HOUSE DOCKET, NO. 3521 FILED ON: 2/19/2021

HOUSE . . . . . No. 4152

The Commonwealth of Massachusetts

PRESENTED BY:

Russell E. Holmes

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act establishing an internet bill of rights.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
Russell E. Holmes	*6th Suffolk*	*2/19/2021*

HOUSE DOCKET, NO. 3521 FILED ON: 2/19/2021

HOUSE . . . . . No. 4152

By Mr. Holmes of Boston, a petition (accompanied by bill, House, No. 4152) of Russell E. Holmes relative to providing for protections in the processing of personal data and the free movement of personal data. The Judiciary.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Second General Court
(2021-2022)

An Act establishing an internet bill of rights.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws are hereby amended by inserting after chapter 93L the following chapter:-

Chapter 93M

Internet Bill of Rights

Section 1. As used in this chapter the following terms shall, unless the context clearly requires otherwise, have the following meanings:

"Binding corporate rules", personal data protection policies adhered to by a controller or processor established in the commonwealth for transfers or a set of transfers of personal data to a controller or processor in 1 or more locations outside the commonwealth within a group of undertakings, or group of enterprises engaged in a joint economic activity.

"Biometric data", personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person that allows or confirms the unique identification of the natural person, such as facial images or dactyloscopic data.

"Consent", any freely given, specific, informed and unambiguous indication of a data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the data subject.

"Controller", the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; provided, that where the purposes and means of processing are determined by general or special law, the controller or the specific criteria for its nomination may be provided for by general or special law.

"Cross-border processing", either: (i) processing of personal data that takes place in the context of the activities of establishments in the commonwealth and 1 or more locations outside the commonwealth of a controller or processor in the commonwealth where the controller or processor is established in the commonwealth and 1 or more locations outside the commonwealth; or (ii) processing of personal data that takes place in the context of the activities of a single establishment of a controller or processor in the commonwealth but which substantially affects or is likely to substantially affect data subjects in the commonwealth and 1 or more locations outside the commonwealth.

"Data concerning health", personal data related to the physical or mental health of a natural person, including the provision of health care services, that reveals information about the person's health status.

"Data subject", an identified or identifiable natural person.

"Enterprise", a natural or legal person engaged in an economic activity, irrespective of the person's legal form, including partnerships or associations regularly engaged in an economic activity.

"Filing system", any structured set of personal data that is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

"Foreign destination", another state, a foreign country, a territory of the United States or a foreign country or an organization located outside the commonwealth.

"Genetic data", personal data relating to the inherited or acquired genetic characteristics of a natural person that gives unique information about the physiology or the health of the natural person and which result, in particular, from an analysis of a biological sample from the natural person.

"Group of undertakings", a controlling undertaking and its controlled undertakings.

"Identifiable natural person", a natural person who may 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 1 or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Information society service", any service normally provided for remuneration, without the parties being simultaneously present, by electronic means and at the individual request of a recipient of services. A service shall be deemed provided by electronic means if the service is sent initially and received at the service's destination by means of electronic equipment for the processing, including digital compression, and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means.

"International organization", an organization and the organization's subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between 2 or more countries.

"Joint controllers", 2 or more controllers that jointly determine the purposes and means of processing.

"Main establishment", the place of a controller or processor's central administration in the commonwealth; provided, however, that if the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the commonwealth and the latter establishment has the power to have such decisions implemented, the establishment having taken the decisions shall be considered to be the main establishment; and, provided further, that if a processor has no central administration in the commonwealth, the main establishment shall be the establishment of the processor in the commonwealth where the main processing activities in the context of the activities of an establishment of the processor take place, to the extent that the processor is subject to specific obligations under this chapter.

"Personal data", any information relating to a data subject.

"Personal data breach", a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"Processing", any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor", a natural or legal person, public authority, agency or other body that processes personal data on behalf of a controller.

"Profiling", 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 analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

"Pseudonymization", 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 the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to a data subject.

"Recipient", a natural or legal person, public authority, agency or another body, to which personal data is disclosed, whether a third party or not; provided, however, that public authorities that receive personal data in the framework of a particular inquiry in accordance with general or

special law shall not be regarded as recipients and the processing of data by said public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

"Relevant and reasoned objection", an objection to a draft decision as to whether there is an infringement of this chapter, or whether envisaged action in relation to the controller or processor complies with this chapter, which clearly demonstrates the significance of the risks posed by the draft decision regarding the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the commonwealth.

"Representative", a natural or legal person established in the commonwealth who, designated by the controller or processor in writing pursuant to section 21, represents the controller or processor with regard to the respective obligations of the controller or processor described in this chapter.

"Restriction of processing", the marking of stored personal data with the aim of limiting processing of the data in the future.

"Third party", a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, is authorized to process personal data.

Section 2. (a) Natural persons shall be entitled to protections relative to the processing of personal data and the free movement of personal data. Natural persons possess a right to the protection of personal data. The free movement of personal data within the commonwealth shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

(b) This chapter shall apply 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.

This chapter shall not apply to the processing of personal data: (i) in the course of an activity that falls outside the scope of the commonwealth's authority; (ii) by a natural person in the course of a purely personal or household activity; or (iii) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

(c) This chapter shall apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the commonwealth, regardless of whether the processing takes place in the commonwealth.

(d) This chapter shall apply to the processing of personal data of data subjects who are in the commonwealth by a controller or processor not established in the commonwealth where the processing activities are related to: (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the commonwealth; or (ii) the monitoring of data subjects' behavior as far as the behavior takes place within the commonwealth.

Section 3. (a) Personal data shall be: (i) processed lawfully, fairly and in a transparent manner in relation to the data subject; (ii) collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (iii) adequate, relevant and limited to what is necessary in relation to the purposes for which it is

processed; (iv) accurate and, where necessary, kept up to date; (v) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and (vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

(b) The controller shall be responsible for, and be able to demonstrate compliance with, subsection (a).

(c) Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with subsection (a) of section 62, not be considered to be incompatible with the initial purposes of collection described in clause (ii) of subsection (a). Personal data may be stored for longer than described in clause (v) of said subsection (a) if the personal data shall be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with subsection (a) of section 62; provided, that the storage shall be subject to implementation of the appropriate technical and organizational measures required by this chapter in order to safeguard the rights and freedoms of the data subject.

(d) Every reasonable step shall be taken to ensure that inaccurate personal data, having regard to the purposes for which it is processed, is erased or rectified without delay.

Section 4. (a) Processing shall be legal only if and to the extent that at least 1 of the following applies:

(i) the data subject has given consent to the processing of the data subject’s personal data for 1 or more specific purposes;

(ii) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(iii) processing is necessary for compliance with a legal obligation to which the controller is subject;

(iv) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(v) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(vi) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child; provided, however, that this clause shall not apply to processing carried out by public authorities in the performance of official tasks.

(b) State agencies may maintain or introduce more specific provisions to adapt the application of the rules of this chapter with regard to processing for compliance with clauses (iii) and (v) of subsection (a) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing, including for other specific processing situations as provided for in sections 85 to 91, inclusive.

(c) The basis for the processing described in clauses (iii) and (v) of subsection (a) shall be determined by the attorney general.

The purpose of the processing shall be determined by the attorney general. The attorney general shall promulgate rules and regulations necessary to implement this chapter, including but not limited to regulations regarding: (i) the general conditions governing the lawfulness of processing by the controller; (ii) the types of data subject to the processing; (iii) the data subjects concerned; (iv) the entities to, and the purposes for which, the personal data may be disclosed; (v) the purpose limitation described in clause (ii) of subsection (a) of section 3; (vi) storage periods; and (vii) processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in sections 85 to 91, inclusive. The regulations shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Where the processing for a purpose other than that for which the personal data has been collected is not based on the data subject's consent, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data was initially collected, consider: (1) any link between the purposes for which the personal data was collected and the purposes of the intended further processing; (2) the context in which the personal data was collected, in particular regarding the relationship between data subjects and the controller; (3) the nature of the personal data, in particular whether special categories of personal data is processed, pursuant to subsections (a) to (c), inclusive, of section 6, or whether personal data related to criminal convictions and offenses is processed, pursuant to subsection (d) of said section 6; (4) the possible consequences of the intended further processing for data subjects; and (5) the existence of appropriate safeguards, which may include encryption or pseudonymization.

Section 5. (a) Where processing is based on consent, the controller shall be able to demonstrate that the data subject consented to processing of the data's subject's personal data.

(b) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of the declaration that constitutes a violation of this chapter shall not be binding.

(c) A data subject shall have the right to withdraw the data subject's consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before the withdrawal. Prior to giving consent, the data subject shall be informed that the data subject is giving consent. Withdrawing consent shall be as easy as giving consent.

(d) When assessing whether consent is freely given, consideration shall be given as to whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

(e) Where clause (i) of subsection (a) of section 4 applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. The controller shall make reasonable efforts to verify that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

Section 6. (a) 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 prohibited.

(b) Subsection (a) shall not apply if:

(i) the data subject has given explicit consent to the processing of personal data for 1 or more specified purposes, except where general, special or federal law provides that the prohibition referred to in subsection (a) may not be lifted by the data subject;

(ii) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by general, special or federal law or a collective agreement pursuant to a general or special law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(iii) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(iv) processing is carried out in the course of legitimate processing activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim; provided, that the processing relates solely to the members or to former members of the body or to persons who have regular contact with the body in connection with the body’s purposes and that the personal data is not disclosed outside that body without the consent of the data subjects;

(v) processing relates to personal data which is manifestly made public by the data subject;

(vi) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

(vii) processing is necessary for reasons of substantial public interest, on the basis of a general or special law that shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(viii) processing is necessary for the purposes of: (1) preventive or occupational medicine; (2) the assessment of the working capacity of the employee; (3) medical diagnosis; (4) the provision of health or social care; or (5) treatment or the management of health or social care systems and services on the basis of general or special law;

(ix) processing is necessary pursuant to contract with a health professional and subject to the conditions and safeguards described in subsection (c);

(x) processing is necessary for reasons of public interest in the area of public health, including but not limited to protecting against serious threats to health or ensuring high standards of quality and safety of health care, on the basis of a general, special or federal law that provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(xi) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with subsection (a) of section

62 based on general or special law that shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(c) Personal data referred to in subsection (a) may be processed for the purposes referred to in clauses (viii) and (ix) of subsection (b) when the data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy pursuant to state or federal law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under state or federal law or rules established by national competent bodies.

State agencies may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

(d) Processing of personal data relating to criminal convictions and offences or related security measures based on subsection (a) of section 4 shall be carried out only under the control of official authority or when the processing is authorized by general or special law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

(e) If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this chapter; provided, that if the controller is able to demonstrate that the controller is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible; and, provided further, that sections 10 to 15,

inclusive, shall not apply except where the data subject, for the purpose of exercising the data subject's rights under said sections, provides additional information enabling the data subject's identification.

Section 7. (a) The controller shall take appropriate measures to provide any information referred to in sections 8 and 9 and any communication pursuant to sections 10 to 17, inclusive, and section 28 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally; provided, that the identity of the data subject is proven by other means.

(b) The controller shall facilitate the exercise of data subject rights pursuant to sections 10 to 17. In the cases referred to in subsection (e) of section 6, the controller shall not refuse to act on the request of the data subject for exercising the data subject's rights pursuant to said sections 10 to 17, unless the controller demonstrates that the controller is not in a position to identify the data subject.

(c) The controller shall provide information on action taken on a request pursuant to sections 10 to 17 to the data subject without undue delay and in any event within 1 month of receipt of the request; provided, however, that the period to provide information may be extended by 2 further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any extension within 1 month of receipt of the request, together with the reasons for the delay. Where the data subject makes the

request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(d) If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within 1 month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the attorney general and seeking a judicial remedy.

(e) Information provided pursuant to sections 8 and 9 and any communication and any actions taken pursuant to sections 10 to 17, inclusive, and section 28 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: (i) charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

(f) Notwithstanding subsection (e) of section 6, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in sections 10 to 16, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

(g) The information to be provided to data subjects pursuant to sections 8 and 9 may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically, the icons shall be machine-readable.

Section 8. (a) Where personal data relating to a data subject is collected from the data subject, the controller shall, at the time when personal data is obtained, provide the data subject with all of the following information:

(i) the identity and the contact details of the controller and, where applicable, of the controller's representative;

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

(iii) the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;

(iv) where the processing is based on clause (vi) of subsection (a) of section 4, the legitimate interests pursued by the controller or by a third party; and

(v) the recipients or categories of recipients of the personal data, if any.

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

(vii) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability;

(viii) where the processing is based on clause (i) of subsection (a) of section 4 or clause (i) of subsection (b) of section 6, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(ix) the right to lodge a complaint with the attorney general;

(x) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and

(xi) the existence of automated decision-making, including profiling, referred to in section 17 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the predicted consequences of the processing for the data subject.

(b) Where the controller intends to further process the personal data for a purpose other than that for which the personal data was collected, the controller shall provide the data subject prior to further processing with information on the other purpose and any relevant further information described in subsection (a).

(c) Subsections (a) and (b) shall not apply where and insofar as the data subject already has the information.

Section 9. (a) Where personal data has not been obtained from the data subject, the controller shall provide the data subject with the following information:

(i) the identity and the contact details of the controller and, where applicable, of the controller's representative;

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

(iii) the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;

(iv) the categories of personal data concerned;

(v) the recipients or categories of recipients of the personal data, if any

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

(vii) where the processing is based on clause (vi) of subsection (a) of section 4, the legitimate interests pursued by the controller or by a third party;

(viii) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(ix) where processing is based on clause (i) of subsection (a) of section 4 or clause (i) of subsection (b) of section 6, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(x) the right to lodge a complaint with the attorney general;

(xi) from which source the personal data originates and, if applicable, whether it came from publicly accessible sources; and

(xii) the existence of automated decision-making, including profiling, referred to section 17 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the predicted consequences of the processing for the data subject.

(b) The controller shall provide the information referred to in subsection (a) within a reasonable period after obtaining the personal data, but at the latest within 1 month, having regard to the specific circumstances in which the personal data is processed; provided, that if the personal data is to be used for communication with the data subject, the controller shall provide

the information at the latest at the time of the first communication to that data subject; and provided further, that if a disclosure to another recipient is envisaged, the controller shall provide the information at the latest when the personal data is first disclosed.

(c) Where the controller intends to further process the personal data for a purpose other than that for which the personal data was obtained, the controller shall provide the data subject prior to further processing with information on the other purpose and any relevant further information described in subsection (a).

(d) Subsections (a) to (c), inclusive, shall not apply if:

(i) the data subject already has the information;

(ii) the provision of the information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in subsection (a) of section 62 or in so far as the obligation referred to in subsection (a) is likely to render impossible or seriously impair the achievement of the objectives of the processing; provided, that the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(iii) obtaining or disclosure is expressly required by state or federal law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(iv) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by state or federal law, including a statutory obligation of secrecy.

Section 10. (a) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning the data subject is being processed. If personal data concerning the data subject is being processed, the data subject shall have the right to access:

(i) the personal data;

(ii) the purposes of the processing;

(iii) the categories of personal data concerned;

(iv) the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in foreign destinations;

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

(vi) 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 or to object to such processing;

(vii) the right to lodge a complaint with the attorney general;

(viii) where the personal data is not collected from the data subject, any available information as to the source of the personal data; and

(ix) the existence of automated decision-making, including profiling, referred to in section 17 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the predicted consequences of the processing for the data subject.

(b) Where personal data is transferred to a foreign destination, the data subject shall have the right to be informed of the appropriate safeguards pursuant to section 40 relating to the transfer.

(c) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy of personal data shall not adversely affect the rights and freedoms of others.

Section 11. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning the data subject. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Section 12. (a) The data subject shall have the right to obtain from the controller the erasure of personal data concerning the data subject without undue delay and the controller shall have the obligation to erase personal data without undue delay if:

(i) the personal data is no longer necessary in relation to the purposes for which the personal data was collected or otherwise processed;

(ii) the data subject withdraws consent on which the processing is based pursuant to clause (i) of subsection (a) of section 4 or clause (i) of subsection (b) of section 6, and there is no other legal ground for the processing;

(iii) the data subject objects to the processing pursuant to subsection (a) of section 16 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to subsection (b) of said section 16;

(iv) the personal data was unlawfully processed;

(v) the personal data must be erased for compliance with a legal obligation pursuant to state or federal law to which the controller is subject; or

(vi) the personal data was collected in relation to the offer of information society services referred to in subsection (e) of section 5.

(b) Where the controller has made personal data public and is obliged required by subsection (a) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers that are processing the personal data that the data subject has requested the erasure by the controllers of any links to, or copy or replication of, the personal data.

(c) Subsections (a) and (b) shall not apply to the extent that processing is necessary for:

(i) exercising the right of freedom of expression and information;

(ii) compliance with a legal obligation that requires processing by state or federal law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(iii) reasons of public interest in the area of public health in accordance with clauses (viii) to (x), inclusive, of subsection (b) of section 6 and subsection (c) of said section 6;

(iv) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with subsection (a) of section 62 in so far as the right referred to in subsection (a) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(v) the establishment, exercise or defense of legal claims.

Section 13. (a) The data subject shall have the right to obtain from the controller restriction of processing if:

(i) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(ii) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of the use of the personal data instead;

(iii) the controller no longer needs the personal data for the purposes of the processing, but the personal data is required by the data subject for the establishment, exercise or defense of legal claims; or

(iv) the data subject objected to processing pursuant to subsection (a) of section 16 pending the verification of whether the legitimate grounds of the controller override those of the data subject.

(b) Where processing has been restricted pursuant to subsection (a), the personal data shall, with the exception of storage, only be processed with the data subject's consent or for the

establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the commonwealth.

(c) A data subject who obtained restriction of processing pursuant to subsection (a) shall be informed by the controller before the restriction of processing is lifted.

Section 14. The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with section 11, subsection (a) of section 12 and section 13 to each recipient to whom the personal data has been disclosed, unless communication proves impossible or involves disproportionate effort. The controller shall inform the data subject about recipients to which communication was impossible or involved disproportionate effort if the data subject requests the information.

Section 15. (a) The data subject shall have the right to receive the personal data concerning the data subject, which the data subject provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit the data to another controller without hindrance from the controller to which the personal data was provided, if the processing is: (i) based on consent pursuant to clause (i) of subsection (a) of section 4 or clause (i) of subsection (b) of section 6 or on a contract pursuant to clause (ii) of subsection (a) of section 4; and (ii) carried out by automated means.

In exercising the right to transmit data, the data subject shall have the right to have the personal data transmitted directly from 1 controller to another, where technically feasible.

(b) The exercise of the right described in subsection (a) shall not prejudice section 12. The right described in subsection (a) shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the

controller. The right described in subsection (a) shall not adversely affect the rights and freedoms of others.

Section 16. (a) The data subject shall have the right to object, on grounds relating to the data subject's particular situation, at any time to processing of personal data concerning the data subject that is based on clauses (v) or (vi) of subsection (a) of section 4, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

(b) Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning the data subject for the marketing, including profiling to the extent that the profiling is related to the marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for the direct marketing purposes.

(c) Not later than at the time of the first communication with the data subject, the right to object described in subsections (a) and (b) shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(d) In the context of the use of information society services, the data subject may exercise the data subject's right to object by automated means using technical specifications.

(e) Where personal data is processed for scientific or historical research purposes or statistical purposes pursuant to subsection (a) of section 62, the data subject, on grounds relating to the data subject's particular situation, shall have the right to object to processing of personal

data concerning the data subject, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Section 17. (a) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject.

(b) Subsection (a) shall not apply if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller or based on the data subject's explicit consent; provided, that the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express the data subject’s point of view and to contest the decision.

(c) Subsection (a) shall not apply if the decision is authorized by state or federal law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; provided, that the decision shall not be based on special categories of personal data referred to in subsection (a) of section 6 unless clause (i) or (vi) of subsection (b) of said section 6 applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 18. (a) 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, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this

chapter. The measures shall be reviewed and updated where necessary. Where proportionate in relation to processing activities, the measures shall include the implementation of appropriate data protection policies by the controller.

(b) Adherence to approved codes of conduct as referred to in section 34 or approved certification mechanisms as referred to in section 36 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Section 19. (a) 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, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this chapter and protect the rights of data subjects.

The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed, including but not limited, to the amount of personal data collected, the extent of processing, the period of storage and accessibility to the data. In particular, the measures shall ensure that by default personal data is not made accessible without the individual's intervention to an indefinite number of natural persons.

(b) An approved certification mechanism pursuant to section 36 may be used as an element to demonstrate compliance with subsection (a).

Section 20. Joint controllers shall, in a transparent manner, determine the joint controllers' respective responsibilities for compliance with the obligations pursuant to this chapter, in particular as regards the exercising of the rights of the data subject and the joint controllers' respective duties to provide the information referred to in sections 8 and 9, by means of an arrangement between the joint controllers unless, and in so far as, the respective responsibilities of the controllers are determined by state or federal law to which the controllers are subject. The arrangement may designate a contact point for data subjects; provided, that the arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject; and, provided further that the data subject may exercise the data subject's rights pursuant to this chapter in respect of and against each of the controllers.

Section 21. (a) Where subsection (d) of section 2 applies, the controller or the processor shall designate in writing a representative in the commonwealth.

(b) Subsection (a) shall not apply to: (i) processing that is occasional, does not include, on a large scale, processing of special categories of data as referred to in subsection (a) of section 6 or processing of personal data relating to criminal convictions and offenses referred to in subsection (d) of said section 6, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (ii) a public authority or body.

(c) The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, the attorney general and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this chapter.

(d) The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Section 22. (a) 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 organizational measures in such a manner that processing will meet the requirements of this chapter and ensure the protection of the rights of the data subject.

(b) The processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, 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.

(c) Processing by a processor shall be governed by a contract or other legal act pursuant to state or federal law 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. The contract or other legal act shall stipulate, in particular, that the processor:

(i) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to foreign destinations, unless required to do

so by state or federal law to which the processor is subject; provided, that, the processor shall inform the controller of the legal requirement before processing, unless the law prohibits the information on important grounds of public interest;

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

(iii) takes all measures required pursuant to section 26;

(iv) respects the conditions referred to in subsections (b) and (d) for engaging another processor;

(v) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights described in sections 7 to 17, inclusive;

(vi) assists the controller in ensuring compliance with the obligations pursuant to sections 26 to 30, inclusive, taking into account the nature of processing and the information available to the processor;

(vii) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless state or federal law requires storage of the personal data; and

(viii) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this section and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller;

provided, that the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Chapter or other state or federal data protection provisions.

(d) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in subsection (c) shall be imposed on the other processor by way of a contract or other legal act pursuant to state or federal law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this chapter. Where the other processor fails to fulfill said data protection obligations, the initial processor shall remain fully liable to the controller for the performance of the other processor's obligations.

(e) Adherence of a processor to an approved code of conduct as referred to in section 34 or an approved certification mechanism as referred to in section 36 may be used as an element by which to demonstrate sufficient guarantees as referred to in subsections (a) and (d).

(f) Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in subsections (b) and (c) may be based, in whole or in part, on standard contractual clauses referred to in subsection (g), including when they are part of a certification granted to the controller or processor pursuant to sections 36 and 37.

(g) The attorney general may lay down standard contractual clauses for the matters referred to in subsections (c) and (d)).

(h) The contract or the other legal act referred to in subsections (c) and (d) shall be in writing, including in electronic form.

(i) Without prejudice to sections 55 to 57, inclusive, if a processor infringes this chapter by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Section 23.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 the data except on instructions from the controller, unless required to do so by state or federal law.

Section 24. (a) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under the responsibility of the controller or representative. The record shall contain:

(i) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(ii) the purposes of the processing;

(iii) a description of the categories of data subjects and of the categories of personal data;

(iv) the categories of recipients to whom the personal data has been or will be disclosed including recipients in foreign destinations;

(v) where applicable, transfers of personal data to foreign destinations, including the identification of that destination and, in the case of transfers referred to in the clause (ii) of subsection (a) of section 43, the documentation of suitable safeguards;

(vi) where possible, the envisaged time limits for erasure of the different categories of data; and

(vii) where possible, a general description of the technical and organizational security measures referred to in subsection (a) of section 26.

(b) Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

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

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

(iii) where applicable, transfers of personal data to foreign destinations, including the identification of that destination and, in the case of transfers referred to in the clause (ii) of subsection (a) of section 43, the documentation of suitable safeguards; and

(iv) where possible, a general description of the technical and organizational security measures referred to in subsection (a) of section 26.

(c) The records referred to in subsections (a) and (b) shall be in writing, including in electronic form. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the attorney general on request.

(d) The obligations referred to in subsections (a) and (b) shall not apply to an enterprise or an organization employing fewer than 250 persons unless the processing by the enterprise or an organization is likely to result in a risk to the rights and freedoms of data subjects, the

processing is not occasional, or the processing includes special categories of data as referred to in subsection (a) of section 6 or personal data relating to criminal convictions and offences referred to in subsection (d) of said section 6.

Section 25. The controller and the processor and, where applicable, representatives of the controller or processor, shall cooperate, on request, with the attorney general in the performance of the attorney general's tasks pursuant to this chapter.

Section 26. (a) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, as appropriate:

(i) the pseudonymization and encryption of personal data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(b) In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction,

loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

(c) Adherence to an approved code of conduct as referred to in section 34 or an approved certification mechanism as referred to in section 36 may be used as an element by which to demonstrate compliance with the subsection (a).

(d) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process the personal data except on instructions from the controller, unless the person is required to do so by state or federal law.

Section 27. (a) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the attorney general, 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 attorney general is not made within 72 hours, the notification shall be accompanied by reasons for the delay.

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

(c) The notification referred to in subsection (a) shall, at a minimum:

(i) 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;

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

(iii) describe the likely consequences of the personal data breach; and

(iv) 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.

(d) 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.

(e) The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the attorney general to verify compliance with this section.

Section 28. (a) When 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. The communication shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in clauses (ii) to (iv), inclusive, of subsection (c) of section 27.

(b) The communication described in subsection (a) shall not be required if:

(i) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those measures that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

(ii) the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of data subjects referred to in subsection (a) is no longer likely to materialize; or

(iii) the communication would involve disproportionate effort; provided, that there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(c) If the controller has not already communicated the personal data breach to the data subject, the attorney general, having considered the likelihood of the personal data breach resulting in a high risk, may require the controller to communicate the breach or may decide that any of the conditions referred to in subsection (b) are met.

Section 29. (a) 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, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

(b) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment described in subsection (a).

(c) A data protection impact assessment described in subsection (a)shall in particular be required in the case of:

(i) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(ii) processing on a large scale of special categories of data referred to in subsection (a) of section 6 or of personal data relating to criminal convictions and offences referred to in subsection (d) of said section 6; or

(iii) a systematic monitoring of a publicly accessible area on a large scale.

(d) The attorney general shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to subsection (a).

(e) The attorney general may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

(f) The assessment shall contain, at a minimum:

(i) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(iii) an assessment of the risks to the rights and freedoms of data subjects referred to in subsection (a); and

(iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this chapter taking into account the rights and legitimate interests of data subjects and other persons concerned.

(g) Compliance with approved codes of conduct referred to in section 34 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by the controllers or processors, in particular for the purposes of a data protection impact assessment.

(h) Where appropriate, the controller shall seek the views of data subjects or representatives of data subjects on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(i) Where processing pursuant to clauses (iii) or (v) of subsection (a) of section 4: (1) has a legal basis in state or federal law to which the controller is subject; (2) that law regulates the specific processing operation or set of operations in question; and (3) a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, subsections (a) to (g), inclusive shall not apply unless the attorney generals deems it to be necessary to carry out such an assessment prior to processing activities.

(j) Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Section 30. (a) The controller shall consult the attorney general prior to processing where a data protection impact assessment pursuant to section 29 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

(b) Where the attorney general is of the opinion that the intended processing referred to in subsection (a) would infringe this chapter, in particular where the controller has insufficiently identified or mitigated the risk, the attorney general shall, within period of up to 8 weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of the powers referred to in section 46; provided, that the period may be extended by 6 weeks, taking into account the complexity of the intended processing. The attorney general shall inform the controller and, where applicable, the processor, of any extension within 1 month of receipt of the request for consultation together with the reasons for the delay. The periods may be suspended until the attorney general obtains information requested for the purposes of the consultation.

(c) When consulting the attorney general pursuant to subsection (a), the controller shall provide the attorney general with:

(i) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(ii) the purposes and means of the intended processing;

(iii) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this chapter;

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

(v) the data protection impact assessment provided for in section 29; and

(vi) any other information requested by the attorney general.

Notwithstanding subsection (a), general or special law may require controllers to consult with, and obtain prior authorization from, the attorney general in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 31. (a) The controller and the processor shall designate a data protection officer in any case where:

(i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(ii) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(iii) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to subsections (a) to (c), inclusive, of section 6 or personal data relating to criminal convictions and offences referred to in subsection (d) of said section 6.

(b) A group of undertakings may appoint a single data protection officer; provided, that a data protection officer is easily accessible from each establishment.

(c) Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several authorities or bodies, taking account of organizational structure and size.

(d) In cases other than those referred to in subsection (a), the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by state or federal law shall, designate a data protection officer. The data protection officer may act for the associations and other bodies representing controllers or processors.

(e) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in section 33. The data protection officer may be a staff member of the controller or processor, or fulfill the tasks on the basis of a service contract. The controller or the processor shall publish the contact details of the data protection officer and communicate the details to the attorney general.

Section 32. (a) The controller and the processor 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. The controller and processor shall support the data protection officer in performing the tasks referred to in section 33 by providing resources necessary to carry out the tasks and access to personal data and processing operations, and to maintain the data protection officer’s expert knowledge.

(b) The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of the tasks referred to in section 33. The data protection officer shall not be dismissed or penalized by the controller or the processor for

performing the tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

(c) Data subjects may contact the data protection officer with regard to all issues related to processing of personal data and to the exercise of data subjects' rights under this Regulation.

(d) The data protection officer shall be bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with state or federal law.

(e) The data protection officer may fulfill other tasks and duties; provided, that the controller or processor shall ensure that the tasks and duties do not result in a conflict of interests.

Section 33. The data protection officer shall:

(i) inform and advise the controller or the processor and the employees who carry out processing of controller or processor obligations pursuant to this chapter and other general or special laws regarding data protection;

(ii) monitor compliance with this chapter, with other general or special laws regarding data protection and with the policies of the controller or processor 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;

(iii) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section 29;

(iv) cooperate with the attorney general; and

(v) act as the contact point for the attorney genera; on issues relating to processing, including the prior consultation referred to in section 30, and consult, where appropriate, with regard to any other matter.

The data protection officer shall in the performance of these tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 34. (a) The attorney general shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this chapter, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

(b) Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this chapter, such as with regard to:

(i) fair and transparent processing;

(ii) the legitimate interests pursued by controllers in specific contexts;

(iii) the collection of personal data;

(iv) the pseudonymization of personal data;

(v) the information provided to the public and to data subjects;

(vi) the exercise of the rights of data subjects;

(vii) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(viii) the measures and procedures referred to in sections 18 and 19 and the measures to ensure security of processing referred to in section 26;

(ix) the notification of personal data breaches to supervisory authorities and the communication of the personal data breaches to data subjects;

(x) the transfer of personal data to foreign destinations; or

(xi) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to sections 51 and 53.

(c) In addition to adherence by controllers or processors subject to this chapter, codes of conduct approved pursuant to subsection (e) and having general validity pursuant to subsection (i) may also be adhered to by controllers or processors that are not subject to this chapter pursuant to subsections (c) and (d) of section 2 in order to provide appropriate safeguards within the framework of personal data transfers to foreign destinations pursuant to clause (iv) of subsection (b) of section 40. Said controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

(d) A code of conduct referred to in subsection (b) shall contain mechanisms which enable the body referred to in subsection (a) of section 35 to carry out the mandatory monitoring

of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the attorney general.

(e) Associations and other bodies referred to in subsection (b) which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the attorney general. The attorney general shall provide an opinion on whether the draft code, amendment or extension complies with this chapter and shall approve the draft code, amendment or extension if the draft, amendment or extension provides sufficient appropriate safeguards.

(f) The attorney general shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Section 35. (a) Without prejudice to the tasks and powers of the attorney general pursuant to subsection (b) of section 45 and subsections (a) to (c), inclusive, of section 46, the monitoring of compliance with a code of conduct pursuant to section 34 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the attorney general.

(b) A body may be accredited to monitor compliance with a code of conduct where that body has:

(i) demonstrated independence and expertise in relation to the subject-matter of the code to the satisfaction of the attorney general;

(ii) established procedures which allow the body to assess the eligibility of controllers and processors concerned to apply the code, to monitor compliance with code provisions and to periodically review code operation;

(iii) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(iv) demonstrated to the satisfaction of the attorney general that the body's tasks and duties do not result in a conflict of interests.

(c) Without prejudice to the tasks and powers of the attorney general or the provisions of sections 77 to 84, inclusive, a body shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. The body shall inform the attorney general of the actions and the reasons for taking the actions.

(d) The attorney general shall revoke the accreditation of a body if the requirements for accreditation are not, or are no longer, met or where actions taken by the body infringe this chapter.

(e) This section shall not apply to processing carried out by public authorities and bodies.

Section 36. (a) The attorney general shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this chapter of processing operations by controllers and

processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

(b) In addition to adherence by controllers or processors subject to this chapter, data protection certification mechanisms, seals or marks approved pursuant to subsection (e) may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this chapter pursuant to subsections (c) and (d) of section 2 within the framework of personal data transfers to foreign destinations pursuant to clause (v) of subsection (b) of section 40. Said controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

(c) The certification shall be voluntary and available via a process that is transparent.

(d) A certification pursuant to this section does not reduce the responsibility of the controller or the processor for compliance with this chapter and is without prejudice to the tasks and powers of the attorney general pursuant to sections 45 and 46.

(e) A certification shall be issued by the certification bodies referred to in section 37 or by the attorney general, on the basis of criteria approved by the attorney general pursuant to section 46. Where the criteria are approved by the attorney general, this may result in a common certification, the Commonwealth Data Protection Seal.

(f) The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in section 37, or where applicable, the attorney general, with all information and access to the controller or processor's processing activities that is necessary to conduct the certification procedure.

(g) Certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions; provided, that the relevant criteria continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in section 37 or by the attorney general where the criteria for the certification are not or are no longer met.

(h) The attorney general shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Section 37. (a) Without prejudice to the tasks and powers of the attorney general pursuant to subsection (b) of section 45 and subsections (a) to (c), inclusive, of section 46, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the attorney general in order to allow the attorney general to exercise their powers pursuant to clause (xiv) of subsection (a) of section 46 where necessary, issue and renew certification. The attorney general shall accredit the certification bodies.

(b) A certification body shall be accredited by the attorney general only if the body has:

(i) demonstrated independence and expertise in relation to the subject-matter of the certification to the satisfaction of the attorney general;

(ii) undertaken to respect the criteria described in subsection (e) of section 36;

(iii) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(iv) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by

the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(v) demonstrated, to the satisfaction of the attorney general, that the body's tasks and duties do not result in a conflict of interests.

(c) The accreditation of certification bodies pursuant to subsections (a) and (b) shall take place on the basis of requirements approved by the attorney general .

(d) The certification bodies shall be responsible for the proper assessment leading to the certification or the withdrawal of the certification without prejudice to the responsibility of the controller or processor for compliance with this chapter. The accreditation shall be issued for a maximum period of 5 years and may be renewed on the same conditions; provided, that the certification body meets the requirements set out in this section. The certification bodies shall provide the attorney general with the reasons for granting or withdrawing the requested certification.

(e) The requirements referred to in subsection (c) and the criteria referred to in subsection (e) of section 36 shall be made public by the attorney general in an easily accessible form.

(f) Without prejudice to sections 77 to 84, inclusive, the attorney general shall revoke an accreditation of a certification body pursuant to subsection (a) where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this chapter.

(g) The attorney general may promulgate rules and regulations: (i) specifying the requirements to be taken into account for the data protection certification mechanisms described

in subsection (a) of section 35; and (ii) laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognize those certification mechanisms, seals and marks.

Section 38. Any transfer of personal data that is undergoing processing or is intended for processing after transfer to a foreign destination shall take place only if, subject to the other provisions of this chapter, the conditions laid down in this section and sections 39 to 44, inclusive, are complied with by the controller and processor, including for onward transfers of personal data from a foreign destination to another foreign destination. All provisions in this section and sections 39 to 44, inclusive, shall be applied in order to ensure that the level of protection of natural persons guaranteed by this chapter is not undermined.

Section 39. (a) A transfer of personal data to a foreign destination may take place where the attorney general has decided that the foreign destination in question ensures an adequate level of protection. The transfer shall not require any specific authorization.

(b) When assessing the adequacy of the level of protection, the attorney general shall, in particular, take account of the following elements:

(i) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and special, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of the legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another foreign destination that are complied with in that foreign destination, case-law, as well as effective and enforceable data

subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(ii) the existence and effective functioning of 1 or more independent supervisory authorities in the state or country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising data subjects' rights and for cooperation with the supervisory authorities and the attorney general; and

(iii) the international commitments the country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from the country or organization's participation in multilateral or regional systems, in particular in relation to the protection of personal data.

(c) The attorney general, after assessing the adequacy of the level of protection, may decide, by regulation, that a foreign destination ensures an adequate level of protection within the meaning of subsection (b). The regulation shall provide for a mechanism for a periodic review, at least every 4 years, which shall take into account all relevant developments in the foreign destination. The regulation shall specify the scope and application and, where applicable, identify the supervisory authority or authorities referred to in clause (ii) of subsection (b).

(d) The attorney general shall, on an ongoing basis, monitor developments in foreign destinations that could affect the functioning of decisions adopted pursuant to subsection (c).

(e) The attorney general shall, where available information reveals, in particular following the review referred to in subsection (c), that a foreign destination no longer ensures an adequate level of protection within the meaning of subsection (b), to the extent necessary, repeal,

amend or suspend the decision referred to in subsection (c) by means of regulation without retroactive effect. On duly justified imperative grounds of urgency, the attorney general shall adopt immediately applicable regulations.

(f) The attorney general shall enter into consultations with a foreign destination with a view to remedying the situation giving rise to the decision described in subsection (e).

(g) A decision described in subsection (e) is without prejudice to transfers of personal data to the foreign destination in question pursuant to sections 40 to 43, inclusive.

(h) The attorney general shall publish a list of the states, countries, territories and organizations for which the attorney general has decided that an adequate level of protection is or is no longer ensured.

Section 40. (a) In the absence of a decision pursuant subsection (c) of section 39, a controller or processor shall only transfer personal data to a foreign destination if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(b) The appropriate safeguards may be provided for, without requiring any specific authorization from the attorney general, by:

(i) a legally binding and enforceable instrument between public authorities or bodies;

(ii) binding corporate rules in accordance with section 41;

(iii) standard data protection clauses adopted by the attorney general;

(iv) an approved code of conduct pursuant to section 34 together with binding and enforceable commitments of the controller or processor in the foreign destination to apply the appropriate safeguards, including as regards data subjects' rights; or

(v) an approved certification mechanism pursuant to section 36 together with binding and enforceable commitments of the controller or processor in the foreign destination to apply the appropriate safeguards, including as regards data subjects' rights.

(c) Subject to the authorization from the attorney general, the appropriate safeguards may also be provided for, in particular, by:

(i) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the foreign destination; or

(ii) provisions to be inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights.

Section 41. (a) The attorney general shall approve binding corporate rules, provided that the rules: (i) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including employees; (ii) expressly confer enforceable rights on data subjects with regard to the processing of the data subjects' personal data; and (iii) fulfill the requirements of subsection (b).

(b) The binding corporate rules described in subsection (a) shall specify:

(i) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of the group's members;

(ii) the data transfers or set of transfers, including the categories of personal data, the type of processing and purposes of the processing, the type of data subjects affected and the identification of the foreign destination in question;

(iii) the legally binding nature of the rules, both internally and externally;

(iv) the application of the general data protection principles, in particular purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(v) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with section 17, the right to lodge a complaint with the attorney general in accordance with section 53, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(vi) how the information on the binding corporate rules, in particular on clauses (iv) and (v), is provided to the data subjects in addition to the information required in sections 8 and 9;

(vii) the tasks of any data protection officer designated in accordance with section 31 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(viii) the complaint procedures;

(ix) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules; provided, that the mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject; and, provided further, that results of the verification shall be communicated to the person or entity referred to in clause (vii) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the attorney general;

(x) the mechanisms for reporting and recording changes to the rules and reporting those changes to the attorney general;

(xi) the cooperation mechanism with the attorney general to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the attorney general the results of verifications of the measures referred to in clause (ix);

(xii) the mechanisms for reporting to the attorney general any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a foreign destination that are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(xiii) the appropriate data protection training to personnel having permanent or regular access to personal data.

(c) The attorney general may specify by regulation the format and procedures for the exchange of information between controllers, processors and the attorney general for binding corporate rules within the meaning of this section.

Section 42. Any judgment of a court or tribunal and any decision of an administrative authority of a foreign destination requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting foreign destination and the United States or the commonwealth, without prejudice to other grounds for transfer pursuant to this chapter.

Section 43. (a) In the absence of an adequacy decision pursuant to subsection (c) of section 39, or of appropriate safeguards pursuant to section 40, including binding corporate rules, a transfer or a set of transfers of personal data to a foreign destination shall take place only if:

(i) the data subject explicitly consented to the proposed transfer, after having been informed of the possible risks of the transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(ii) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(iv) the transfer is necessary for important reasons of public interest;

(v) the transfer is necessary for the establishment, exercise or defense of legal claims;

(vi) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vii) the transfer is made from a register which, according to state or federal law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by state or federal law for consultation are fulfilled in the particular case.

(b) Where a transfer could not be based on a provision of section 39 or 40, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in subsection (a) apply, a transfer to a foreign destination may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the attorney general of the transfer. The controller shall, in addition to providing the information referred to in sections 8 and 9, inform the data subject of the transfer and of the compelling legitimate interests pursued.

(c) A transfer pursuant to subsection (b) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended

for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if those persons are to be the recipients.

(d) Clauses (i) to (iii), inclusive, of subsection (a) and subsection (b) shall not apply to activities carried out by public authorities in the exercise of their public powers.

(e) The public interest referred to in clause (iv) of subsection (a) shall be recognized in federal law or in the law of the state to which the controller is subject.

(f) In the absence of an adequacy decision, general or special law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a foreign destination.

(g) The controller or processor shall document the assessment as well as the suitable safeguards referred to in subsection (b) in the records referred to in section 24.

Section 44. In relation to foreign destinations, the attorney general shall take appropriate steps to:

(i) develop cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(ii) provide mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(iii) engage relevant stakeholders in discussion and activities aimed at furthering cooperation in the enforcement of legislation for the protection of personal data; and

(iv) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with other foreign destinations.

Section 45. (a) The attorney shall be responsible for monitoring the application of this chapter, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the commonwealth.

(b) The attorney general shall:

(i) monitor and enforce the application of this chapter;

(ii) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, including, but not limited to, activities addressed specifically to children that shall receive specific attention;

(iii) advise, in accordance with general and special law, the general court, municipalities, state agencies and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(iv) promote the awareness of controllers and processors of their obligations pursuant to this chapter;

(v) upon request, provide information to any data subject concerning the exercise of their rights pursuant to this chapter and, if appropriate, cooperate with the supervisory authorities in foreign destinations to that end;

(vi) handle complaints lodged by a data subject, or by a body, organization or association in accordance with section 54, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation

within a reasonable period, in particular if further investigation or coordination with a supervisory authority in a foreign destination is necessary;

(vii) cooperate with, including sharing information and providing mutual assistance to, supervisory authorities in foreign destinations;

(viii) conduct investigations on the application of this chapter, including on the basis of information received from a supervisory authority in a foreign destination or other public authority;

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

(x) adopt standard contractual clauses referred to in subsection (g) of section 22 and clause (iii) of subsection (b) of section 40;

(xi) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to subsection (d) of section 29;

(xii) give advice on the processing operations referred to in subsection (b) of section 30;

(xiii) encourage the drawing up of codes of conduct pursuant to subsection (a) of section 34 and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to subsection (e) of said section 34;

(xiv) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to subsection (a) of section 36, and approve the criteria of certification pursuant to subsection (e) of said section 36;

(xv) where applicable, carry out a periodic review of certifications issued in accordance with subsection (g) of section 36;

(xvi) draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to section 35 and of a certification body pursuant to section 37;

(xvii) conduct the accreditation of a body for monitoring codes of conduct pursuant to section 35 and of a certification body pursuant to section 37;

(xviii) authorize contractual clauses and provisions referred to in subsection (c) of section 40;

(xix) approve binding corporate rules pursuant to section 41;

(xx) keep internal records of infringements of this chapter and of measures taken in accordance with clause (ii) of subsection (a) of section 46; and

(xxi) fulfill any other tasks related to the protection of personal data.

(c) The attorney general shall facilitate the submission of complaints referred to in clause (vi) of subsection (b) by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

(d) The performance of the tasks described in subsection (b) shall be free of charge for the data subject and, where applicable, for the data protection officer; provided, however, that where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the attorney general may charge a reasonable fee based on administrative costs, or refuse to act on the request; and, provided further, that the attorney general shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Section 46. (a) The attorney general shall have the power to:

(i) order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information the attorney general requires for the performance of the attorney general’s duties pursuant to this chapter;

(ii) carry out investigations in the form of data protection audits;

(iii) carry out a review on certifications issued pursuant to subsection (g) of section 36;

(iv) notify the controller or the processor of an alleged infringement of this chapter;

(v) obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of the attorney general’s duties pursuant to this chapter;

(vi) obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with state or federal procedural law;

(vii) issue warnings to a controller or processor that intended processing operations are likely to infringe on this chapter;

(viii) issue reprimands to a controller or a processor where processing operations have infringed on this chapter;

(ix) order the controller or the processor to comply with the data subject's requests to exercise the data subject’s rights pursuant to this chapter;

(x) order the controller or processor to bring processing operations into compliance with this chapter, where appropriate, in a specified manner and within a specified period;

(xi) order the controller to communicate a personal data breach to the data subject;

(xii) impose a temporary or definitive limitation, including a ban on processing;

(xiii) order the rectification or erasure of personal data or restriction of processing pursuant to sections 11 to 13, inclusive, and the notification to recipients to whom the personal data has been disclosed pursuant to subsection (b) of section 12 and section 14;

(xiv) withdraw a certification or order the certification body to withdraw a certification issued pursuant to sections 36 or 37, or order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(xv) impose an administrative fine pursuant to section 56, in addition to, or instead of measures referred to in this subsection, depending on the circumstances of each individual case;

(xvi) order the suspension of data flows to a recipient in a foreign destination;

(xvii) advise the controller in accordance with the prior consultation procedure referred to section 30;

(xviii) issue, on the attorney general's initiative or on request, opinions to the general court, the governor or, in accordance with general and special law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(xix) authorize processing referred to in subsection (c) of section 30;

(xx) issue an opinion and approve draft codes of conduct pursuant to subsection (e) of section 34;

(xxi) accredit certification bodies pursuant to section 37;

(xxii) issue certifications and approve criteria of certification in accordance with subsection (e) of section 36;

(xxiii) adopt standard data protection clauses referred to in subsection (g) of section 22 and clause (iii) of subsection (b) of section 40;

(xxiv) authorize contractual clauses referred to in clause (i) of subsection (c) of section 40;

(xxv) authorize administrative arrangements referred to in clause (ii) of subsection (c) of section 40; and

(xxvi) approve binding corporate rules pursuant to section 41.

(b) The exercise of the powers conferred on the attorney general pursuant to this section shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in general and special law.

(c) The attorney general shall have the power to commence or engage otherwise in legal proceedings in order to enforce the provisions of this chapter.

(d) Annually, the attorney general shall compile a report on activities taken pursuant to this chapter, which may include a list of types of infringement notified and types of measures taken in accordance with subsection (a). The reports shall be transmitted to the clerks of the house of representatives and the senate and the joint committee on advanced information technology, the internet and cybersecurity. The attorney general shall make the reports available to the public on the attorney general’s website.

Section 47. (a) Upon adopting a decision regarding a complaint pursuant to this chapter, the attorney general shall transmit the decision to the main establishment or single establishment of the controller or processor, including a summary of the relevant facts and grounds.

(b) Where a complaint is dismissed or rejected, the attorney general shall notify the complainant and the controller.

(c) Where the attorney general dismisses or rejects parts of a complaint and acts on other parts of that complaint, a separate decision shall be adopted for each part of the complaint.

(d) After being notified of the decision, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the commonwealth. The controller or processor shall notify the measures taken for complying with the decision to the attorney general.

(e) Where, in exceptional circumstances, the attorney general has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in section 48 shall apply.

Section 48. (a) In exceptional circumstances, where the attorney general considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, the attorney general may immediately adopt provisional measures intended to produce legal effects in the commonwealth with a specified period of validity which shall not exceed 3 months.

(b) Where the attorney general has taken a measure pursuant to subsection (a) and considers that final measures need urgently be adopted, the attorney general may request an

urgent opinion or an urgent binding decision from the superior court, giving reasons for requesting such opinion or decision.

(c) The attorney general may request an urgent opinion or an urgent binding decision, as the case may be, from the superior court where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.(d) The superior court shall provide n urgent opinion or an urgent binding decision referred to in subsections (b) and (c) within 2 weeks of the request by the attorney general.

Section 49. (a) The attorney general shall, on the attorney general's own initiative or, where relevant, at the request of the general court:

(i) advise the general court on any issue related to the protection of personal data in the commonwealth, including on any proposed amendment of this chapter;

(ii) advise the general court on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(iii) issue guidelines, recommendations and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in subsection (b) of section 22;

(iv) examine, on the attorney general's own initiative, on request of the general court, any question covering the application of this chapter and issue guidelines, recommendations and best practices in order to encourage consistent application of this chapter;

(v) draw up guidelines concerning the application of measures referred to in section 46 and the setting of administrative fines pursuant to section 55;

(vi) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to sections 34 and 36;

(vii) approve the criteria of certification pursuant to subsection (e) of section 36 and maintain a public register of certification mechanisms and data protection seals and marks pursuant to subsection (h) of said section 36 and of the certified controllers or processors established in foreign destinations pursuant to subsection (g) of said section 36.;

(viii) approve the requirements referred to in subsection (c) of section 37 with a view to the accreditation of certification bodies referred to in said section 37;

(ix) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide; and

(x) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

(b) The guidelines, recommendations and best practices described in clause (iv) of subsection (a) shall include, but not be limited to, guidelines, recommendations and best practices:

(i) for further specifying the criteria and conditions for decisions based on profiling pursuant to subsection (b) of section 17;

(ii) for establishing the personal data breaches and determining the undue delay referred to in subsections (a) and (b) of section 27 and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(iii) as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in subsection (a) of section 28;

(iv) for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in section 41; and

(v) for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of subsection (a) of section 43.

(c) The attorney general shall, on the attorney general's own initiative or, where relevant, at the request of the general court, review the practical application of the guidelines, recommendations and best practices.

(d) Where the general court requests advice from the attorney general, the general court may indicate a time limit, taking into account the urgency of the matter.

(e) The attorney general shall forward the attorney general's opinions, guidelines, recommendations, and best practices to the general court and make the opinions, guidelines, recommendations and best practices public on the attorney general's website.

(f) The attorney general shall, where appropriate, consult interested parties and give interested parties the opportunity to comment within a reasonable period. The attorney general shall publish the results of the consultation procedure publicly on the attorney general's website.

Section 50. In addition to the report on activities described in subsection (d) of section 46, the attorney general shall annually compile a report regarding the protection of natural persons with regard to processing in the commonwealth and, where relevant, foreign destinations. The reports shall include a review of the practical application of the guidelines, recommendations and best practices referred to in subsection (b) of section 49. The reports shall be transmitted to the clerks of the house of representatives and the senate and the joint committee on advanced information technology, the internet and cybersecurity. The attorney general shall make the reports available to the public on the attorney general's website.

Section 51. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the attorney general, in particular if the data subject lives or works in the commonwealth or the alleged infringement took place in the commonwealth, if the data subject considers that the processing of personal data relating to the data subject infringes this chapter. The attorney general shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to section 52.

Section 52. Without prejudice to any other administrative or non-judicial remedy:

(i) each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of the attorney general concerning the natural or legal person; and

(ii) each data subject shall have the right to a an effective judicial remedy where the attorney general does not handle a complaint or does not inform the data subject within 3 months on the progress or outcome of the complaint lodged pursuant to section 51.

Proceedings against the attorney general shall be brought before the superior court. Where proceedings are brought against an opinion or decision of the attorney general, the attorney general shall forward that opinion or decision to the court.

Section 53. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with the attorney general pursuant to section 51, each data subject shall have the right to an effective judicial remedy where the data subject considers that the data subject’s rights under this chapter have been infringed as a result of the processing of the data subject’s personal data in non-compliance with this chapter. Proceedings against a controller or a processor shall be brought before the superior court.

Section 54. (a) A data subject shall have the right to mandate a not-for-profit body, organization or association to lodge a complaint on behalf of the data subject, to exercise the rights referred to in sections 51 to 53, inclusive, on behalf of the data subject and to exercise the right to receive compensation referred to in section 55 on behalf of the data subject; provided, that the body, organization or association: (i) has been properly constituted in accordance with state or federal law; (ii) has statutory objectives in the public interest; and (iii) is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data.

(b) Any body, organization or association referred to in subsection (a), independently of a data subject's mandate, has the right to lodge a complaint with the attorney general pursuant to

section 51 and to exercise the rights referred to in sections 52 and 53 if the body, organization or association considers that the rights of a data subject pursuant this chapter have been infringed as a result of the processing.

Section 55. (a) Any person who has suffered material or non-material damage as a result of an infringement of this chapter shall have the right to receive compensation from the controller or processor for the damage suffered.

(b) Any controller involved in processing shall be liable for the damage caused by processing which infringes this chapter. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this chapter specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(c) A controller or processor shall be exempt from liability as specified in subsection (b) if the controller or processor proves that the controller or processor is not in any way responsible for the event giving rise to the damage.

(d) Where more than 1 controller or processor, or both a controller and a processor, are involved in the same processing and where the controller and processor are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. Where a controller or processor has paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in subsection (b).

(e) Court proceedings for exercising the right to receive compensation shall be brought before the superior court.

Section 56. (a) The attorney general shall ensure that the imposition of administrative fines pursuant to this section in respect of infringements of this chapter referred to in subsections (d) to (f), inclusive, shall in each individual case be effective, proportionate and dissuasive.

(b) Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in subsections (vii) to (xiv), inclusive and (xvi) of section 46. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to:

(i) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by the data subjects;

(ii) the intentional or negligent character of the infringement;

(iii) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(iv) the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to sections 19 and 26;

(v) any relevant previous infringements by the controller or processor;

(vi) the degree of cooperation with the attorney general, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(vii) the categories of personal data affected by the infringement;

(viii) the manner in which the infringement became known to the attorney general, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(ix) where measures referred to in clauses (vii) to (xvi) of subsection (a) of section 46 have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(x) adherence to approved codes of conduct pursuant to section 34 or approved certification mechanisms pursuant to section 36; and

(xi) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

(c) If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this chapter, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

(d) Infringements of the following provisions shall, in accordance with subsection (b), be subject to administrative fines up to $10,000,000, or in the case of an undertaking, up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(i) the obligations of the controller and the processor pursuant to subsection (e) of section 5, subsection (e) of section 6, sections 19 to 33, inclusive, and sections 36 and 37;

(ii) the obligations of the certification body pursuant to sections 36 and 37; or

(iii) the obligations of the monitoring body pursuant to subsection(c) of section 35.

(e) Infringements of the following provisions shall, in accordance with subsection (b), be subject to administrative fines up to $20,000,000, or in the case of an undertaking, up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(i) the basic principles for processing, including conditions for consent, pursuant to sections 3 and 4, subsections (a) to (d), inclusive, of section 5, and subsections (a) to (c), inclusive, of section 6;

(ii) the data subjects' rights pursuant to sections 7 to 17, inclusive;

(iii) the transfers of personal data to a recipient in a foreign destination pursuant to sections 38 to 43, inclusive;

(iv) any obligations pursuant to general or special law adopted pursuant to sections 58 to 64, inclusive;

(v) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the attorney general pursuant to clauses (vii) to (xvi), inclusive, of subsection (a) of section 46 or failure to provide access in violation of clauses (i) to (vi), inclusive, of said subsection (a) of said section 46.

(f) Non-compliance with an order by the attorney general as referred to in clauses (vii) to (xvi), inclusive, of subsection (a) of section 46 shall, in accordance with subsection (b), be subject to administrative fines up to $20,000,000 , or in the case of an undertaking, up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

(g) Without prejudice to the corrective powers of the attorney general as referred to in clauses (vii) to (xvi), inclusive, of subsection (a) of section 46, the general court may enact

general and special laws providing rules on whether and to what extent administrative fines may be imposed on public authorities and bodies.

(h) The exercise by the attorney general of powers pursuant to this section shall be subject to appropriate procedural safeguards in accordance with state and federal law, including effective judicial remedy and due process.

Section 57. The general court may enact general and special laws providing rules on other penalties applicable to infringements of this chapter, in particular for infringements that are not subject to administrative fines pursuant to section 56, and shall take all measures necessary to ensure that they are implemented. The penalties shall be effective, proportionate and dissuasive.

Section 58. (a) The general court shall enact general or special laws to reconcile the right to the protection of personal data pursuant to this chapter with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

(b) For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, the general court shall enact general or special laws that provide for exemptions or derogations from sections 4 to 50, inclusive, and sections 59 to 64 if exemptions or derogations are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

Section 59. Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with general, special or federal law in order to

reconcile public access to official documents with the right to the protection of personal data pursuant to this chapter.

Section 60. The attorney general may further determine the specific conditions for the processing of a social security number, driver’s license number or any other identifier of general application. In that case, the social security number, driver’s license number or other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this chapter.

Section 61. The general court may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of: (i)recruitment; (ii) the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work; (iii) equality and diversity in the workplace; (iv) health and safety at work; (v) protection of employer's or customer's property; (vi) the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment; and (vii) the termination of the employment relationship. The rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

Section 62. (a) Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this chapter, for the rights and freedoms of the data subject. The safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization. The measures may include pseudonymization; provided, that the public interest, scientific or historical research purposes or statistical purposes can be fulfilled in with pseudonymization. Where said purposes can be fulfilled by further processing that does not permit or no longer permits the identification of data subjects, the purposes shall be fulfilled in that manner.

(b) Where personal data is processed for scientific or historical research purposes or statistical purposes, general or special law may provide for derogations from the rights referred to in sections 10, 11, 13 and 16 subject to the conditions and safeguards referred to in subsection (a), in so far as the rights are likely to render impossible or seriously impair the achievement of the specific purposes and the derogations are necessary for the fulfilment of those purposes.

(c) Where personal data is processed for archiving purposes in the public interest, general or special law may provide for derogations from the rights referred to in sections 10, 11, 13, 14, 15 and 16, subject to the conditions and safeguards referred to in subsection (a), in so far as the rights are likely to render impossible or seriously impair the achievement of the specific purposes and the derogations are necessary for the fulfilment of those purposes.

(d) Where processing referred to in subsections (b) and (c) serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in said subsections (b) and (c).

Section 63. The general court may enact general or special laws establishing specific rules to set out the powers of the attorney general described in clauses (v) and (vi) of subsection (a) of section 46 in relation to controllers or processors that are subject, pursuant to state or federal law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy; provided, that the rules are necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. The rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

Section 64. Churches and religious associations or communities that apply comprehensive rules relating to the protection of natural persons with regard to processing may continue to apply said rules; provided, that the rules are brought into line with this chapter; and, provided further, that the churches and religious associations or communities shall be subject to the supervision of the attorney general.

Section 65. (a) Every 4 years, the attorney general shall submit a report on the evaluation and review of this chapter to the clerks of the house of representatives and the senate and the joint committee on advanced information technology, the internet and cybersecurity. The attorney general shall make the reports available to the public on the attorney general's website. In evaluating and reviewing this chapter, the attorney general shall examine, in particular, the application and functioning of sections 38 to 44 regarding the transfer of personal data to foreign destinations, with particular regard to decisions adopted pursuant to subsection (c) of section 39. The attorney general shall take into account the positions and findings of state agencies and other relevant bodies or sources. The attorney general shall, if necessary, submit drafts of legislation to

amend this chapter, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

(b) The attorney general shall, if appropriate, submit legislative proposals with a view to amending other general or special laws on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing; including, but not limited to, the rules relating to the protection of natural persons with regard to processing by state institutions, bodies, offices and agencies and the free movement of data.

SECTION 2. Notwithstanding chapter 93M of the General Laws, agreements involving the transfer of personal data to foreign destinations which were in place prior to the effective date of this act, and which comply with state and federal law as applicable prior to the effective date of this act, shall remain in force until amended, replaced or revoked.