**Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters and amending**

**1° the Act of 7 March 1980 on the organisation of the judicial system, as amended;**

**2° the Act of 29 May 1998 approving the Convention on the basis of Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), signed in Brussels on 26 July 1995, as amended;**

**3° the Act of 20 December 2002 approving - the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, signed in Brussels on 26 July 1995; - the Agreement relating to the provisional application between certain Member States of the European Union of the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, signed in Brussels on 26 July 1995;**

**4° the Act of 15 June 2004 relating to the classification of documents and security clearances, as amended;**

**5° the Act of 16 June 2004 on the Reorganisation of the State Socio-educational Centre, as amended;**

**6° the Act of 25 August 2006 relating to identification procedures by genetic fingerprinting in criminal matters and amending the Code of Criminal Procedure, as amended;**

**7° the Act of 24 June 2008 relating to the control of travelers in accommodation establishments;**

**8° the Act of 29 March 2013 relating to the organisation of criminal records, as amended;**

**9° the Act of 19 December 2014 facilitating the cross-border exchange of information concerning road safety offenses;**

**10° the Act of 25 July 2015 on the creation of an automated control and sanction system, as amended;**

**11° the Act of 5 July 2016 on the reorganisation of the State Intelligence Service**

**12° the Act of 23 July 2016 establishing a specific status for certain personal data processed by the State Intelligence Service;**

**13° the Act of 22 February 2018 on the exchange of personal data and information in police matters;**

**14° the Act of 18 July 2018 on the Grand Ducal Police; and**

**15° the Act of 18 July 2018 on the General Police Inspectorate.**

## Chapter 1 – General provisions

### Art. 1. Subject-matter and scope

(1) This Act applies to the processing of personal data carried out 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, by any competent public authority or any other body or entity, for the same purposes, to whom the exercise of public authority and public powers have been entrusted, hereinafter referred to as 'the competent authority'.

(2) This Act also applies to the processing of personal data:

a) by the Grand Ducal Police in the performance of tasks other than those referred to in paragraph 1 and provided for by special laws,

b) by the State Intelligence Service in the performance of its tasks provided in article 3 of the Act of 5 July 2016 on the reorganisation of the State Intelligence Service,

c) by the National Security Authority in the performance of its tasks provided for in article 20 of the amended Act of 15 June 2004 relating to the classification of documents and security clearances,

d) by the Luxembourg Army in the performance of its tasks provided for in article 2 of the amended Act of 23 July 1952 on military organisation,

e) by the Financial Intelligence Unit in the performance of its tasks provided for in Articles 74-1 to 74-6 of the amended Act of 7 March 1980 on judicial organisation, and

f) by the Luxembourg authorities in the context of activities falling within the scope of Chapter 2 of Title V of the Treaty on European Union on the common foreign and security policy.

(3) 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.

### Art. 2. Definitions

(1) For the purposes of this Act:

1° "personal data" means any information relating to an identified or identifiable natural person ('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 note 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 authority” means:

a) any public authority competent for 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, as well as civil servants and state officials of public administrations and services to whom special laws have conferred certain administrative or judicial police powers, under the conditions and within the limits laid down by those laws, or

b) any other body or entity entrusted by Member State law to exercise public authority and public powers 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;

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 Union or Luxembourg law, the controller or the specific criteria for its nomination may be provided for by Union or Luxembourg law;

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

10° “recipient” means a natural or legal person, public authority, agency or another 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 in accordance with the law 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° “personal data 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

a) the supervisory authority established by the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, hereinafter referred to as the “National Data Protection Commission”, and

b) the judicial supervisory authority established by article 40;

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, including the International Criminal Police Organisation (ICPO – Interpol).

(2) For the purposes of this Act, where the concepts used are not defined in paragraph 1, the definitions in Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as ‘Regulation (EU) 2016/679’, shall apply.

## Chapter 2 - Principles

### Art. 3. Principles relating to processing of personal data

(1) Personal data referred to in this Act shall be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

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

(d) 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;

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

(f) 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.

(2) Processing carried out by the same or another controller for any of the purposes set out in Article 1 other than those for which the data were collected shall be permitted if they are necessary and proportionate to that purpose, subject to compliance with the provisions laid down in this Chapter and in Chapters IV and V.

(3) Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1.

(4) The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

### Art. 4. Time-limits for storage and review

(1) The controller shall set appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data. The time limits are to be set taking into account the purpose of the processing.

(2) The controller shall establish procedural measures with a view to ensuring compliance with the time limits, which determine the persons acting in the name and on behalf of the controller in this measure, including the data protection officer, as well as the time limits within which these persons must carry out their respective tasks. The procedural measures are made available to the data subject in accordance with Article 11 and to the competent supervisory authority upon request.

**Art. 5. Distinction between different categories of data subject**

The controller shall, where applicable and as far as possible, make a clear distinction between personal data of different categories of data subjects, such as:

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

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

(d) other 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, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in letters a) and b).

**Art. 6. Distinction between personal data and verification of quality of personal data**

(1) Personal data based on facts shall be distinguished, as far as possible, from personal data based on personal assessments.

(2) The competent authorities shall take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.

(3) If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16.

**Art. 7. Lawfulness of processing**

(1) The processing is lawful only if and to the extent that processing is necessary for the performance of the tasks of the competent authority, defined in Article 2(1), point 7), for one of the purposes set out in Article 1 and where this task is carried out on the basis of the legislative provisions governing the competent authority in question.

(2) The processing ensures the proportionality of the storage period of the personal data, taking into account the subject-matter of the filing system and the nature or the severity of the violations and facts in question.

**Art. 8. Specific processing conditions**

(1) Personal data collected by competent authorities for the purposes set out in Article 1 shall not be processed for purposes other than those set out in that article unless such processing is authorised by European Union law or by a provision of Luxembourg law. In this case, the processing of these personal data is carried out in compliance with the provisions of

Regulation (EU) 2016/679 or of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework.

(2) Where competent authorities are entrusted with the performance of tasks other than those set out in Article 1, Regulation (EU) 2016/679 or, where applicable, the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework apply to the processing of data carried out for these other purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(3) Where European Union law or a provision of Luxembourg law applicable to the transmitting competent authority provides specific conditions for processing, the transmitting competent authority shall inform the recipient of such personal data of those conditions and the requirement to comply with them.

(4) The transmitting competent authority shall not apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data to other competent authorities established on the territory of the Grand Duchy of Luxembourg.

**Art. 9. Processing of special categories of personal data**

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 shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

a) where authorised by European Union law or pursuant of this Act or another provision of Luxembourg law;

b) to protect the vital interests of the data subject or of another natural person; or

c) where such processing relates to data which are manifestly made public by the data subject.

**Art. 10. Automated individual decision-making**

(1) A decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, shall be prohibited unless authorised by a national legal provision or by European Union law and where the controller provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

(2) Decisions referred to in paragraph 1 shall not be based on special categories of personal data referred to in Article 9, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

(3) Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 9 shall be prohibited.

## Chapter 3 – Rights of the data subject

**Art. 11. Communication and modalities for exercising the rights of the data subject**

(1) The controller shall take reasonable steps to provide any information referred to in Article 12 and make any communication relating to the processing with regard to Articles 10, 13 to 17 and 30 to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by

electronic means. 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 under Article 10 and Articles 13 to 17.

(3) The controller shall inform the data subject in writing about the follow up to his or her request without undue delay.

(4) The information provided under Article 12, and any communication made or action pursuant to Article 10, Articles 13 to 17, and Article 30 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

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

b) refuse to act on the request.

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

(6) Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 13 or 15, he may request the provision of additional information necessary to confirm the identity of the data subject.

**Art. 12. Information to be made available or given to the data subject**

(1) The controller shall make available to the data subject at least the following information:

a) the identity and the contact details of the controller;

b) the contact details of the data protection officer;

c) the purposes of the processing for which the personal data are intended;

d) the right to lodge a complaint with one of the two supervisory authorities referred to in Articles 39 and 40 and the contact details of the supervisory authority;

e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

(2) In addition to the information referred to in paragraph 1, the controller shall give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

a) the legal basis for the processing;

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

c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject

(3) The controller may delay, restrict or omit the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society, taking into account the relevant processing activity, and with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

a) avoid obstructing official or legal inquiries, investigations or procedures;

b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

c) protect public security;

d) protect national security and national defence; or

e) protect the rights and freedoms of others.

**Art. 13. Right of access by the data subject**

Subject to Article 14, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of and legal basis for the processing;

b) the categories of personal data concerned;

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

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) 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;

f) the right to lodge a complaint with one of the two supervisory authorities referred to in Articles 39 and 40 and the contact details of the supervisory authority;

g) communication of the personal data undergoing processing and of any available information as to their origin.

**Art. 14. Limitations to the right of access**

(1) The controller may restrict, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society, taking into account the relevant processing activity, and with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

a) avoid obstructing official or legal inquiries, investigations or procedures;

b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

c) protect public security;

d) protect national security and national defence; or

e) protect the rights and freedoms of others.

(2) In the cases referred to in paragraph 1, the controller shall inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. The controller shall inform the data subject of the possibility of lodging a complaint with the competent supervisory authority or seeking a judicial remedy.

(3) The controller shall document the factual or legal reasons on which the decision is based. That information shall be made available to the competent supervisory authority.

**Art. 15. Right to rectification or erasure of personal data and restriction of processing**

(1) The controller shall rectify without undue delay, inaccurate personal data of the data subject. Taking into account the purposes of the processing, the incomplete personal data of the data subject are completed, including by means of a supplementary statement provided by the data subject to this end.

(2) The controller shall erase the personal data of the data subject without undue delay where processing of these data infringes the provisions foreseen in Article 3, 7 or 9, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

(3) Instead of erasure, the controller shall restrict processing where:

a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained, or

b) the personal data must be maintained for the purposes of evidence.

Where processing is restricted pursuant to point a) of the first subparagraph of this paragraph, the controller shall inform the data subject before lifting the restriction of processing.

(4) The controller shall inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. The controller may restrict, wholly or partly, the provision of such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society, taking into account the relevant processing activity, and with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:

a) avoid obstructing official or legal inquiries, investigations or procedures;

b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

c) protect public security;

d) protect national security and national defence; or

e) protect the rights and freedoms of others.

The controller shall inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

(5) The controller shall communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

(6) Where personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3, the controller shall notify the recipients in order that the latter may rectify or erase the personal data or restrict processing of the personal data under their responsibility.

**Art. 16. Exercise of rights by the data subject and verification by the supervisory authority**

(1) In the cases referred to in Article 12(3), Article 14(1) and Article 15(4), the rights of the data subject may be exercised through the competent supervisory authority.

(2) The controller shall inform the data subject of the possibility of exercising his or her rights through the competent supervisory authority pursuant to paragraph 1.

(3) Where the right referred to in paragraph 1 is exercised, the competent supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

### Art. 17. Rights of the data subject in criminal investigations and proceedings

If the personal data relates to facts which are the subject of a preliminary investigation or a pre-trial judicial inquiry (*instruction préparatoire)*, which have been referred to a trial court, which are the subject of a summons, or if these facts are referred to the competent authority on the basis of the Amended Act of 10 August 1992 relating to the protection of youth, the rights set out in Articles 12, 13 and 15 shall be exercised in accordance with the provisions of the Criminal Procedure Code, or any other applicable legal provisions.

## Chapter 4 – Controller and processor

## Section 1- General obligations

### Art. 18. Obligations of the controller

(1) The controller shall, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Act. Those measures shall be reviewed and updated where necessary.

(2) Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

### Art. 19. Data protection by design and by default

(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 for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, the controller shall implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Act and protect the rights of data subjects.

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

### Art. 20. Joint controllers

(1) Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with this Act, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 11 and 12, by means of an arrangement between them. The arrangement shall designate the single contact point for data subjects in order to exercise their rights.

(2) Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under the provisions adopted pursuant to this law in respect of and against each of the controllers.

### Art. 21. Processor

(1) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Act and ensure the protection of the rights of the data subject.

(2) The processor shall not engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(3) The processing by a processor shall be governed by a contract or other legal act under European Union law, Luxembourg law or the law of another Member State, 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 obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a) acts only on instructions from the controller;

b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless a legal provision requires storage of the personal data;

e) makes available to the controller all information necessary to demonstrate compliance with this article;

f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.

(4) The contract or the other legal act referred to in paragraph 3 shall be in writing, including in an electronic form.

(5) If a processor determines, in infringement of this Act, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing.

**Art. 22. Processing under the authority of the controller or processor**

The processor, and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required by law.

**Art. 23. Records of processing activities**

(1) Controllers shall maintain a record of all categories of processing activities under their responsibility. That record shall contain all of the following information:

a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;

b) the purposes of the processing;

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

d) a description of the categories of data subject and of the categories of personal data;

e) where applicable, the use of profiling;

f) where applicable, the categories of transfers of personal data to a third country or an international organisation;

g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;

h) where possible, the envisaged time limits for erasure of the different categories of personal data;

i) where possible, a general description of the technical and organisational security measures referred to in Article 28(1).

(2) Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

a) the name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;

b) the categories of processing carried out on behalf of each controller;

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

d) where possible, a general description of the technical and organisational security measures referred to in Article 28(1).

(3) The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form. The controller and the processor shall make those records available to the supervisory authority on request.

**Art. 24. Logging**

(1) Logs shall be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

(2) The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

(3) The controller and the processor shall make the logs available to the supervisory authority on request of the latter.

**Art. 25. Cooperation with the supervisory authority**

The controller and the processor shall cooperate, on request, with the competent supervisory authority in the performance of its tasks.

**Art. 26. Data protection impact assessment**

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

(2) The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the law, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

**Art. 27. Prior consultation of the competent supervisory authority**

(1) The controller or processor shall consult the competent supervisory authority prior to processing, which will form part of a new filing system to be created, where:

a) a data protection impact assessment as provided for in Article 26 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

(2) The competent supervisory authority shall be consulted during the preparation of a proposal for a legislative measure or a proposal for a Grand Ducal regulation, which relates to processing.

(3) The supervisory authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

(4) The controller shall provide the supervisory authority with the data protection impact assessment pursuant to Article 26 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

(5) Where the competent supervisory authority is of the opinion that the intended processing referred to in paragraph 1 of this article would infringe this Act, in particular where the controller has insufficiently identified or mitigated the risk, the competent supervisory authority shall provide, within a period of up to six weeks of receipt of the request for consultation, written advice provide in writing an opinion to the controller and, where applicable, to the processor, and may use any of its powers referred to in Article 14 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework or in Article 43 of this Act, depending on the competent supervisory authority. That period may be extended by a month, taking into account the complexity of the intended processing. The 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.

## Section 2 - Security of personal data

**Art. 28. Security of processing**

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 9.

(2) In respect of automated processing, the controller or processor shall implement, following an evaluation of the risks, measures designed to:

a) deny unauthorised persons access to processing equipment used for processing (‘equipment access control’);

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

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

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

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

f) 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 (‘communication control’);

g) 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 (‘input control’);

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

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

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

**Art. 29. Notification of a personal data breach to the supervisory authority**

(1) In the case of a personal data breach, the controller shall notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(2) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

(3) The notification referred to in paragraphs 1 and 2 shall at least:

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

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach, and

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

(5) The controller shall document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

(6) Where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, the information referred to in paragraph 3 shall be communicated to the controller of that Member State without undue delay.

**Art. 30. Communication of a personal data breach to the data subject**

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

(2) The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in points b), c) and d) of Article 29(3).

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

a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) 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;

c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

(4) If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require 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 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 12(3).

## Section 3 - Data protection officer

**Art. 31. Designation of the data protection officer**

(1) The controller shall designate a data protection officer.

(2) The data protection officer shall be designated on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law and practice and ability to fulfil the tasks referred to in Article 33.

(3) A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.

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

**Art. 32. Position of the data protection officer**

(1) The controller shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The controller shall support the data protection officer in performing the tasks referred to in Article 33 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

**Art. 33. Tasks of the data protection officer**

(1) The controller shall entrust the data protection officer at least with the following tasks:

a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to this Act and to other Union or Luxembourg data protection provisions;

b) to monitor compliance with this Act, with other Union or Luxembourg data protection provisions 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;

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 26;

d) to cooperate with the competent supervisory authority;

e) to act as the contact point for the data subject and the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 27, and to consult, where appropriate, with regard to any other matter in relation to his or her tasks.

## Chapter 5 – Transfer of personal data to third countries or international organisations

**Art. 34. General principles for transfers of personal data**

(1) A transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation, shall, subject to compliance with the other provisions of this Act, take place only where the conditions laid down in this chapter are met, namely:

a) the transfer is necessary for the purposes set out in Article 1;

b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1;

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

d) the European Commission has adopted an adequacy decision pursuant to Article 35, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 36, or, in the absence of an adequacy decision pursuant to Article 35 and of appropriate safeguards in accordance with Article 36, derogations for specific situations apply pursuant to Article 37; and

e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, 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 the prior authorisation by another Member State in accordance with point c) of paragraph 1 shall be 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.

(3) All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Act is not undermined.

**Art. 35. Transfers on the basis of an adequacy decision**

(1) A transfer of personal data to a third country or to an international organisation may take place if the European Commission, pursuant to Article 36 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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 penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, hereinafter referred to as 'Directive (EU) 2016/680', hasdecided that the third country, a territory or one or more specific sectors in that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

(2) A decision adopted pursuant to Article 36(5) of Directive (EU) 2016/680 is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question, pursuant to Articles 36 and 37.

**Art. 36. Transfers subject to appropriate safeguards**

(1) In the absence of a decision pursuant to Article 35, a transfer of personal data to a third country or an international organisation may take place where:

a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

(2) The controller shall inform the competent supervisory authority about categories of transfers under point b) of paragraph 1.

(3) When a transfer is based on point b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the competent supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

**Art. 37. Derogations for specific situations**

(1) In the absence of an adequacy decision pursuant to Article 35, or of appropriate safeguards pursuant to Article 36, a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that the transfer is necessary:

a) in order to protect the vital interests of the data subject or another person;

b) to safeguard legitimate interests of the data subject;

c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;

d) in individual cases for the purposes set out in Article 1; or

e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1.

(2) Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points d) and e) of paragraph 1.

(3) Where a transfer is based on paragraph 1, point b), such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

**Art. 38. Transfers of personal data to recipients established in third countries**

(1) By way of derogation from point b) of Article 34(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, the competent authorities referred to in Article 2, point 7, a) may, in individual and specific cases, transfer personal data directly to recipients established in third countries only if the other provisions of this Act are complied with and all of the following conditions are fulfilled:

a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by European Union law for the purposes set out in Article 1;

b) 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;

c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1 in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

d) the authority that is competent for the purposes referred to in Article 1 in the third country is informed without undue delay, unless this is ineffective or inappropriate; and

e) 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) An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between the Grand Duchy of Luxembourg and third countries in the field of judicial cooperation in criminal matters and police cooperation.

(3) The transferring competent authority shall inform the supervisory authority about transfers under this Article.

(4) Where a transfer is based on paragraph 1, such a transfer shall be documented.

## Chapter 6 - Independent supervisory authorities

### Section 1 - Administrative supervisory authority

**Art. 39. Competence of the National Data Protection Commission**

The supervisory authority established by Article 3 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework is competent to monitor and verify compliance with the provisions of this law.

## Section 2 - Judicial supervisory authority

### Art. 40. Creation, competence and composition of the judicial supervisory authority

(1) A supervisory authority for judicial data is hereby established, hereinafter referred to as the 'judicial supervisory authority'.

(2) By way of derogation from Article 39, the processing of personal data carried out by the courts of the judicial order, including the public prosecutor's office, and the administrative order acting in their judicial capacities, whether for the purposes referred to in Article 1 of this Act or for those referred to in Regulation (EU) 2016/679, is subject to the supervision of the judicial supervisory authority.

(3) The judicial supervisory authority is composed of six members and their deputies as follows:

1) the President of the Superior Court of Justice or his delegate;

2) a representative from the other courts of the judicial order;

3) the President of the Administrative Court or his delegate;

4) the Chief Public Prosecutor or his delegate;

5) a representative of the Public Prosecutor's Office of the district of Luxembourg or of the district of Diekirch, and

6) a representative of the National Data Protection Commission.

A civil servant or an employee of the judicial administration assumes the role of secretary of the judicial supervisory authority. One or more other officials or employees of the judicial administration may be appointed as members of the secretariat of the judicial supervisory authority, including one as deputy secretary.

(4) The members and their deputies as well as the civil servants and employees fulfilling roles within the secretariat of the judicial supervisory authority are appointed by order of the Minister responsible for Justice on a proposal:

1) of the President of the Superior Court of Justice for the deputy members referred to in paragraph 3, paragraph 1, points 1) and 2), and for the civil servants and employees referred to in paragraph 3, paragraph 2;

2) of the Chief Public Prosecutor for the members and deputy members referred to in paragraph 3, points 4) and 5), and

3) of the President of the National Data Protection Commission for the member referred to in paragraph 3, point 6).

(5) Only members and deputy members who have served for at least three years within the judicial courts, administrative courts or the National Data Protection Commission, respectively, may be appointed. The term of office of members and their deputies is six years and is renewable once. Mandates shall end in the event of the resignation as a member of the judicial supervisory authority or as a member of the judicial courts, administrative courts or the National Data Protection Commission, or in case of voluntary or forced retirement. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of his duties. In the event of a member or alternate

member vacancy, a new member shall be appointed as the replacement, in accordance with paragraph 4, and shall complete the mandate of the member who is being replaced.

(6) During their term of office, members of the judicial supervisory authority each receive a non-pensionable monthly bonus of fifty index points. This bonus is thirty points for deputy members of the judicial supervisory authority and twenty points for the members of its secretariat.

In the event of the appointment of a delegate within the meaning of paragraphs 3 and 4, the member having appointed a delegate may not benefit from the bonus referred to in the first paragraph during the duration of this delegation.

**Art. 41. Functioning of the judicial supervisory authority**

(1) The presidency of the judicial supervisory authority is held by the President of the Superior Court of Justice or his delegate and its vice-presidency is held by the President of the Administrative Court or his delegate.

(2) The judicial supervisory authority may only validly deliberate when at least three of its members or deputy members, including at least one member, are present. Any member unable to participate in a meeting shall inform their deputy.

The judicial supervisory authority may appoint experts who, upon request of the supervisory authority, may attend meetings in an advisory capacity.

(3) The judicial supervisory authority shall meet, upon being convened by its president, whenever the matters falling within its remit so require. The meetings of the judicial supervisory authority shall be chaired by its president or, in the event of his absence, by its vice-president, otherwise in accordance with the provisions of its internal regulations referred to in paragraph 10.

Except in cases of emergency, the notice, containing the agenda and specifying the place, day and time of the meeting, is sent by post or electronically at least eight calendar days before the date set for the meeting at the addresses provided by the members.

(4) The president opens and closes the meeting and presides over the discussions. If the president determines that the quorum to deliberate is not reached, he closes the meeting. In this case, he convenes the judicial supervisory authority again within eight calendar days with the same agenda. The judicial supervisory authority then sits and validly deliberates regardless of the number and status of the members present.

(5) The president and the other members of the judicial supervisory authority each have one vote. The vote is taken by a show of hands. Decisions are taken by a majority of the votes cast, except for abstentions. In the event of a tied vote, the meeting's president has the casting vote.

(6) After each meeting, the secretary draws up minutes indicating the names of the members present or excused, the agenda for the meeting as well as the decisions taken and, where applicable, the reasons on which they are based. The minutes are signed by the president and the secretary and communicated to the members of the judicial supervisory authority.

(7) The judicial supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Act. In the performance of their tasks and exercise of their powers, the members of the judicial supervisory authority shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

(8) Members of the judicial supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

(9) The members of the judicial supervisory authority are subject to a duty of professional secrecy within the meaning of Article 458 of the Penal Code both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or the exercise of their powers.

(10) The judicial supervisory authority shall adopt internal regulations to determine its necessary procedures and working arrangements not provided for in this Act. These regulations are published in the Official Journal of the Grand Duchy of Luxembourg.

**Art. 42. Tasks of the judicial supervisory authority**

(1) Within the limits of its powers under Article 40(2), and where the processing of personal data by the authorities referred to therein falls within the scope of this Act, the judicial supervisory authority shall:

a) monitor and enforce the application of the provisions of this Act;

b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

c) advise the Chamber of Deputies, the Government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

d) promote the awareness of controllers and processors under its jurisdiction of their obligations under this Act;

e) upon request, provide information to any data subject concerning the exercise of their rights under this Act and, if appropriate, cooperate with the National Data Protection Commission and foreign supervisory authorities to this end;

(f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 47, and investigate, to the extent appropriate, the subject-matter of the complaint and inform the complainant of the progress and outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

g) check the lawfulness of processing pursuant to Article 16 and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article, or of the reasons why the check has not been being carried out;

h) cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Act;

i) conduct investigations on the application of this Act, including on the basis of information received from another supervisory authority or other public authority;

j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

k) provide advice on the processing operations referred to in Article 27.

The judicial supervisory authority shall facilitate the submission of complaints referred to in paragraph 1, f), by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

The performance of the tasks of the judicial supervisory authority is free of charge for the data subject and for the data protection officers competent for the processing of data falling within the scope of this Act.

Where a request is manifestly unfounded or excessive, in particular because it is repetitive, the judicial supervisory authority may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. The judicial supervisory authority shall bear the burden of demonstrating that the request is manifestly unfounded or excessive.

(2) Where the processing of personal data carried out by the authorities referred to in Article 40(2) falls within the scope of Regulation (EU) 2016/679, the duties of the judicial supervisory authority are those referred to in Article 57 of that regulation.

**Art. 43. Powers of the judicial supervisory authority**

(1) Where the processing of personal data carried out by the authorities referred to in Article 40(2) falls within the scope of this Act, the judicial supervisory authority has the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions of this Act;

b) to order the controller or processor to bring processing operations into compliance with the provisions adopted under this Act, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 15;

c) to impose a temporary or definitive limitation, including a ban, on processing.

The judicial supervisory authority obtains access from the controller or the processor to all the personal data that is processed and to all the other information necessary for the performance of its duties.

The judicial supervisory authority advises the controller in accordance with the prior consultation procedure referred to in Article 27 and issues, on its own initiative or on request, opinions to the Chamber of Deputies and the Government or other institutions and bodies, as well as to the public, on any issues related to the protection of personal data within its competence.

The judicial supervisory authority has the power to bring infringements of provisions of this Act to the attention of judicial authorities in order to enforce the provisions of this Act.

(2) Where the processing of personal data carried out by the authorities referred to in Article 40(2) falls within the scope of Regulation (EU) 2016/679, the powers of the judicial supervisory authority are those referred to in Article 58 of that regulation.

## Chapter 7 - Remedies, liability and penalties

**Art. 44. Right to lodge a complaint with a supervisory authority**

(1) Any data subject may lodge a complaint with the National Data Protection Commission against personal data processing operations if they consider that the processing of personal data relating to him or her infringes the provisions of this Act.

(2) By way of derogation from paragraph 1, complaints against personal data processing operations carried out by the courts of the judicial order, including the public prosecutor, and the administrative order acting in their judicial capacities are treated as procedural incidents before the court with jurisdiction to rule on the dispute to which the data subject is a party, in accordance with the procedural provisions applicable to the dispute concerned.

(3) For any claim against personal data processing operations carried out by the courts of the judicial order, including the public prosecutor, and the administrative order in the exercise of their judicial functions, which cannot be handled in accordance with paragraph 2, the data subject may lodge the matter with the judicial supervisory authority.

(4) If the complaint is not lodged with the competent supervisory authority, the supervisory authority with which the complaint was lodged shall transmit it to the competent supervisory authority, without undue delay. The data subject shall be informed about the transmission.

(5) The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 45.

**Art. 45. Right to a judicial remedy against a decision of a supervisory authority**

(1) When the processing of personal data covered by a complaint falls within the scope of this Act, a judicial appeal may be brought by the data subject before the council chamber of the Court of Appeal against decisions taken by the judicial supervisory authority pursuant to Article 44(3).

The request is recorded in a register kept for this purpose at the registry of the council chamber of the Court of Appeal. The request must be filed with the registry of the council chamber of the Court of Appeal within one month of the notification date of the decision in question by the judicial supervisory authority to the data subject, or, where the judicial supervisory authority has not ruled on the data subject's complaint, from the expiry of a period of three months from the date of which the data subject lodged the request with the judicial supervisory authority, failing which it shall be inadmissible. The court clerk notifies the data subject and the controller at least eight days before the date and time of the hearing.

The controller or their representative and the data subject and, where applicable, their representative alone have the right to attend the hearing and to provide briefs and make requisitions, whether verbal or written, that they deem appropriate. The hearing of the council chamber shall not be public.

The notifications and warnings referred to in this paragraph are made in the forms provided for notifications in law enforcement matters. Neither the time limit for appeal, nor the referral to the council chamber of the Court of Appeal pursuant to this paragraph shall have any suspensive effect.

(2) When the processing of personal data covered by the complaint falls within the scope of Regulation (EU) 2016/679, the data subject may lodge an appeal against decisions taken by the National Data Protection Commission on the basis of Article 44(1) and against decisions taken by the judicial supervisory authority on the basis of Article 44(3) before the Administrative Court, which rules on the merits of the case.

**Art. 46. Representation of data subjects**

(1) Without prejudice to legal provisions relating to the representation of the parties before the judicial and administrative courts, the data subject has the right to appoint a legal person, fulfilling the conditions provided for in paragraph 2, to exercise the rights referred to in Articles 44 and 45 on their behalf.

(2) In order to be able to represent the data subject, and in order for the complaint or appeal to be admissible, the legal person referred to in paragraph 1 must fulfil the following conditions:

a) be properly constituted as an association or foundation in accordance with the provisions of the Amended Act of 21 April 1928 on non-profit associations and foundations;

b) in the case of a non-profit association, having been recognised as being of public utility in accordance with Article 26-2 of the law referred to in a);

c) the protection of data subjects' rights and freedoms with regard to the protection of personal data must appear in the statutes of the association or foundation as the purpose or one of the purposes for which the association or foundation was created;

d) have legal personality when the complaint or legal action is lodged in the name of the data subject;

e) have been mandated in writing and prior to the exercise of the person's rights referred to in Articles 44 and 45.

(3) A mandate issued pursuant to this Article having as its object the defence of the general interest is void.

**Art. 47. Penalties**

(1) An infringement of Articles 3 to 15, 18 to 30, and 34 to 38 of this Act shall be punishable by an administrative fine of 500 to 250,000 euros, which shall be imposed by a decision of the supervisory authority. An appeal against this decision can be lodged with the Administrative Court, which rules on the merits of the case.).

(2) The competent supervisory authority may, by way of a decision, impose a periodic penalty payment of 100 euros per day of delay in order to compel the controller to comply with the injunctions issued by either the National Data Protection Commission on the basis of Article 14, points 1, 3 and 4 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, or the judicial supervisory authority pursuant to Article 43, b) and c).

The penalty shall be calculated from the date stipulated in the decision pronouncing the penalty. This date cannot be earlier than the date of notification of the decision. An appeal against this decision can be lodged with the Administrative Court, which rules on the merits of the case..

(3) Furthermore, an infringement of Articles 9, 10 and 29 of this Act with fraudulent intent or with intent to harm shall be punished by imprisonment from eight days to one year and a fine of 251 to 125,000 euros or one of these penalties only. The court with which an appeal is lodged pronounces the cessation of the processing contrary to the provisions of the aforementioned articles and a penalty payment, the maximum of which is set by the aforementioned court.

(4) The National Data Protection Commission and the Public Prosecutor shall cooperate for the administrative or criminal enforcement of infringements or breaches of the provisions of this Act and those of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework. To this end, the National Data Protection Commission, the Public Prosecutor and the Grand Ducal Police may exchange any information they deem useful or necessary.

(5) Where there are indications that justify the opening of administrative proceedings by the National Data Protection Commission liable to result in the imposition of an administrative sanction for one or more facts constituting an infringement of paragraph 8 or Articles 48 and 49 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, the National Data Protection Commission shall inform the Public Prosecutor, who decides, within two months of the receipt of this information, whether prosecution will be initiated. In this case, he shall inform the National Data Protection Commission of its decision.

If the Public Prosecutor decides to prosecute, the National Data Protection Commission shall refrain from proceeding. In the event of a negative decision or in the absence of a response from the Public Prosecutor after the two-month period, the National Data Protection Commission proceeds in accordance with the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework.

Where, during the proceedings, the National Data Protection Commission finds the existence of indications that the suspected persons may have infringed the provisions of paragraph 8 or

of Articles 48 and 49 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, it shall relinquish the case and transmit it to the Public Prosecutor, who proceeds in accordance with the Code of Criminal Procedure.

If, during the course of the investigation and before summoning to appear, the Public Prosecutor considers that the conditions for a criminal prosecution have not been met, but that administrative sanctions may apply, he shall transmit the case to the National Data Protection Commission, which proceeds in accordance with the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework.

(6) When a complaint based on facts liable to constitute an infringement of paragraph 8 or of Articles 48 and 49 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework is lodged with the Public Prosecutor, and he decides to prosecute, he shall inform the National Data Protection Commission. In this case, the National Data Protection Commission does not proceed. If the Public Prosecutor decides not to prosecute, the National Data Protection Commission proceeds in accordance with the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework.

If, during the course of the investigation and before summoning to appear, the Public Prosecutor considers that the conditions for a criminal prosecution have not been met, but that administrative sanctions may apply, he or she shall transmit the case to the National Data Protection Commission, which proceeds in accordance with the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework.

(7) The provisions of paragraphs 4 to 6 also apply to the judicial supervisory authority when it carries out the tasks and has the powers provided for in Regulation (EU) 2016/679.

(8) Anyone who knowingly prevents or hinders, in any way whatsoever, the execution of the tasks incumbent on the judicial supervisory authority shall be punished by imprisonment from eight days to one year and a fine of 251 to 125 000 euros or one of these penalties only.

(9) The provisions of Articles 51 to 53 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework are applicable to the judicial supervisory authority when it acts within the framework of its powers relating to Regulation (EU) 2016/679 or provided for by this Act. The Luxembourg Registration Duties, Estates and VAT Authority is responsible for the collection of penalties and periodic penalty payments imposed by the judicial supervisory authority. The procedure for registrations shall apply.

## Chapter 8 - Final provisions

### Section 1 - Amending provisions

#### Art. 48. Amended Act of 7 March 1980 on the organisation of the judicial system

Article 75-8 of the amended Act of 7 March 1980 on the organisation of the judicial system is replaced as follows:

“Art. 75-8. The right of any person to have access to personal data relating to them, which are processed by Eurojust, as provided for in Article 19 of the aforementioned Council Decision of 28 February 2002, is granted in accordance with the provisions for the right of access in Luxembourg as provided for by Articles 13, 14 and 16 of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.”

**Art. 49. Amended Act of 29 May 1998 approving the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), signed in Brussels on 26 July 1995**

Article 3 of the amended Act of 29 May 1998 approving the Convention based on Article K.3 of the Treaty on European Union on the establishment of a European Police Office (Europol Convention), signed in Brussels on 26 July 1995 is replaced as follows:

"Art. 3.

The supervisory authority provided for in Article 2, paragraph 1, point 15), letter a), of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters is designated as the national supervisory authority provided for in Article 23 of the Convention, with the task of monitoring compliance with the provisions on the protection of personal data in the context of the operation of the Europol information system."

**Art. 50. Act of 20 December 2002 approving - the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, signed in Brussels on 26 July 1995; - the Agreement relating to the provisional application between certain Member States of the European Union of the Convention drawn up on the basis of Article K.3 of the Treaty on European Union on the use of information technology for customs purposes, signed in Brussels on 26 July 1995**

Article 2 of the Act of 20 December 2002 approving - the Convention drawn up on the basis of article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, signed in Brussels, on July 26, 1995; - the Agreement relating to the provisional application between certain Member States of the European Union of the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, signed in Brussels on 26 July 1995 is replaced as follows:

"Art. 2.

The supervisory authority provided for in Article 2, paragraph 1, point 15), letter a), of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters is designated as the national supervisory authority provided for in Article 17 of the Convention, with the task of monitoring compliance with the provisions on the protection of personal data in the context of the operation of the customs information system."

**Art. 51. Amended Act of 15 June 2004 relating to the classification of documents and security clearances**

In Article 23 of the amended Act of 15 June 2004 relating to the classification of documents and security clearances, the first paragraph is replaced as follows:

"The processing, by the National Security Authority, of the information collected within the framework of its duties is carried out in accordance with the provisions of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters."

**Art. 52. Amended Act of 16 June 2004 on the Reorganisation of the State Socio-educational Centre**

The amended Act of 16 June 2004 on the Reorganisation of the State Socio-educational Centre is amended as follows:

1. In paragraph 4, subparagraph 2 of Article 11bis, the first sentence is replaced as follows:

""“The Public Prosecutor is considered, with regard to the processing of personal data, as controller within the meaning of Article 4, point 7, of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as 'Regulation (EU) 2016/279'.”

2. In paragraph 4, subparagraph 3 of Article 11bis, the first sentence is replaced as follows:

“The director of the centre is considered as controller within the meaning of Article 4, point 7), of Regulation (EU) 2016/679 with regard to the processing of personal data in the context of the accommodation and supervision of the resident.”

**Art. 53. Amended Act of 25 August 2006 relating to identification procedures by genetic fingerprinting in criminal matters and amending the Code of Criminal Procedure**

The amended Act of 25 August 2006 relating to procedures for identification by genetic fingerprinting in criminal matters and amending the Code of Criminal Procedure is amended as follows:

1. In Article 1, the second sentence is replaced as follows:

“The processing of this data is subject to the requirements of Article 9 of the Act of 1 August 2018 on to the protection of natural persons with regard to the processing of personal data in criminal and national security matters.”

2. In Article 13, paragraph 2 is replaced as follows:

“(2) An established DNA profile is to be considered as personal data, within the meaning of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters, from the moment when the alphanumeric code of the DNA analysis has been associated with information relating to the natural person in question making it possible to identify them.”

**Art. 54. Act of 24 June 2008 relating to the control of travellers in accommodation establishments**

In Article 3 of the Act of 24 June 2008 relating to the control of travellers in accommodation establishments, the first sentence is replaced as follows:

“The accommodation provider is obliged to communicate the accommodation file related to persons accommodated to the Grand-Ducal Police for the purposes of the prevention and detection of criminal offences, the investigation and prosecution thereof or the execution of criminal penalties, including the protection against threats to public security and the prevention of such threats.”

**Art. 55. Act of 29 March 2013, as amended, relating to the organisation of criminal records**

In Article 8 of the amended Act of 29 March 2013 on the organisation of criminal records, the second sentence of point 2 is replaced as follows:

“On a quarterly basis, the SRE sends the judicial supervisory authority a list of its requests for issuance and the reasons for these requests provided for in Article 40 of the Act of 1 August 2018 on to the protection of natural persons with regard to the processing of personal data in criminal and national security matters”

**Art. 56. Amended Act of 19 December 2014 facilitating the cross-border exchange of information concerning road safety offenses**

Article 6 of the amended Act of 19 December 2014 facilitating the cross-border exchange of information concerning road safety offenses is replaced as follows:

“Art. 6.

(1) The processing of personal data within the framework of this Act is carried out for the purposes of prevention, investigation and establishment of criminal or administrative offences falling within its scope and is carried out in accordance with Articles 24 to 32 of the aforementioned Decision 2008/615/JHA and the thereto not contrary provisions of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.

(2) Any data subject has the right to obtain information about the personal data transmitted under this Act, including the date of the request and the competent authority of the Member State of the offence, in accordance with Articles 11 to 17 of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.”

**Art. 57. Amended Act of 25 July 2015 on the creation of an automated control and sanction system**

Article 10 of the amended Act of 25 July 2015 on the creation of an automated control and sanction system is replaced as follows:

“Art. 10.

The Centre processes personal data, which are necessary for the accomplishment of its duties which are carried out in accordance with the provisions of the Act of 1 August 2018 on to the protection of natural persons with regard to the processing of personal data in criminal and national security matters.”

**Art. 58. Act of 5 July 2016 on the reorganisation of the State Intelligence Service**

The Act of 5 July 2016 on the reorganisation of the State Intelligence Service is amended as follows:

1. In paragraph 4 of Article 9, the last sentence is replaced as follows:

“Subject to the conditions defined in the first paragraph, the SRE may directly exchange personal data with foreign intelligence services, including by means of shared transmission facilities, in accordance with Articles 34 and 38 of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.”

2. Paragraph 1 of Article 10 is replaced as follows:

“(1) The SRE processes the personal data, which are necessary for the accomplishment of its legal duties, in accordance with the provisions of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.”

3. Paragraph 2.3 of Article 10 is replaced as follows:

“On a quarterly basis, the SRE sends a list of its requests for issuance and the reasons for these requests to the judicial supervisory authority provided for in Article 40 of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.”

4. Paragraph 3.1 of Article 10 is replaced as follows:

“The director is controller with regard to the data referred to in paragraphs 1 and 2. He or she shall appoint a data protection officer, who, under the authority of the director, is charged with the consistent application of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters and the implementation of security measures for the processing carried out by the SRE.”

**Art. 59. Act of 23 July 2016 establishing a specific status for certain personal data processed by the State Intelligence Service**

The Act of 23 July 2016 establishing a specific status for certain personal data processed by the State Intelligence Service is amended as follows:

1. Paragraph 11 of Article 3 is replaced as follows:

“(11) During the exercise of the tasks of the experts, the director of the State Intelligence Service is the controller within the meaning of Article 2, point 8), of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters, and the National Archives are considered to be a processor of the State Intelligence Service within the meaning of Article 2, point 9), of the same law.”

2. The first sentence of paragraph 15 of Article 3 is replaced as follows:

“The final report may not contain any personal data or any element likely to allow the identification of a person without the express consent of the data subject, in accordance with Article 6, paragraph 1, letter a), of Regulation (EU) 2016/679.”

3. Point 1 of paragraph 2 of Article 4 is replaced as follows:

“1. The historical databases identified within the meaning of Article 3, paragraph 6, point 2, are definitively transferred to the National Archives as provided for in Article 7 of the amended Act of 25 June 2004 on the reorganisation of the cultural institutes of the State and subject to the provisions of Regulation (EU) 2016/679. The National Archives becomes the controller for the data from the date of final transfer;”

4. Paragraphs 1 and 2 of Article 5 are replaced by the following:

“(1) Access by a data subject to data concerning him or her during the execution of the tasks of the experts is carried out in accordance with the provisions of Articles 13, 14 and 16 of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.

(2) Personal data, noted during the experts' tasks and covering persons who have already submitted a request for access, are communicated to the data subject in accordance with the provisions referred to in paragraph 1.”

5. Paragraph 5 of Article 5 is replaced as follows:

“(5) In the execution of their tasks, the experts shall have complete access to the historical databases of the State Intelligence Service as well as access to the personal data and shall process the data in accordance with the principle of lawfulness within the meaning of Article 5, paragraph 1, letter b), of Regulation (EU) 2016/679.”

**Art. 60. Act of 22 February 2018 on the exchange of personal data and information in police matters**

The Act of 22 February 2018 on the exchange of personal data and information in police matters is amended as follows:

1. In Article 1, point 3), the words “of Articles 18 and 19 of the amended Act of 2 August 2002 on data protection with regard to the processing of personal data” are replaced by the words “of Chapter V of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters”.”
2. Paragraph 2 of Article 25 is replaced as follows:

   “(2) The transmission of data and information is carried out in a form that allows the National Data Protection Commission to verify whether all the conditions required by law were met at the time of transmission. The documentation of the transmission must be kept for a period of two years.”
3. Paragraph 1 of Article 26 is replaced as follows:

   “(1) The data and information transmitted to the relevant administration of the State form part of the processing activities for which the administration or its representative is the controller within the meaning of Article 4, point 7), of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The National Data Protection Commission is competent to verify the application of the provisions of the aforementioned Regulation and the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.”
4. Article 28 is replaced as follows:

   “The National Data Protection Commission monitors and verifies compliance with the conditions of access provided for by this Act. The report to be sent to the Minister in charge of Data Protection, pursuant to Article 10 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, contains a specific part relating to the performance of its supervisory duties carried out under this Act.”

**Art. 61. Act of 18 July 2018 on the Grand Ducal Police**

In Article 43 of the Act of 18 July 2018 on the Grand-Ducal Police, paragraph 6 is replaced as follows:

“The supervisory authority provided for in Article 2, paragraph 1, point 15), letter a), of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters monitors and verifies compliance with the access conditions provided for by this Article. The report to be sent to the Minister in charge of Data Protection, pursuant to Article 10 of the Act of 1 August 2018 on the organisation of the

National Data Protection Commission and the general data protection framework, contains a specific part relating to the performance of its supervisory tasks carried out under this Article."

### Art. 62. Act of 18 July 2018 on the General Police Inspectorate

Article 15 of the Act of 18 July 2018 on the General Police Inspectorate is amended as follows:

1. Paragraph 3 is replaced as follows:

"(3) Within the framework of the tasks set out in Articles 4, 7 and 9, the GPI has access to the access logs for the processing of personal data for which the Director General of the Police is the controller."

2. Paragraph 6 is replaced as follows:

"(6) The supervisory authority provided for in Article 2, paragraph 1, point 15), letter a), of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters monitors and verifies compliance with the access conditions provided for in this Article. The report to be sent to the Minister in charge of Data Protection, pursuant to Article 10 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, contains a specific part relating to the performance of its supervisory tasks carried out under this Article."

## Section 2 - Transitional provisions, compliance and reference title

### Art. 63. Transitional provisions and compliance

(1) Exceptionally and if it requires disproportionate effort, automated personal data processing systems installed before 6 May 2016 shall be brought into compliance with Article 24 by 6 May 2023 at the latest.

(2) By way of derogation from paragraph 1, and in exceptional circumstances, the automated personal data processing system referred to in paragraph 1 may be brought into compliance with Article 24 by a date to be determined by a decision of the Government Council and after 6 May 2023 when, failing this, serious difficulties arise for the operation of the automated processing system in question. The deadline cannot be set beyond 6 May 2026.

### Art. 64. Reference title

The reference to this Act shall be as follows: "Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters".