their functions on a full-time basis, among whom two members of the police services within the meaning of article 2, 2°, of the Act of 7 December 1998 organising an integrated police service structured at two levels.

The investigations unit is exclusively subordinate to the Supervisory Body. The Supervisory Body is in charge of the investigations unit, assigns its tasks and receives a report on all the assignments carried out.

§ 5. The members of the investigations unit are appointed by the Supervisory Body which can also terminate their mandate when they no longer fulfil the conditions set out in article

232 or on serious grounds. The members of the investigations unit are appointed for a renewable term of six years, on the basis of their competence.

§ 6. Before taking up office, the members of the investigations unit take the oath prescribed under article 2 of the Decree of 20 July 1831 before the chairman of the Supervisory Body.

**Art. 232.** § 1. At the time of their appointment, the members of the Supervisory Body must meet the following conditions:

1° Belgian citizenship;

2° full civil and political rights;

3° irreproachable behaviour;

4° proof of expertise in the field of the protection of personal data and police information management;

5° holder of a "top secret" security clearance granted in accordance with the Act of 11 December 1998 on classification and security clearances, security certificates and security recommendations;

6° not holding a function in a policy cell of a federal or regional minister.

§ 2. At the time of their appointment, the chairman and the magistrate of the Public Prosecutor's Office must have a minimum of ten years' relevant experience or expertise in the field of the protection of personal data and police information management.

§ 3. At the time of his appointment, the member-expert of the Supervisory Body must meet the following specific conditions:

1° ten years' experience in the field of the protection of personal data and police information management;

2° holder of a Bachelor's or Master's in laws that gives access to public sector posts, level A.

§ 4. Where, for whatever reason, the mandate of a member of the Supervisory Body becomes vacant, a replacement shall be appointed for the remaining term of the mandate.

§ 5. At the time of their appointment, the members of the investigations unit must meet the following conditions:

1° Belgian citizenship;

2° full civil and political rights;

3° irreproachable behaviour;

4° proof of expertise in the field of the protection of personal data and police information management;

5° holder of a "top secret" security clearance granted in accordance with the Act of 11 December 1998 on classification and security clearances, security certificates and security recommendations;

6° not holding a function in a policy cell of a federal or regional minister.

§ 6. At the time of their appointment, the members of staff of the police service who are members of the investigations unit must meet the following specific conditions:

1° not less than ten years' seniority and, as a minimum, holding the rank of police commissioner, level A, if the member of staff held an administrative or logistical management position;

2° not having received a performance review rated "unsatisfactory" during the five years that precede the submission of their application and not having been the subject of serious disciplinary action that remains to be expunged;

3° a minimum of two years' experience in the processing of police information or the protection of personal data.

§ 7. At the time of their appointment, the experts of the investigations unit must meet the following specific conditions:

1° five years' experience in the field of the protection of personal data and police information management;

2° holder of a Bachelor's or Master's in laws that gives access to public sector posts, level A.

**Art. 233.** § 1. The Supervisory Body sets its rules of procedure and can determine its internal organisation. The rules of procedure shall be submitted to the Chamber of Representatives for approval.

With due regard for the principles of collegiality, the chairman chairs the meetings of the Supervisory Body and ensures the daily management of the activities. He sees to the proper functioning of the Supervisory Body, to the proper execution of its tasks and to the application of the rules of procedure. The aforesaid rules of procedure set out which member assumes the tasks of chairman when the latter is absent or unavoidably detained.

§ 2. Within the limits of their powers, the members of the Supervisory Body do not receive or ask for instructions, whether directly or indirectly, from anyone. They are not allowed to attend deliberations or to be present when a decision on files which they have a direct personal interest in is taken or which their blood relatives or relatives by affinity up to the fourth degree have a direct interest in.

§ 3. The members of the Supervisory Body and its members of staff do not bear any civil liability for their decisions, actions or conducts while performing the legal tasks of the supervisory authority except in the event of fraud or gross negligence.

§ 4. For the duration of their mandate and contract and thereafter, the members of the Supervisory Body are bound by secrecy with regard to the facts, actions or information that came to their attention in the course of their duties. Any breach of professional secrecy is penalised in accordance with article 458 of the Criminal Code.

**Art. 234.** § 1. The members of the Supervisory Body enjoy the same status as the councillors at the Court of Auditors. The pay scheme of the councillors of the Court of Auditors, contained in the Act of 21 March 1964 concerning the salaries of the members of the Court of Auditors, as amended by the Acts of 14 March 1975 and 5 August 1992, is applicable to the members of the Supervisory Body. Their thus far acquired pecuniary seniority is taken into account and they are also entitled to interim increases within this scale.

The members of the investigations unit are paid a salary in accordance with scale A3 of the staff regulations of the officials of the Data Protection Authority established by the Act of 3 December 2017 establishing the Data Protection Authority. Their thus far acquired pecuniary seniority is taken into account and they are also entitled to interim increases within this scale. They qualify for all the pecuniary advantages provided for in the staff regulations of the officials of the Data Protection Authority.

The members of the Supervisory Body and the members of the investigations unit qualify for the pension scheme applicable to civil servants. These pensions are covered by the exchequer. In terms of their pension, the mandate of the members of the Supervisory Body and of the investigations unit is considered to be equivalent to a permanent appointment.

§ 2. At the end of their mandate within the supervisory authority, the members of the investigations unit who are also a member of the police services can return to their original corps and enjoy the same status as they had when they were appointed to the Supervisory Body. During their mandate, they retain their rights to promotion and pay increase at the service or the administration they came from. Any member of the police services who is also a member of the investigations unit, and who applies for a position with the police services and is deemed suitable for a position with the police services, shall enjoy priority over any other applicants for the same position, even if the latter enjoy priority by law. This priority shall apply during the final year of the six-year term at the Supervisory Body.

Under the same conditions, a priority term of two years is granted at the start of the tenth year in the employment of the Supervisory Body.

§ 3. Members of the Supervisory Body who are a magistrate of the judiciary, a public servant or a member of the police services are granted leave to take up a post in the public interest for the duration of their mandate. Throughout their mandate at the Supervisory Body or the investigations unit, they retain their rights to promotion and pay increase at the service or administration they came from.

**Art. 235.** § 1. The Supervisory Body has its own secretariat consisting of an executive assistant, a lawyer and an IT specialist. These members of staff are paid as follows, in accordance with the staff regulations for officials of the federal public service:

- Executive assistant: scale A1

- Lawyer: scale A3

- IT specialist: scale A3

They are hired by the Supervisory Body which is free to avail of the services of a HR management expert.

§ 2. The secretariat and its staff work under the authority of the members of the Supervisory Body and the daily management of the chairman of the Supervisory Body.

**CHAPTER II. – Tasks**

**Art. 236.** § 1. The Supervisory Body is entrusted with the tasks set out in article 71, § 1, third paragraph, 1° to 3°.

§ 2. The Supervisory Body provides advice, either of its own accord, or at the request of the government or of the Chamber of Representatives, of an administrative or judicial authority,

on any matter relating to police information management, as stipulated, inter alia, in Section 12 of Chapter 4 of the Act of 5 August 1992 on the Police Service.

The Supervisory Body issues its opinion within sixty days of the necessary information having been communicated to the supervisory authority. The opinions of the Supervisory Body are substantiated. The Supervisory Body issues its opinion to the relevant authority.

In cases where the opinion of the Supervisory Body is required by virtue of a provision of this Act in urgent and duly justified cases, the term referred to in the second paragraph is reduced to a minimum of fifteen days.

§ 3. In the context of the mandate provided for in article 71, § 1, third paragraph, 3°, the Supervisory Body is in particular tasked with monitoring compliance with the rules governing the communication of information and personal data stored in the police databases, direct access to the General National Database and the technical databases and direct searches in these databases, including compliance with the obligation referred to in article 44/7, third paragraph, of the Act of 5 August 1992 on the Police Service, incumbent on all the members of the police services, to feed this database.

**Art. 237.** The Supervisory Body acts of its own motion, at the request of the Data Protection Authority referred to in article 2, 1°, of the Act of 3 December 2017 establishing the Data Protection Authority, of the judicial or administrative authorities, of the Minister for Justice, the Minister for the Interior, the minister with responsibility for privacy or of the Chamber of Representatives.

In cases where the Supervisory Body acts of its own motion, it shall notify the Chamber of Representatives without delay.

Where an audit takes place at local police level, the Supervisory Body notifies the local mayor or the police board and sends them its report.

Where the audit concerns information and personal data relating to the exercise of the tasks of the judicial police, the report compiled by the Supervisory Body shall also be forwarded to the competent magistrate of the Public Prosecutor's Office.

**Art. 238.** The Supervisory Body reports to the Chamber of Representatives in any one of the following cases:

1° annually, on the basis of a general activity report which, where necessary, contains general conclusions and proposals and which covers the period from 1 January to 31 December of the previous year. This report is transmitted to the president of the Chamber of Representatives on 1 June at the latest and to the competent ministers referred to in article 237, first paragraph;

2° any time it deems useful or at the request of the Chamber of Representatives, on the basis of an interim activity report on specific investigation files which, where necessary, may contain general conclusions and proposals. This report is forwarded to the president of the Chamber of Representatives and to the competent ministers referred to in article 237, first paragraph;

3° whenever it is entrusted with a task by the Chamber of Representatives;

4° whenever it has established that, on expiry of a term it deems reasonable, its conclusions were disregarded or that the measures taken are unsuitable or inadequate. In this particular case, a term of no less than sixty days applies.

**Art. 239**. § 1. On the basis of an investigation into their functioning, the Supervisory Body checks whether the content of the General National Database, the basic databases, the special databases and the technical databases, including the procedure for processing the data and information stored therein, are consistent with the provisions of articles 44/1 up to and including 44/11/13 of the Act of 5 August 1992 on the Police Service and its implementing measures.

§ 2. The Supervisory Body shall in particular check the regularity of the following processing activities in the General National Database, the basic databases, the special databases and the technical databases:

1° the evaluation of the data and information;

2° the registration of the data and information;

3° the validation of the data and information by the relevant competent authorities;

4° the collection of the data and information on the basis of concreteness or reliability;

5° the erasure and archiving of data and information once the retention period has expired.

§ 3. The Supervisory Body in particular checks the true nature of the following functionalities and processing activities prescribed by the competent police authorities:

1° the relationships between the categories of data and information recorded at the time of collection;

2° receipt of the data and information by the authorities and the services authorised to consult them by law;

3° communication of the data and information to the statutorily authorised authorities and services;

4° the connection with other data-processing systems;

5° the special rules governing the collection of data and information on the basis of appropriateness, relevance, necessity and concrete reliability.

**Art. 240.** The Supervisory Body:

1° raises citizens' awareness of and fosters greater understanding of the risks, rules, safeguards and the rights relating to the processing of personal data by the services listed in article 26, 7°, a), d), and f);

2° familiarises controllers and processors with their legal obligations relating to the processing of personal data;

3° on request, furnishes any data subject with information about the exercise of his or her rights under this Act and, where appropriate, cooperates with the supervisory authorities in other Member States to facilitate this. Requests from another supervisory authority are acted on without undue delay and in any case within thirty days of receipt;

4° deals with complaints, examines the content of the complaint to the extent necessary and notifies the complainant within a reasonable period of time of the progress and the result of the investigation, in particular if further investigation or coordination with another supervisory authority is required. The Supervisory Body may decide not to act on complaints or reports that are manifestly unfounded.

5° compiles a list of the type of processing activities requiring a data protection impact assessment, in accordance with article 35.4 of the Regulation, and keeps that list up to date;

6° promotes the drafting of codes of conduct pursuant to article 40.1 of the Regulation, issues opinions and, in accordance with article 40.5 of the Regulation, approves codes of conduct that provide sufficient safeguards;

7° promotes the introduction of data protection certification mechanisms and data protection seals and marks, and approves the certification criteria pursuant to article 42 of the Regulation;

8° where applicable, periodically checks the certifications issued;

9° compiles and publishes the accreditation criteria for a body that monitors compliance with the codes of conduct pursuant to article 41 of the Regulation, and of certification body pursuant to article 43 of the Regulation;

10° ensures the accreditation of a body monitoring compliance with the codes of conduct and of a certification body.

**Art. 241.** The Supervisory Body can delegate one or more of its members, members of the investigations unit or its staff, to represent the Supervisory Body on committees or in groups it, in its capacity of supervisory authority of the police sector, is required or chooses to participate in.

**Art. 242.** The Supervisory Body may conduct a broad public inquiry or engage in wide public consultation or conduct a more targeted inquiry or engage in more targeted consultation into/with the representatives of the police sector.

**Art. 243.** § 1. The Supervisory Body carries out the international obligations ensuing from the mandates and competences it is vested with by law. These obligations may entail that the Supervisory Body cooperates with any other body or other data protection authority of another State by using the competences it is vested with pursuant to the applicable legislation.

This cooperation can relate to:

1° the introduction of expertise pools;

2° the exchange of information;

3° mutual assistance in the context of control measures;

4° the sharing of human and financial resources.

The cooperation can be formalised in the form of cooperation agreements.

§ 2. In that context, the Supervisory Body is authorised to appoint some of its members, members of the investigations unit or members of staff, as representatives to international authorities.

## CHAPTER III. - Competences of the Supervisory Body, its members and the members of the investigations unit

**Art. 244.** § 1. The Supervisory Body, its members and the members of the investigations unit have unlimited access to any information and data processed by the services referred to in article 26, 7°, a), d), and f), and in particular the police services pursuant to article 44/1 to 44/11/13 of the Act of 5 August 1992 on the Police Service, including the information and data stored in the General National Database, the basic databases, the special databases, the technical databases and the international databases fed by the Belgian police services.

The police services shall, of their own accord, provide the Supervisory body with the regulations and internal guidelines relating to the processing of personal data and any police information they deem necessary to allow the Supervisory Body to fulfil its tasks. The Supervisory Body and the investigations unit are entitled to requisition any documents they deem necessary to allow them to fulfil their task.

The Supervisory Body, its members or the members of the investigations unit are authorised to carry out on-the-spot investigations. To that effect, they have an unlimited right of access to the premises where the information and data referred to in the first paragraph are processed and for the duration of the processing.

§ 2. They have the authority to confiscate any objects, documents and data of a computer system they deem necessary at those premises unless they relate to an ongoing preliminary or judicial investigation.

Where the commissioner of police or his deputy is of the opinion that the confiscation may put a person in physical danger, the matter shall be submitted for decision to the chairman of the Supervisory Body or to the magistrate deputising for the latter. The objects and documents confiscated shall be listed in a special register.

§ 3. The members of the Supervisory Body and the investigations unit can make any useful findings anywhere.

Where required in the context of its tasks, the Supervisory Body or its members can request the assistance of the police.

§ 4. The Supervisory Body, its members or the members of the investigations unit can impose mandatory deadlines for reply on the members of the federal or local police whom they address questions to in the discharge of their duties.

§ 5. For the purposes of the exercise of the supervision organised by this Act, the Supervisory Body shall have access to the information of article 3, first paragraph, 1° to 6°, 9° and 9° /1, and second paragraph of the Act of 8 August 1983 establishing a National Register of natural persons.

For the purpose of exercising this supervision, the Supervisory Body can use national registry numbers.

**Art. 245.** § 1. Without prejudice to the legal provisions on the immunity and prerogatives of the judiciary, the members of the Supervisory Body and of the investigations unit can invite anyone they deem necessary for questioning. The members or the former members of the police services are obliged to comply with any written convocation.

The members or former members of the police services may make statements about facts covered by professional secrecy.

§ 2. The chairman of the Supervisory Body can summon members or former members of the police services through the intermediary of a judicial officer. These members or former members shall testify once they have taken the oath stipulated in article 934, second paragraph, of the Judicial Code.

The members or former members of the police services shall disclose any secrets they have knowledge of to the Supervisory Body, unless they relate to an ongoing preliminary or judicial investigation.

Where a member or former member of the police service is of the opinion that he is unable to disclose a secret he has knowledge of because its disclosure may put someone in physical danger, the matter shall be submitted for decision to the chairman of the Supervisory Body or the magistrate deputising for the latter.

Where a member or former member of the police service is of the opinion that he is unable to disclose a secret he has knowledge of, the matter shall be submitted for decision to the commissioner-general or to the commanding officer of the police service with jurisdiction over the data subject.

§ 3. The Supervisory Body may request the assistance of experts and interpreters. They shall take the oath referred to in article 290 of the Code of Criminal Procedure. Their fees are settled in accordance with the rate of the legal expenses in criminal matters.

§ 4. Article 9 of the Act of 3 May 1880 on parliamentary inquiries is applicable to the members or former members of the police services interviewed as witnesses or summoned by the Supervisory Body and to the experts and interpreters summoned.

The reports recording the infringements committed shall be compiled by a member of the Supervisory Body or by a member of the investigations unit and forwarded to the public prosecutor in whose jurisdiction they were committed.

Any member or former member of the police services who refuses to testify before the Supervisory Body and refuses to lend his cooperation is subject to a prison sentence of one month to two years and a fine of one hundred euro to one thousand euro or by one of these penalties only.

**Art. 246.** Without prejudice to article 44/1 of the Act of 5 August 1992 on the Police Service, all the State services, including the public prosecutor's offices and all court registries, the provinces, the municipalities, the associations they form part of, the public institutions subordinate to them, are obliged to, on request, provide the Supervisory Body, its members or the members of the investigations unit with any information the latter deem useful to monitor compliance with the legislation within their remit, to hand over any data mediums for inspection and to provide copies thereof in whatever form.

Any information that forms part of an ongoing preliminary or judicial investigation shall be submitted subject to the prior consent of the competent public prosecutor's office only.

**Art. 247.** The Supervisory Body decides on the course of action to be taken on any complaints within the meaning of article 240, first paragraph, 4°, and has the authority to:

1° decide that processing was performed in accordance with the provisions of the regulations on the processing of personal data;

2° warn the services referred to in article 26, 7°, a), d) and f), or their processor, that the intended processing of personal data may infringe the regulations on the processing of personal data;

3° reprimand the services referred to in article 26, 7°, a), d) and f), or their processor, if the processing of personal data resulted in a breach of a provision of the regulations on the processing of personal data;

4° instruct the services referred to in article 26, 7°, a), d) and f), or their processor, to bring a processing activity into line with the provisions of the regulations on the processing of personal data, where appropriate, in a certain manner and by a certain deadline.

5° impose a temporary or definitive processing restriction, including a processing ban;

6° order the rectification or erasure of personal data;

7° forward the file to the competent public prosecutor's office which shall notify it of the action taken in relation to the file;

8° withdraw a certification referred to in article 240 or instruct the certification body to withdraw a certification issued, or instruct the certification body not to issue a certification;

9° instruct the services referred to in article 26, 7°, a), d) and f), or their processor, to notify the data subject of a personal data breach.

**Art. 248.** § 1. The Supervisory Body shall notify the parties of its decision and of the option to lodge an appeal with the court of appeal for the place of residence or the registered office of the complainant within thirty days as of the notification of the decision.

Subject to the legal exemptions or unless the Supervisory Body, by reasoned decision, rules otherwise, the decision shall be provisionally enforceable, notwithstanding any appeal.

§ 2. Decisions of the Supervisory Body taken on the basis of article 247, 1°, 3°, 4°, 5°, 6°, 8° or 9° can be appealed before the court of appeal for the place of residence or the registered office of the complainant, which shall deal with the case as in proceedings for interim measures in accordance with articles 1035 to 1038, 1040 and 1041 of the Judicial Code.

**Art. 249.** The Supervisory Body shall notify the service referred to in article 26, 7°, a), d) and f) of the investigations it conducted into the processing of personal data by its processors and of the results.

Where infringements of the regulations on the processing of personal data by other controllers come to light, the Supervisory Body shall also notify the services listed in article 26, 7°, a), d) and f).

**Art. 250.** Within a maximum of two weeks of receipt of the request, the Supervisory Body shall provide the competent authority with a reasoned opinion on the designation, the promotion, the appointment or the mutation of the members of the police services tasked with the administration of the General National Database.

Within one month of receipt of the request, the Supervisory Body shall provide the competent minister with a detailed opinion on the desirability of disciplinary proceedings against the head of the department managing the General National Database or its deputy.

## CHAPTER IV. - Financing

**Art. 251.** To fund the activities of the Supervisory Body, a provision is made in the general expenditure budget of the State.

Each year, the Supervisory Body shall prepare a draft budget for its activities. Assisted by the Court of Auditors, the Chamber of Representatives examines the Supervisory Body's detailed budgetary proposals, approves them and checks the implementation of its budget and examines and approves the detailed accounts.

Together with its annual budgetary proposal, the Supervisory Body submits a strategic plan.

To prepare its budget and accounts, the Supervisory Body shall use a budget and accounts schedule comparable to the schedule of the Chamber of Representatives.

## CHAPTER IV. - Financing

**Art. 251.** To fund the activities of the Supervisory Body, a provision is made in the general expenditure budget of the State.

Each year, the Supervisory Body shall prepare a draft budget for its activities. Assisted by the Court of Auditors, the Chamber of Representatives examines the Supervisory Body's detailed budgetary proposals, approves them and checks the implementation of its budget and examines and approves the detailed accounts.

Together with its annual budgetary proposal, the Supervisory Body submits a strategic plan.

To prepare its budget and accounts, the Supervisory Body shall use a budget and accounts schedule comparable to the schedule of the Chamber of Representatives.

# TITLE 8. - Final provisions

**Art. 252.** In cases where personal data are processed for several purposes by one and the same controller or processor, or referred to in several regulations, these various regulations shall apply simultaneously. In the event of inconsistencies between some of their provisions, the rules of this Act shall apply.

## CHAPTER I. - Amending provisions

**Art. 253.** The existing acts, Royal Decrees and any other regulations referring to the Privacy Act of 8 December 1992, are deemed to refer to this Act or, where appropriate, to the Regulation.

The King can refer any references in current laws and Royal Decrees to the provisions of the Privacy Act of 8 December 1992 and to the Commission for the protection of privacy by means of references to the corresponding provisions of this Act and the Regulation and to the competent supervisory authority.

**Art. 254.** In Chapter 6, Section 2, of the Act of 3 December 2017 establishing the Data Protection Authority an article 56/1 is inserted which reads as follows:

"Art. 56.1. In implementation of article 51 of Regulation (EU) 2016/679 and in accordance with article 41.4 of 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, the Data Protection Authority shall represent the various supervisory authorities on the European Data Protection Board referred to in article 68 of Regulation 2016/679.".

**Art. 255.** In article 108, § 1, first paragraph, of that same Act the words "de betekening van [the service of]" are removed.

**Art. 256.** In articles 3, 31 and 35 of the Act of 18 July 1991 governing the review of the police and intelligence services and of the Coordination Unit for Threat Assessment, the words "Algemene Dienst Inlichtingen en Veiligheid [General Intelligence and Security Service]" are replaced by the words "Algemene Dienst Inlichting en Veiligheid [General Intelligence and Security Service]".

**Art. 257.** In the French text of the title of Chapter III and Sections 1 and 2 of that same Chapter, in the title of Chapter IV and in articles 2, 3, first paragraph, 2°, 28, 33, 38, 39, 40, 48, 53 and 65 of that same Act, the words "services de renseignements [intelligence service]" are replaced by the words "services de renseignement [intelligence service]".

In the French text of articles 28, 40, 41, 48, 50, 61 and 67 the words "service de renseignements [intelligence service]" are replaced by the words "service de renseignement [intelligence service]".

In the French text of articles 41 and 44 the words "des services de police ou de renseignements [police or intelligence services]" are replaced by the words "des services de police ou de renseignement [police or intelligence service]".

In the French text of article 44 the words "d'un service de police ou de renseignements [of a police or intelligence service]" are replaced by the words "d'un service de police ou de renseignement [of a police or intelligence service]".

In the French text of article 53 the words "des missions de renseignements [intelligence missions]" are replaced by the words "des missions de renseignement [intelligence missions]".

**Art. 258.** Article 3, first paragraph, of that same Act, last amended by the Act of 6 December 2015, is completed by the provisions sub 7° and 8°, which read as follows:

"7° "the Data Protection Act" means the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data;

8° "a data protection authority" means an authority that monitors the processing of personal data.".

**Art. 259.** In article 28 of that same Act, last amended by the Act of 21 April 2016, the following amendments are made:

1° in the third paragraph, 5°, the words "de inlichtingen [the information]," are inserted between the words "domein van [field of]" and "het strafrecht [criminal law]";

2° in the third paragraph, 5°, the words "het recht van de bescherming van persoonsgegevens [the right to protection of personal data]" are inserted between the words "het publiek recht, [public law]," and the words "of technieken inzake management [or management techniques]";

3° the fourth paragraph is completed by the words ", nor of another data protection authority, nor of the administrative commission tasked with monitoring specific and exceptional methods to collect data by the intelligence and security services".

**Art. 260.** In article 29, first paragraph, of that same Act, last amended by the Act of 21 April 2016, the provision sub 8° is completed by the words ", security certificates and security recommendations".

**Art. 261.** In article 31, first paragraph, 4°, of that same Act, inserted by the Act of 30 November 1998, the words ", alsook voor de organisatie en het bestuur van de Veiligheid van de Staat wanneer die organisatie en dat bestuur een rechtstreekse invloed hebben op de uitvoering van de opdrachten inzake de handhaving van de openbare orde en de persoonsbescherming [, including in terms of the organisation and administration of State Security in cases where that organisation and that administration have a direct influence on the execution of tasks relating to public order and personal protection]" are removed.

**Art. 262.** In article 32 of that same Act, last amended by the Act of 6 January 2014, the following amendments are made:

1° in the first paragraph the word "of [or]" is replaced by ",";

2° the first paragraph is completed by the words "or at the request of another data protection authority";

3° in the second paragraph the words "in het kader van de activiteiten en methodes bedoeld in artikel 33, eerste lid [in the context of the activities and methods referred to in article 33, first paragraph]" are inserted between the words "beweging optreedt [association acting for]" and ", brengt het [it shall bring]".

**Art. 263.** In article 33 of that same Act, last amended by the Act of 6 January 2014, the following amendments are made:

1° a paragraph is inserted between the first and second paragraph, which reads as follows:

"Standing Committee I also examines the processing of personal data by the intelligence services and their processors.";

2° in the fourth paragraph, which becomes the fifth paragraph, the word "of [or]" is replaced by ",";

3° in the fourth paragraph, which becomes the fifth paragraph, the words "of de verwerkingen van persoonsgegevens [or the processing of personal data]" are inserted between the words "de werkwijzen [the methods]" and the words "die de [which]".

4° in the seventh paragraph, which becomes the eighth paragraph, the words "Het Vast Comité I mag enkel [Standing Committee I may only]" are replaced by the words "Behalve als de wet zijn advies oplegt, mag het Vast Comité I enkel [Except in cases where its opinion is binding by law, Standing Committee I may only]".

**Art. 264.** In article 34 of that same Act, last amended by the Act of 10 July 2006, the following amendments are made:

1° a paragraph is inserted between the first and second paragraph, which reads as follows:

"Standing Committee I shall also examine any requests relating to the processing of personal data by the intelligence services and their processors.";

2° in the third paragraph, which becomes the fourth paragraph, the word "of [or]" is replaced by ",";

3° in the third paragraph, which becomes the fourth paragraph, the words "of een verzoek [or a request]" are inserted between the words "een aangifte [a notification]" and the words "die kennelijk [which is manifestly]";

4° in the fourth paragraph, which becomes the fifth paragraph, the word "of [or]" is replaced by ",";

5° in the fourth paragraph, which becomes the fifth paragraph, the words "of een verzoek [or a request]" are inserted between the words "klacht, aangifte [complaint, notification]" and the words "en om het [and to]";

6° in the fourth paragraph, which becomes the fifth paragraph, the words "of het verzoek [or the request]" are inserted between the words "die de klacht [(order reversed) who lodged]" and the words "heeft ingediend [(order reversed) the complaint]";

7° the fifth paragraph, which becomes the sixth paragraph, is completed by the following words:

"except in the case of investigations relating to the processing of personal data by the intelligence services and their processors, to which Standing Committee I simply shall merely reply that the necessary verifications were carried out".

**Art. 265.** Article 35 of that same Act is completed by a paragraph 3, which reads as follows:

"§ 3. Each year, Standing Committee I shall report to the Chamber of Representatives on the opinions it issued in its capacity of data protection authority, on the investigations conducted and the measures taken in that same capacity and on its cooperation with other data protection authorities. A copy of this report shall also be sent to the competent ministers, to State Security and to the General Intelligence and Security Service who have the option of submitting their comments to Standing Committee I.".

**Art. 266.** In article 38, second paragraph, of that same Act, inserted by the Act of 10 July 2006, the word "Vast [Standing]" is inserted between the words "het [the]" and "Comité [Committee]".

**Art. 267.** In article 40, second paragraph, of that same Act, last amended by the Act of 10 July 2006, the following amendments are made:

1° the words "de klachten en aangiften [the complaints and notifications]" are replaced by the words "de klachten, aangiften en verzoeken [the complaints, notifications and requests]";

2° in the French text, the words "ce d'appui [for the benefit of]" are removed;

3° the words "of handelingen [or activities]" are replaced by the words ", handelingen of verwerkingen van persoonsgegevens [activities or processing of personal data]".

**Art. 268.** In article 44 of that same Act the second paragraph is completed by the words:

"or in terms of the processing of personal data or information security.".

**Art. 269.** Article 45, second paragraph, of that same Act, inserted by the Act of 1 April 1999, is completed by the words ", security certificates and security recommendations".

**Art. 270.** In article 46 of that same Act the following amendments are made:

1° the words "except in the cases referred to in article 13/1 of the Act of 30 November 1998 governing the police and intelligence services and those referred to in articles 226, 227 and 230 of the Data Protection Act" are inserted between the words "een wanbedrijf [an offence]" and the words ", maakt hij [he shall]";

2° the article is completed by a paragraph, which reads as follows:

"Any member of Investigations Unit I who has knowledge of an offence as referred to in articles 226, 227 and 230 of the Data Protection Act, shall notify Standing Committee I without delay. The latter shall take the necessary action in accordance with the rules set out in article 54.".

**Art. 271.** In Chapter III of that same Act, a Section 4 is inserted, which reads "Competences of Standing Committee I as data protection authority".

**Art. 272.** In Section 4, inserted by article 271, an article 51/1 is inserted, which reads as follows:

"Art. 51/1. In its capacity of data protection authority, Standing Committee I either acts on its own initiative, or at the request of another data protection authority, or at the request of each data subject.".

**Art. 273.** In that same Section 4, an article 51/2 is inserted, which reads as follows:

"Art. 51/2. In order to be admissible, the request shall be submitted in writing, dated, signed and substantiated and come with proof of identity of the data subject.".

**Art. 274.** In that same Section 4, an article 51/3 is inserted, which reads as follows:

"Art. 51/3. Standing Committee I decides on the action it shall take on the file and has the authority to:

1° decide that processing was performed in accordance with the provisions of the regulations on the processing of personal data;

2° warn the service concerned or its processor that the intended processing of personal data may infringe the regulations on the processing of personal data;

3° reprimand the services concerned or its processor if the processing of personal data resulted in a breach of a provision of the regulations on the processing of personal data;

4° instruct the service concerned or its processor to bring a processing activity into line with the provisions of the regulations on the processing of personal data, where appropriate, in a certain manner and by a certain deadline.

5° impose a temporary or definitive processing restriction, including a processing ban;

6° order the rectification or erasure of personal data;

7° forward the file to the competent public prosecutor's office which shall notify it of the action taken in relation to the file;

**Art. 275.** In that same Section 4, an article 51/4 is inserted, which reads as follows:

"Art. 51/4. Standing Committee I shall notify the service concerned of the investigations it conducted into the processing of personal data by its processors and of the results.

Where infringements of the regulations on the processing of personal data by other controllers come to light, Standing Committee I shall also notify the service concerned.

**Art. 276.** In article 4, § 2, of the Act of 3 December 2017 establishing the Data Protection Authority, the following amendments are made:

1° The second paragraph is replaced by:

"The Data Protection Authority is the competent supervisory authority unless an applicable law provides otherwise.";

2° between the second and the third paragraphs a paragraph is inserted, which reads as follows:

"Without prejudice to this Act and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, no other law can provide for the establishment of an authority vested with the powers and the competences conferred on a data protection authority under the Regulation.".

**Art. 277.** Article 18 of that same Act is completed by a second paragraph, which reads as follows:

"The decision to take legal action on behalf of the Data Protection Authority shall be taken by the committee.".

**Art. 278.** In Chapter 5, Section 1, of that same Act an article 54/1 is inserted, which reads as follows:

"Art. 54/1. § 1. To ensure the consistent application of national, European and international legislation on the protection of natural persons with regard to the processing of personal data, the Data Protection Authority and the competent supervisory referred to in Titles 2 and 3 of the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data shall work in close collaboration, inter alia, as regards the processing of complaints, opinions and recommendations that relate to the competences of two or more supervisory authorities.

Without prejudice to specific provisions, the joint processing of complaints, opinions and recommendations shall be effected on the basis of the one-stop-shop principle to be ensured by the Data Protection Authority.

§ 2. To ensure the cooperation referred to in paragraph 1, the supervisory authorities shall sign a cooperation protocol.".

**Art. 279.** In article 111 of that same Act the second paragraph is replaced as follows:

"Admission to the deliberations of a sectoral committee under a general authorisation remains possible, provided the person seeking admission provides either the National Register Sectoral Committee or the Social Security and Health Sectoral Committee or, once these committees have been disbanded by law, the body to be established by the legislature to deliberate on the exchange of personal data or the use of the national registry number, with a signed undertaking confirming that he accepts the terms of the deliberations in question and this without prejudice to the powers of inspection of the Data Protection Authority. The general authorisations granted shall be published on the website of the body charged with their receipt.".

**CHAPTER II. - Repeal provisions**

**Art. 280.** The Privacy Act of 8 December 1992 is repealed.

The Royal Decree of 13 February 2001 implementing the Privacy Act of 8 December 1992 is repealed.

The Royal Decree of 17 December 2003 establishing the further rules on the composition and the activities of certain sectoral committees set up within the Commission for the protection of privacy is repealed.

Article 15, § 3, of the Act of 25 December 2016 on the processing of passenger information is repealed.

**CHAPTER III. - Entry into force and transitional provisions**

**Art. 281.** This Act shall enter into force on the date it is published in the Belgian Official Journal.

By way of derogation from the first paragraph, article 20 shall enter into force on the first day of the month following the expiration of a period of six months commencing on the day after the publication of this Act in the Belgian Official Journal.

**Art. 282.** The legal provisions as set out in the Regulation and this Act do not prejudice the validity of the personal data processing activities controllers or processors carried out before the aforementioned obligations entered into force.

**Art. 283.** The international agreements on the transfers of personal data to third countries or international organisations concluded prior to 6 May 2016 which are consistent with the Privacy Act of 8 December 1992 and European law applicable prior to that date shall remain in force until they are amended, replaced or repealed.

**Art. 284.** By way of derogation from article 281, automated processing systems the competent authorities referred to in Title 2 put in place prior to 6 May 2016 shall be brought into line with article 56, § 1 by 6 May 2023 at the latest.

**Art. 285.** § 1. By way of derogation from article 281, the members of the Supervisory Body who were sworn in and are effectively in office when this Act enters into force and who were appointed in accordance with article 36ter/1 of the Privacy Act of 8 December 1992 shall ipso jure remain appointed in accordance with paragraphs 2, 3 and 4 as members of the Supervisory Body or as members of the investigations unit within the meaning of this Act until their current six-year mandate, which started on 1 September 2015, comes to an end.

As of the entry into force of this Act and for the duration of their aforesaid mandate they shall ipso jure be deemed to meet articles 231 and 232 of this Act.

§ 2. The current members shall ipso jure be appointed as members of the Supervisory Body or of the investigations unit in accordance with the new appointment requirements as provided for under this Act and in accordance with paragraphs 3 and 4.

§ 3. The chairman of the Supervisory Body shall ipso jure remain in office as chairman of the Supervisory Body within the meaning of this Act.

The member of the Commission for the protection of privacy shall ipso jure be appointed as member of the Supervisory Body originating from the Public Prosecutor's Office within the meaning of this Act and the current Dutch-speaking expert-lawyer shall ipso jure be appointed in the capacity of expert within the meaning of this Act as member of the Supervisory Body.

§ 4. The other three current members, two of whom from the police services and one French-speaking expert, non-lawyer, shall ipso jure be appointed as members of the investigations unit within the meaning of this Act in their respective capacities of members of the police services and expert.

§ 5. By way of derogation from article 231, § 1, of this Act, the member of the Supervisory Body, appointed in his capacity of member of the Commission for the protection of privacy, shall, as of the entry into force of this Act until the end of his current mandate, which came into effect on 1 September 2015, continue to fulfil his functions on either a full-time or part-time basis. Where the mandate is exercised on a part-time basis, his salary shall amount to 20 % of the salary paid to the other members as referred in article 234.

**Art. 286.** This Act shall be the subject of a detailed joint evaluation by the Minister for Social Affairs, the Minister for Public Health, the Minister for Justice, the Minister for the Interior, the Minister for Defence, under the leadership of the minister with responsibility for Privacy, during the third year after its entry into force.

The evaluation referred to in the first paragraph shall inter alia relate to:

1° the impact of the designation of several supervisory authorities on the rights of data subjects.

For the purpose of the evaluation of this point, account shall inter alia be taken of the functioning of the one-stop-shop system.

2° the impact of the designation of several supervisory authorities on the flow of information and personal data.

For the purpose of the evaluation of this point, account shall inter alia be taken of:

- the efficiency of the cooperation between the supervisory authorities;

- the coherence of their decisions, opinions and recommendations; and

- the impact of their activities on the balance between the interests representing the flows, on the one hand, and respect for the rights of data subjects, on the other hand.

3° the list of the competent authorities referred to in article 26, 7°.

For the purpose of the evaluation of this point, account shall inter alia be taken of:

- the prior opinions and the published annual reports of the various competent supervisory authorities referred to in this Act;

- the results of the evaluations referred to in article 97, § 1, of the Regulation, article 62, § 6, of the Directive and, where appropriate, article 62, § 1, of the Directive;

- the opinions and recommendations of the European Data Protection Board.

The minister with responsibility for Privacy shall present the result of the evaluation to the Chamber of Representatives.