

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:
<i>Russell E. Holmes</i>	<i>6th Suffolk</i>	<i>2/19/2021</i>

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:

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

3 Chapter 93M

4 Internet Bill of Rights

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

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

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

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

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

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

31 “Data concerning health”, personal data related to the physical or mental health of a
32 natural person, including the provision of health care services, that reveals information about the
33 person’s health status.

34 “Data subject”, an identified or identifiable natural person.

35 “Enterprise”, a natural or legal person engaged in an economic activity, irrespective of
36 the person’s legal form, including partnerships or associations regularly engaged in an economic
37 activity.

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

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

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

47 “Group of undertakings”, a controlling undertaking and its controlled undertakings.

48 “Identifiable natural person”, a natural person who may be identified, directly or
49 indirectly, in particular by reference to an identifier such as a name, an identification number,
50 location data, an online identifier or to 1 or more factors specific to the physical, physiological,
51 genetic, mental, economic, cultural or social identity of that natural person.

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

58 “International organization”, an organization and the organization’s subordinate bodies
59 governed by public international law, or any other body which is set up by, or on the basis of, an
60 agreement between 2 or more countries.

61 “Joint controllers”, 2 or more controllers that jointly determine the purposes and means of
62 processing.

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

72 “Personal data”, any information relating to a data subject.

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

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

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

83 “Profiling”, any form of automated processing of personal data consisting of the use of
84 personal data to evaluate certain personal aspects relating to a natural person, in particular to
85 analyze or predict aspects concerning that natural person's performance at work, economic
86 situation, health, personal preferences, interests, reliability, behavior, location or movements.

87 “Pseudonymization”, the processing of personal data in such a manner that the personal
88 data can no longer be attributed to a specific data subject without the use of additional
89 information; provided, that the additional information is kept separately and is subject to
90 technical and organizational measures to ensure that the personal data is not attributed to a data
91 subject.

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

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

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

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

107 “Restriction of processing”, the marking of stored personal data with the aim of limiting
108 processing of the data in the future.

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

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

117 (b) This chapter shall apply to the processing of personal data wholly or partly by
118 automated means and to the processing other than by automated means of personal data which
119 form part of a filing system or are intended to form part of a filing system.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

225 Section 6. (a) Processing of personal data revealing racial or ethnic origin, political
226 opinions, religious or philosophical beliefs, or trade union membership, and the processing of
227 genetic data, biometric data for the purpose of uniquely identifying a natural person, data
228 concerning health or data concerning a natural person's sex life or sexual orientation shall be
229 prohibited.

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

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

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

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

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

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

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

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

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

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

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

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

268 62 based on general or special law that shall be proportionate to the aim pursued, respect the
269 essence of the right to data protection and provide for suitable and specific measures to safeguard
270 the fundamental rights and the interests of the data subject.

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

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

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

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

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

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

301 (b) The controller shall facilitate the exercise of data subject rights pursuant to sections
302 10 to 17. In the cases referred to in subsection (e) of section 6, the controller shall not refuse to
303 act on the request of the data subject for exercising the data subject's rights pursuant to said
304 sections 10 to 17, unless the controller demonstrates that the controller is not in a position to
305 identify the data subject.

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

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

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

318 (e) Information provided pursuant to sections 8 and 9 and any communication and any
319 actions taken pursuant to sections 10 to 17, inclusive, and section 28 shall be provided free of
320 charge. Where requests from a data subject are manifestly unfounded or excessive, in particular
321 because of their repetitive character, the controller may: (i) charge a reasonable fee, taking into
322 account the administrative costs of providing the information or communication or taking the
323 action requested; or (ii) refuse to act on the request. The controller shall bear the burden of
324 demonstrating the manifestly unfounded or excessive character of the request.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

372 (iv) the categories of personal data concerned;

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

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

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

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

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

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

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

387 (xii) the existence of automated decision-making, including profiling, referred to section
388 17 and, at least in those cases, meaningful information about the logic involved, as well as the
389 significance and the predicted consequences of the processing for the data subject.

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

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

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

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

402 (i) the data subject already has the information;

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

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

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

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

420 (i) the personal data;

421 (ii) the purposes of the processing;

422 (iii) the categories of personal data concerned;

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

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

427 (vi) the existence of the right to request from the controller rectification or erasure of
428 personal data or restriction of processing of personal data concerning the data subject or to object
429 to such processing;

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

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

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

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

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

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

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

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

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

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

460 (iv) the personal data was unlawfully processed;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

541

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

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

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

557 Section 18. (a) Taking into account the nature, scope, context and purposes of processing
558 as well as the risks of varying likelihood and severity for the rights and freedoms of natural
559 persons, the controller shall implement appropriate technical and organizational measures to
560 ensure and to be able to demonstrate that processing is performed in accordance with this

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

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

567 Section 19. (a) Taking into account the state of the art, the cost of implementation and the
568 nature, scope, context and purposes of processing as well as the risks of varying likelihood and
569 severity for rights and freedoms of natural persons posed by the processing, the controller shall,
570 both at the time of the determination of the means for processing and at the time of the
571 processing itself, implement appropriate technical and organizational measures, such as
572 pseudonymization, which are designed to implement data-protection principles, such as data
573 minimization, in an effective manner and to integrate the necessary safeguards into the
574 processing in order to meet the requirements of this chapter and protect the rights of data
575 subjects.

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

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

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

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

597 (b) Subsection (a) shall not apply to: (i) processing that is occasional, does not include,
598 on a large scale, processing of special categories of data as referred to in subsection (a) of section
599 6 or processing of personal data relating to criminal convictions and offenses referred to in
600 subsection (d) of said section 6, and is unlikely to result in a risk to the rights and freedoms of
601 natural persons, taking into account the nature, context, scope and purposes of the processing; or
602 (ii) a public authority or body.

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

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

610 Section 22. (a) Where processing is to be carried out on behalf of a controller, the
611 controller shall use only processors providing sufficient guarantees to implement appropriate
612 technical and organizational measures in such a manner that processing will meet the
613 requirements of this chapter and ensure the protection of the rights of the data subject.

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

618 (c) Processing by a processor shall be governed by a contract or other legal act pursuant
619 to state or federal law that is binding on the processor with regard to the controller and that sets
620 out the subject-matter and duration of the processing, the nature and purpose of the processing,
621 the type of personal data and categories of data subjects and the obligations and rights of the
622 controller. The contract or other legal act shall stipulate, in particular, that the processor:

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

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

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

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

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

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

637 (vi) assists the controller in ensuring compliance with the obligations pursuant to sections
638 26 to 30, inclusive, taking into account the nature of processing and the information available to
639 the processor;

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

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

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

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

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

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

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

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

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

671

672 Section 23. The processor and any person acting under the authority of the controller or of
673 the processor, who has access to personal data, shall not process the data except on instructions
674 from the controller, unless required to do so by state or federal law.

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

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

680 (ii) the purposes of the processing;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

719 (i) the pseudonymization and encryption of personal data;

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

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

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

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

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

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

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

737 Section 27. (a) In the case of a personal data breach, the controller shall without undue
738 delay and, where feasible, not later than 72 hours after having become aware of it, notify the
739 personal data breach to the attorney general, unless the personal data breach is unlikely to result
740 in a risk to the rights and freedoms of natural persons. Where the notification to the attorney
741 general is not made within 72 hours, the notification shall be accompanied by reasons for the
742 delay.

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

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

746 (i) describe the nature of the personal data breach including where possible, the
747 categories and approximate number of data subjects concerned and the categories and
748 approximate number of personal data records concerned;

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

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

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

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

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

760 Section 28. (a) When the personal data breach is likely to result in a high risk to the rights
761 and freedoms of natural persons, the controller shall communicate the personal data breach to the
762 data subject without undue delay. The communication shall describe in clear and plain language
763 the nature of the personal data breach and contain at least the information and measures referred
764 to in clauses (ii) to (iv), inclusive, of subsection (c) of section 27.

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

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

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

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

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

780 Section 29. (a) Where a type of processing in particular using new technologies, and
781 taking into account the nature, scope, context and purposes of the processing, is likely to result in
782 a high risk to the rights and freedoms of natural persons, the controller shall, prior to the
783 processing, carry out an assessment of the impact of the envisaged processing operations on the
784 protection of personal data. A single assessment may address a set of similar processing
785 operations that present similar high risks.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 852 (iv) where applicable, the contact details of the data protection officer;
- 853 (v) the data protection impact assessment provided for in section 29; and
- 854 (vi) any other information requested by the attorney general.

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

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

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

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

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

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

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

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

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

885 Section 32. (a) The controller and the processor shall ensure that the data protection
886 officer is involved, properly and in a timely manner, in all issues which relate to the protection of
887 personal data. The controller and processor shall support the data protection officer in
888 performing the tasks referred to in section 33 by providing resources necessary to carry out the
889 tasks and access to personal data and processing operations, and to maintain the data protection
890 officer's expert knowledge.

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

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

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

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

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

903 Section 33. The data protection officer shall:

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

907 (ii) monitor compliance with this chapter, with other general or special laws regarding
908 data protection and with the policies of the controller or processor in relation to the protection of
909 personal data, including the assignment of responsibilities, awareness-raising and training of
910 staff involved in processing operations, and the related audits;

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

913 (iv) cooperate with the attorney general; and

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

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

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

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

927 (i) fair and transparent processing;

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

929 (iii) the collection of personal data;

930 (iv) the pseudonymization of personal data;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

995 (b) In addition to adherence by controllers or processors subject to this chapter, data
996 protection certification mechanisms, seals or marks approved pursuant to subsection (e) may be
997 established for the purpose of demonstrating the existence of appropriate safeguards provided by
998 controllers or processors that are not subject to this chapter pursuant to subsections (c) and (d) of
999 section 2 within the framework of personal data transfers to foreign destinations pursuant to
1000 clause (v) of subsection (b) of section 40. Said controllers or processors shall make binding and
1001 enforceable commitments, via contractual or other legally binding instruments, to apply those
1002 appropriate safeguards, including with regard to the rights of data subjects.

1003 (c) The certification shall be voluntary and available via a process that is transparent.

1004 (d) A certification pursuant to this section does not reduce the responsibility of the
1005 controller or the processor for compliance with this chapter and is without prejudice to the tasks
1006 and powers of the attorney general pursuant to sections 45 and 46.

1007 (e) A certification shall be issued by the certification bodies referred to in section 37 or
1008 by the attorney general, on the basis of criteria approved by the attorney general pursuant to
1009 section 46. Where the criteria are approved by the attorney general, this may result in a common
1010 certification, the Commonwealth Data Protection Seal.

1011 (f) The controller or processor which submits its processing to the certification
1012 mechanism shall provide the certification body referred to in section 37, or where applicable, the
1013 attorney general, with all information and access to the controller or processor's processing
1014 activities that is necessary to conduct the certification procedure.

1015 (g) Certification shall be issued to a controller or processor for a maximum period of 3
1016 years and may be renewed under the same conditions; provided, that the relevant criteria
1017 continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies
1018 referred to in section 37 or by the attorney general where the criteria for the certification are not
1019 or are no longer met.

1020 (h) The attorney general shall collate all certification mechanisms and data protection
1021 seals and marks in a register and shall make them publicly available by any appropriate means.

1022 Section 37. (a) Without prejudice to the tasks and powers of the attorney general pursuant
1023 to subsection (b) of section 45 and subsections (a) to (c), inclusive, of section 46, certification
1024 bodies which have an appropriate level of expertise in relation to data protection shall, after
1025 informing the attorney general in order to allow the attorney general to exercise their powers
1026 pursuant to clause (xiv) of subsection (a) of section 46 where necessary, issue and renew
1027 certification. The attorney general shall accredit the certification bodies.

1028 (b) A certification body shall be accredited by the attorney general only if the body has:

1029 (i) demonstrated independence and expertise in relation to the subject-matter of the
1030 certification to the satisfaction of the attorney general;

1031 (ii) undertaken to respect the criteria described in subsection (e) of section 36;

1032 (iii) established procedures for the issuing, periodic review and withdrawal of data
1033 protection certification, seals and marks;

1034 (iv) established procedures and structures to handle complaints about infringements of
1035 the certification or the manner in which the certification has been, or is being, implemented by

1036 the controller or processor, and to make those procedures and structures transparent to data
1037 subjects and the public; and

1038 (v) demonstrated, to the satisfaction of the attorney general, that the body's tasks and
1039 duties do not result in a conflict of interests.

1040 (c) The accreditation of certification bodies pursuant to subsections (a) and (b) shall take
1041 place on the basis of requirements approved by the attorney general .

1042 (d) The certification bodies shall be responsible for the proper assessment leading to the
1043 certification or the withdrawal of the certification without prejudice to the responsibility of the
1044 controller or processor for compliance with this chapter. The accreditation shall be issued for a
1045 maximum period of 5 years and may be renewed on the same conditions; provided, that the
1046 certification body meets the requirements set out in this section. The certification bodies shall
1047 provide the attorney general with the reasons for granting or withdrawing the requested
1048 certification.

1049 (e) The requirements referred to in subsection (c) and the criteria referred to in subsection
1050 (e) of section 36 shall be made public by the attorney general in an easily accessible form.

1051 (f) Without prejudice to sections 77 to 84, inclusive, the attorney general shall revoke an
1052 accreditation of a certification body pursuant to subsection (a) where the conditions for the
1053 accreditation are not, or are no longer, met or where actions taken by a certification body infringe
1054 this chapter.

1055 (g) The attorney general may promulgate rules and regulations: (i) specifying the
1056 requirements to be taken into account for the data protection certification mechanisms described

1057 in subsection (a) of section 35; and (ii) laying down technical standards for certification
1058 mechanisms and data protection seals and marks, and mechanisms to promote and recognize
1059 those certification mechanisms, seals and marks.

1060 Section 38. Any transfer of personal data that is undergoing processing or is intended for
1061 processing after transfer to a foreign destination shall take place only if, subject to the other
1062 provisions of this chapter, the conditions laid down in this section and sections 39 to 44,
1063 inclusive, are complied with by the controller and processor, including for onward transfers of
1064 personal data from a foreign destination to another foreign destination. All provisions in this
1065 section and sections 39 to 44, inclusive, shall be applied in order to ensure that the level of
1066 protection of natural persons guaranteed by this chapter is not undermined.

1067 Section 39. (a) A transfer of personal data to a foreign destination may take place where
1068 the attorney general has decided that the foreign destination in question ensures an adequate level
1069 of protection. The transfer shall not require any specific authorization.

1070 (b) When assessing the adequacy of the level of protection, the attorney general shall, in
1071 particular, take account of the following elements:

1072 (i) the rule of law, respect for human rights and fundamental freedoms, relevant
1073 legislation, both general and special, including concerning public security, defense, national
1074 security and criminal law and the access of public authorities to personal data, as well as the
1075 implementation of the legislation, data protection rules, professional rules and security measures,
1076 including rules for the onward transfer of personal data to another foreign destination that are
1077 complied with in that foreign destination, case-law, as well as effective and enforceable data

1078 subject rights and effective administrative and judicial redress for the data subjects whose
1079 personal data are being transferred;

1080 (ii) the existence and effective functioning of 1 or more independent supervisory
1081 authorities in the state or country or to which an international organization is subject, with
1082 responsibility for ensuring and enforcing compliance with the data protection rules, including
1083 adequate enforcement powers, for assisting and advising the data subjects in exercising data
1084 subjects' rights and for cooperation with the supervisory authorities and the attorney general; and

1085 (iii) the international commitments the country or international organization concerned
1086 has entered into, or other obligations arising from legally binding conventions or instruments as
1087 well as from the country or organization's participation in multilateral or regional systems, in
1088 particular in relation to the protection of personal data.

1089 (c) The attorney general, after assessing the adequacy of the level of protection, may
1090 decide, by regulation, that a foreign destination ensures an adequate level of protection within the
1091 meaning of subsection (b). The regulation shall provide for a mechanism for a periodic review, at
1092 least every 4 years, which shall take into account all relevant developments in the foreign
1093 destination. The regulation shall specify the scope and application and, where applicable,
1094 identify the supervisory authority or authorities referred to in clause (ii) of subsection (b).

1095 (d) The attorney general shall, on an ongoing basis, monitor developments in foreign
1096 destinations that could affect the functioning of decisions adopted pursuant to subsection (c).

1097 (e) The attorney general shall, where available information reveals, in particular
1098 following the review referred to in subsection (c), that a foreign destination no longer ensures an
1099 adequate level of protection within the meaning of subsection (b), to the extent necessary, repeal,

1100 amend or suspend the decision referred to in subsection (c) by means of regulation without
1101 retroactive effect. On duly justified imperative grounds of urgency, the attorney general shall
1102 adopt immediately applicable regulations.

1103 (f) The attorney general shall enter into consultations with a foreign destination with a
1104 view to remedying the situation giving rise to the decision described in subsection (e).

1105 (g) A decision described in subsection (e) is without prejudice to transfers of personal
1106 data to the foreign destination in question pursuant to sections 40 to 43, inclusive.

1107 (h) The attorney general shall publish a list of the states, countries, territories and
1108 organizations for which the attorney general has decided that an adequate level of protection is or
1109 is no longer ensured.

1110 Section 40. (a) In the absence of a decision pursuant subsection (c) of section 39, a
1111 controller or processor shall only transfer personal data to a foreign destination if the controller
1112 or processor has provided appropriate safeguards, and on condition that enforceable data subject
1113 rights and effective legal remedies for data subjects are available.

1114 (b) The appropriate safeguards may be provided for, without requiring any specific
1115 authorization from the attorney general, by:

1116 (i) a legally binding and enforceable instrument between public authorities or bodies;

1117 (ii) binding corporate rules in accordance with section 41;

1118 (iii) standard data protection clauses adopted by the attorney general;

1119 (iv) an approved code of conduct pursuant to section 34 together with binding and
1120 enforceable commitments of the controller or processor in the foreign destination to apply the
1121 appropriate safeguards, including as regards data subjects' rights; or

1122 (v) an approved certification mechanism pursuant to section 36 together with binding and
1123 enforceable commitments of the controller or processor in the foreign destination to apply the
1124 appropriate safeguards, including as regards data subjects' rights.

1125 (c) Subject to the authorization from the attorney general, the appropriate safeguards may
1126 also be provided for, in particular, by:

1127 (i) contractual clauses between the controller or processor and the controller, processor or
1128 the recipient of the personal data in the foreign destination; or

1129 (ii) provisions to be inserted into administrative arrangements between public authorities
1130 or bodies that include enforceable and effective data subject rights.

1131 Section 41. (a) The attorney general shall approve binding corporate rules, provided that
1132 the rules: (i) are legally binding and apply to and are enforced by every member concerned of the
1133 group of undertakings, or group of enterprises engaged in a joint economic activity, including
1134 employees; (ii) expressly confer enforceable rights on data subjects with regard to the processing
1135 of the data subjects' personal data; and (iii) fulfill the requirements of subsection (b).

1136 (b) The binding corporate rules described in subsection (a) shall specify:

1137 (i) the structure and contact details of the group of undertakings, or group of enterprises
1138 engaged in a joint economic activity and of each of the group's members;

1139 (ii) the data transfers or set of transfers, including the categories of personal data, the type
1140 of processing and purposes of the processing, the type of data subjects affected and the
1141 identification of the foreign destination in question;

1142 (iii) the legally binding nature of the rules, both internally and externally;

1143 (iv) the application of the general data protection principles, in particular purpose
1144 limitation, data minimization, limited storage periods, data quality, data protection by design and
1145 by default, legal basis for processing, processing of special categories of personal data, measures
1146 to ensure data security, and the requirements in respect of onward transfers to bodies not bound
1147 by the binding corporate rules;

1148 (v) the rights of data subjects in regard to processing and the means to exercise those
1149 rights, including the right not to be subject to decisions based solely on automated processing,
1150 including profiling in accordance with section 17, the right to lodge a complaint with the attorney
1151 general in accordance with section 53, and to obtain redress and, where appropriate,
1152 compensation for a breach of the binding corporate rules;

1153 (vi) how the information on the binding corporate rules, in particular on clauses (iv) and
1154 (v), is provided to the data subjects in addition to the information required in sections 8 and 9;

1155 (vii) the tasks of any data protection officer designated in accordance with section 31 or
1156 any other person or entity in charge of the monitoring compliance with the binding corporate
1157 rules within the group of undertakings, or group of enterprises engaged in a joint economic
1158 activity, as well as monitoring training and complaint-handling;

1159 (viii) the complaint procedures;

1160 (ix) the mechanisms within the group of undertakings, or group of enterprises engaged in
1161 a joint economic activity for ensuring the verification of compliance with the binding corporate
1162 rules; provided, that the mechanisms shall include data protection audits and methods for
1163 ensuring corrective actions to protect the rights of the data subject; and, provided further, that
1164 results of the verification shall be communicated to the person or entity referred to in clause (vii)
1165 and to the board of the controlling undertaking of a group of undertakings, or of the group of
1166 enterprises engaged in a joint economic activity, and should be available upon request to the
1167 attorney general;

1168 (x) the mechanisms for reporting and recording changes to the rules and reporting those
1169 changes to the attorney general;

1170 (xi) the cooperation mechanism with the attorney general to ensure compliance by any
1171 member of the group of undertakings, or group of enterprises engaged in a joint economic
1172 activity, in particular by making available to the attorney general the results of verifications of
1173 the measures referred to in clause (ix);

1174 (xii) the mechanisms for reporting to the attorney general any legal requirements to
1175 which a member of the group of undertakings, or group of enterprises engaged in a joint
1176 economic activity is subject in a foreign destination that are likely to have a substantial adverse
1177 effect on the guarantees provided by the binding corporate rules; and

1178 (xiii) the appropriate data protection training to personnel having permanent or regular
1179 access to personal data.

1180 (c) The attorney general may specify by regulation the format and procedures for the
1181 exchange of information between controllers, processors and the attorney general for binding
1182 corporate rules within the meaning of this section.

1183

1184 Section 42. Any judgment of a court or tribunal and any decision of an administrative
1185 authority of a foreign destination requiring a controller or processor to transfer or disclose
1186 personal data may only be recognized or enforceable in any manner if based on an international
1187 agreement, such as a mutual legal assistance treaty, in force between the requesting foreign
1188 destination and the United States or the commonwealth, without prejudice to other grounds for
1189 transfer pursuant to this chapter.

1190 Section 43. (a) In the absence of an adequacy decision pursuant to subsection (c) of
1191 section 39, or of appropriate safeguards pursuant to section 40, including binding corporate rules,
1192 a transfer or a set of transfers of personal data to a foreign destination shall take place only if:

1193 (i) the data subject explicitly consented to the proposed transfer, after having been
1194 informed of the possible risks of the transfers for the data subject due to the absence of an
1195 adequacy decision and appropriate safeguards;

1196 (ii) the transfer is necessary for the performance of a contract between the data subject
1197 and the controller or the implementation of pre-contractual measures taken at the data subject's
1198 request;

1199 (iii) the transfer is necessary for the conclusion or performance of a contract concluded in
1200 the interest of the data subject between the controller and another natural or legal person;

1201 (iv) the transfer is necessary for important reasons of public interest;

1202 (v) the transfer is necessary for the establishment, exercise or defense of legal claims;

1203 (vi) the transfer is necessary in order to protect the vital interests of the data subject or of
1204 other persons, where the data subject is physically or legally incapable of giving consent; or

1205 (vii) the transfer is made from a register which, according to state or federal law, is
1206 intended to provide information to the public and which is open to consultation either by the
1207 public in general or by any person who can demonstrate a legitimate interest, but only to the
1208 extent that the conditions laid down by state or federal law for consultation are fulfilled in the
1209 particular case.

1210 (b) Where a transfer could not be based on a provision of section 39 or 40, including the
1211 provisions on binding corporate rules, and none of the derogations for a specific situation
1212 referred to in subsection (a) apply, a transfer to a foreign destination may take place only if the
1213 transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the
1214 purposes of compelling legitimate interests pursued by the controller which are not overridden
1215 by the interests or rights and freedoms of the data subject, and the controller has assessed all the
1216 circumstances surrounding the data transfer and has on the basis of that assessment provided
1217 suitable safeguards with regard to the protection of personal data. The controller shall inform the
1218 attorney general of the transfer. The controller shall, in addition to providing the information
1219 referred to in sections 8 and 9, inform the data subject of the transfer and of the compelling
1220 legitimate interests pursued.

1221 (c) A transfer pursuant to subsection (b) shall not involve the entirety of the personal data
1222 or entire categories of the personal data contained in the register. Where the register is intended

1223 for consultation by persons having a legitimate interest, the transfer shall be made only at the
1224 request of those persons or if those persons are to be the recipients.

1225 (d) Clauses (i) to (iii), inclusive, of subsection (a) and subsection (b) shall not apply to
1226 activities carried out by public authorities in the exercise of their public powers.

1227 (e) The public interest referred to in clause (iv) of subsection (a) shall be recognized in
1228 federal law or in the law of the state to which the controller is subject.

1229 (f) In the absence of an adequacy decision, general or special law may, for important
1230 reasons of public interest, expressly set limits to the transfer of specific categories of personal
1231 data to a foreign destination.

1232 (g) The controller or processor shall document the assessment as well as the suitable
1233 safeguards referred to in subsection (b) in the records referred to in section 24.

1234 Section 44. In relation to foreign destinations, the attorney general shall take appropriate
1235 steps to:

1236 (i) develop cooperation mechanisms to facilitate the effective enforcement of legislation
1237 for the protection of personal data;

1238 (ii) provide mutual assistance in the enforcement of legislation for the protection of
1239 personal data, including through notification, complaint referral, investigative assistance and
1240 information exchange, subject to appropriate safeguards for the protection of personal data and
1241 other fundamental rights and freedoms;

1242 (iii) engage relevant stakeholders in discussion and activities aimed at furthering
1243 cooperation in the enforcement of legislation for the protection of personal data; and

1244 (iv) promote the exchange and documentation of personal data protection legislation and
1245 practice, including on jurisdictional conflicts with other foreign destinations.

1246 Section 45. (a) The attorney shall be responsible for monitoring the application of this
1247 chapter, in order to protect the fundamental rights and freedoms of natural persons in relation to
1248 processing and to facilitate the free flow of personal data within the commonwealth.

1249 (b) The attorney general shall:

1250 (i) monitor and enforce the application of this chapter;

1251 (ii) promote public awareness and understanding of the risks, rules, safeguards and rights
1252 in relation to processing, including, but not limited to, activities addressed specifically to
1253 children that shall receive specific attention;

1254 (iii) advise, in accordance with general and special law, the general court, municipalities,
1255 state agencies and other institutions and bodies on legislative and administrative measures
1256 relating to the protection of natural persons' rights and freedoms with regard to processing;

1257 (iv) promote the awareness of controllers and processors of their obligations pursuant to
1258 this chapter;

1259 (v) upon request, provide information to any data subject concerning the exercise of their
1260 rights pursuant to this chapter and, if appropriate, cooperate with the supervisory authorities in
1261 foreign destinations to that end;

1262 (vi) handle complaints lodged by a data subject, or by a body, organization or association
1263 in accordance with section 54, and investigate, to the extent appropriate, the subject matter of the
1264 complaint and inform the complainant of the progress and the outcome of the investigation

1265 within a reasonable period, in particular if further investigation or coordination with a
1266 supervisory authority in a foreign destination is necessary;

1267 (vii) cooperate with, including sharing information and providing mutual assistance to,
1268 supervisory authorities in foreign destinations;

1269 (viii) conduct investigations on the application of this chapter, including on the basis of
1270 information received from a supervisory authority in a foreign destination or other public
1271 authority;

1272 (ix) monitor relevant developments, insofar as they have an impact on the protection of
1273 personal data, in particular the development of information and communication technologies and
1274 commercial practices;

1275 (x) adopt standard contractual clauses referred to in subsection (g) of section 22 and
1276 clause (iii) of subsection (b) of section 40;

1277 (xi) establish and maintain a list in relation to the requirement for data protection impact
1278 assessment pursuant to subsection (d) of section 29;

1279 (xii) give advice on the processing operations referred to in subsection (b) of section 30;

1280 (xiii) encourage the drawing up of codes of conduct pursuant to subsection (a) of section
1281 34 and provide an opinion and approve such codes of conduct which provide sufficient
1282 safeguards, pursuant to subsection (e) of said section 34;

1283 (xiv) encourage the establishment of data protection certification mechanisms and of data
1284 protection seals and marks pursuant to subsection (a) of section 36, and approve the criteria of
1285 certification pursuant to subsection (e) of said section 36;

1286 (xv) where applicable, carry out a periodic review of certifications issued in accordance
1287 with subsection (g) of section 36;

1288 (xvi) draft and publish the requirements for accreditation of a body for monitoring codes
1289 of conduct pursuant to section 35 and of a certification body pursuant to section 37;

1290 (xvii) conduct the accreditation of a body for monitoring codes of conduct pursuant to
1291 section 35 and of a certification body pursuant to section 37;

1292 (xviii) authorize contractual clauses and provisions referred to in subsection (c) of section
1293 40;

1294 (xix) approve binding corporate rules pursuant to section 41;

1295 (xx) keep internal records of infringements of this chapter and of measures taken in
1296 accordance with clause (ii) of subsection (a) of section 46; and

1297 (xxi) fulfill any other tasks related to the protection of personal data.

1298 (c) The attorney general shall facilitate the submission of complaints referred to in clause
1299 (vi) of subsection (b) by measures such as a complaint submission form which can also be
1300 completed electronically, without excluding other means of communication.

1301 (d) The performance of the tasks described in subsection (b) shall be free of charge for
1302 the data subject and, where applicable, for the data protection officer; provided, however, that
1303 where requests are manifestly unfounded or excessive, in particular because of their repetitive
1304 character, the attorney general may charge a reasonable fee based on administrative costs, or
1305 refuse to act on the request; and, provided further, that the attorney general shall bear the burden
1306 of demonstrating the manifestly unfounded or excessive character of the request.

1307 Section 46. (a) The attorney general shall have the power to:

1308 (i) order the controller and the processor, and, where applicable, the controller's or the
1309 processor's representative to provide any information the attorney general requires for the
1310 performance of the attorney general's duties pursuant to this chapter;

1311 (ii) carry out investigations in the form of data protection audits;

1312 (iii) carry out a review on certifications issued pursuant to subsection (g) of section 36;

1313 (iv) notify the controller or the processor of an alleged infringement of this chapter;

1314 (v) obtain, from the controller and the processor, access to all personal data and to all
1315 information necessary for the performance of the attorney general's duties pursuant to this
1316 chapter;

1317 (vi) obtain access to any premises of the controller and the processor, including to any
1318 data processing equipment and means, in accordance with state or federal procedural law;

1319 (vii) issue warnings to a controller or processor that intended processing operations are
1320 likely to infringe on this chapter;

1321 (viii) issue reprimands to a controller or a processor where processing operations have
1322 infringed on this chapter;

1323 (ix) order the controller or the processor to comply with the data subject's requests to
1324 exercise the data subject's rights pursuant to this chapter;

1325 (x) order the controller or processor to bring processing operations into compliance with
1326 this chapter, where appropriate, in a specified manner and within a specified period;

- 1327 (xi) order the controller to communicate a personal data breach to the data subject;
- 1328 (xii) impose a temporary or definitive limitation, including a ban on processing;
- 1329 (xiii) order the rectification or erasure of personal data or restriction of processing
1330 pursuant to sections 11 to 13, inclusive, and the notification to recipients to whom the personal
1331 data has been disclosed pursuant to subsection (b) of section 12 and section 14;
- 1332 (xiv) withdraw a certification or order the certification body to withdraw a certification
1333 issued pursuant to sections 36 or 37, or order the certification body not to issue certification if the
1334 requirements for the certification are not or are no longer met;
- 1335 (xv) impose an administrative fine pursuant to section 56, in addition to, or instead of
1336 measures referred to in this subsection, depending on the circumstances of each individual case;
- 1337 (xvi) order the suspension of data flows to a recipient in a foreign destination;
- 1338 (xvii) advise the controller in accordance with the prior consultation procedure referred to
1339 section 30;
- 1340 (xviii) issue, on the attorney general's initiative or on request, opinions to the general
1341 court, the governor or, in accordance with general and special law, to other institutions and
1342 bodies as well as to the public on any issue related to the protection of personal data;
- 1343 (xix) authorize processing referred to in subsection (c) of section 30;
- 1344 (xx) issue an opinion and approve draft codes of conduct pursuant to subsection (e) of
1345 section 34;
- 1346 (xxi) accredit certification bodies pursuant to section 37;

1347 (xxii) issue certifications and approve criteria of certification in accordance with
1348 subsection (e) of section 36;

1349 (xxiii) adopt standard data protection clauses referred to in subsection (g) of section 22
1350 and clause (iii) of subsection (b) of section 40;

1351 (xxiv) authorize contractual clauses referred to in clause (i) of subsection (c) of section
1352 40;

1353 (xxv) authorize administrative arrangements referred to in clause (ii) of subsection (c) of
1354 section 40; and

1355 (xxvi) approve binding corporate rules pursuant to section 41.

1356 (b) The exercise of the powers conferred on the attorney general pursuant to this section
1357 shall be subject to appropriate safeguards, including effective judicial remedy and due process,
1358 set out in general and special law.

1359 (c) The attorney general shall have the power to commence or engage otherwise in legal
1360 proceedings in order to enforce the provisions of this chapter.

1361 (d) Annually, the attorney general shall compile a report on activities taken pursuant to
1362 this chapter, which may include a list of types of infringement notified and types of measures
1363 taken in accordance with subsection (a). The reports shall be transmitted to the clerks of the
1364 house of representatives and the senate and the joint committee on advanced information
1365 technology, the internet and cybersecurity. The attorney general shall make the reports available
1366 to the public on the attorney general's website.

1367 Section 47. (a) Upon adopting a decision regarding a complaint pursuant to this chapter,
1368 the attorney general shall transmit the decision to the main establishment or single establishment
1369 of the controller or processor, including a summary of the relevant facts and grounds.

1370 (b) Where a complaint is dismissed or rejected, the attorney general shall notify the
1371 complainant and the controller.

1372 (c) Where the attorney general dismisses or rejects parts of a complaint and acts on other
1373 parts of that complaint, a separate decision shall be adopted for each part of the complaint.

1374 (d) After being notified of the decision, the controller or processor shall take the
1375 necessary measures to ensure compliance with the decision as regards processing activities in the
1376 context of all its establishments in the commonwealth. The controller or processor shall notify
1377 the measures taken for complying with the decision to the attorney general.

1378 (e) Where, in exceptional circumstances, the attorney general has reasons to consider that
1379 there is an urgent need to act in order to protect the interests of data subjects, the urgency
1380 procedure referred to in section 48 shall apply.

1381 Section 48. (a) In exceptional circumstances, where the attorney general considers that
1382 there is an urgent need to act in order to protect the rights and freedoms of data subjects, the
1383 attorney general may immediately adopt provisional measures intended to produce legal effects
1384 in the commonwealth with a specified period of validity which shall not exceed 3 months.

1385 (b) Where the attorney general has taken a measure pursuant to subsection (a) and
1386 considers that final measures need urgently be adopted, the attorney general may request an

1387 urgent opinion or an urgent binding decision from the superior court, giving reasons for
1388 requesting such opinion or decision.

1389 (c) The attorney general may request an urgent opinion or an urgent binding decision, as
1390 the case may be, from the superior court where there is an urgent need to act, in order to protect
1391 the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision,
1392 including for the urgent need to act.(d) The superior court shall provide n urgent opinion or an
1393 urgent binding decision referred to in subsections (b) and (c) within 2 weeks of the request by the
1394 attorney general.

1395 Section 49. (a) The attorney general shall, on the attorney general’s own initiative or,
1396 where relevant, at the request of the general court:

1397 (i) advise the general court on any issue related to the protection of personal data in the
1398 commonwealth, including on any proposed amendment of this chapter;

1399 (ii) advise the general court on the format and procedures for the exchange of information
1400 between controllers, processors and supervisory authorities for binding corporate rules;

1401 (iii) issue guidelines, recommendations and best practices on procedures for erasing links,
1402 copies or replications of personal data from publicly available communication services as
1403 referred to in subsection (b) of section 22;

1404 (iv) examine, on the attorney general’s own initiative, on request of the general court, any
1405 question covering the application of this chapter and issue guidelines, recommendations and best
1406 practices in order to encourage consistent application of this chapter;

1407 (v) draw up guidelines concerning the application of measures referred to in section 46
1408 and the setting of administrative fines pursuant to section 55;

1409 (vi) encourage the drawing-up of codes of conduct and the establishment of data
1410 protection certification mechanisms and data protection seals and marks pursuant to sections 34
1411 and 36;

1412 (vii) approve the criteria of certification pursuant to subsection (e) of section 36 and
1413 maintain a public register of certification mechanisms and data protection seals and marks
1414 pursuant to subsection (h) of said section 36 and of the certified controllers or processors
1415 established in foreign destinations pursuant to subsection (g) of said section 36.;

1416 (viii) approve the requirements referred to in subsection (c) of section 37 with a view to
1417 the accreditation of certification bodies referred to in said section 37;

1418 (ix) promote the exchange of knowledge and documentation on data protection
1419 legislation and practice with data protection supervisory authorities worldwide; and

1420 (x) maintain a publicly accessible electronic register of decisions taken by supervisory
1421 authorities and courts on issues handled in the consistency mechanism.

1422 (b) The guidelines, recommendations and best practices described in clause (iv) of
1423 subsection (a) shall include, but not be limited to, guidelines, recommendations and best
1424 practices:

1425 (i) for further specifying the criteria and conditions for decisions based on profiling
1426 pursuant to subsection (b) of section 17;

1427 (ii) for establishing the personal data breaches and determining the undue delay referred
1428 to in subsections (a) and (b) of section 27 and for the particular circumstances in which a
1429 controller or a processor is required to notify the personal data breach;

1430 (iii) as to the circumstances in which a personal data breach is likely to result in a high
1431 risk to the rights and freedoms of the natural persons referred to in subsection (a) of section 28;

1432 (iv) for the purpose of further specifying the criteria and requirements for personal data
1433 transfers based on binding corporate rules adhered to by controllers and binding corporate rules
1434 adhered to by processors and on further necessary requirements to ensure the protection of
1435 personal data of the data subjects concerned referred to in section 41; and

1436 (v) for the purpose of further specifying the criteria and requirements for the personal
1437 data transfers on the basis of subsection (a) of section 43.

1438 (c) The attorney general shall, on the attorney general's own initiative or, where relevant,
1439 at the request of the general court, review the practical application of the guidelines,
1440 recommendations and best practices.

1441 (d) Where the general court requests advice from the attorney general, the general court
1442 may indicate a time limit, taking into account the urgency of the matter.

1443 (e) The attorney general shall forward the attorney general's opinions, guidelines,
1444 recommendations, and best practices to the general court and make the opinions, guidelines,
1445 recommendations and best practices public on the attorney general's website.

1446 (f) The attorney general shall, where appropriate, consult interested parties and give
1447 interested parties the opportunity to comment within a reasonable period. The attorney general
1448 shall publish the results of the consultation procedure publicly on the attorney general's website.

1449 Section 50. In addition to the report on activities described in subsection (d) of section
1450 46, the attorney general shall annually compile a report regarding the protection of natural
1451 persons with regard to processing in the commonwealth and, where relevant, foreign
1452 destinations. The reports shall include a review of the practical application of the guidelines,
1453 recommendations and best practices referred to in subsection (b) of section 49. The reports shall
1454 be transmitted to the clerks of the house of representatives and the senate and the joint committee
1455 on advanced information technology, the internet and cybersecurity. The attorney general shall
1456 make the reports available to the public on the attorney general's website.

1457 Section 51. Without prejudice to any other administrative or judicial remedy, every data
1458 subject shall have the right to lodge a complaint with the attorney general, in particular if the data
1459 subject lives or works in the commonwealth or the alleged infringement took place in the
1460 commonwealth, if the data subject considers that the processing of personal data relating to the
1461 data subject infringes this chapter. The attorney general shall inform the complainant on the
1462 progress and the outcome of the complaint including the possibility of a judicial remedy pursuant
1463 to section 52.

1464 Section 52. Without prejudice to any other administrative or non-judicial remedy:

1465 (i) each natural or legal person shall have the right to an effective judicial remedy against
1466 a legally binding decision of the attorney general concerning the natural or legal person; and

1467 (ii) each data subject shall have the right to a an effective judicial remedy where the
1468 attorney general does not handle a complaint or does not inform the data subject within 3 months
1469 on the progress or outcome of the complaint lodged pursuant to section 51.

1470 Proceedings against the attorney general shall be brought before the superior court.
1471 Where proceedings are brought against an opinion or decision of the attorney general, the
1472 attorney general shall forward that opinion or decision to the court.

1473 Section 53. Without prejudice to any available administrative or non-judicial remedy,
1474 including the right to lodge a complaint with the attorney general pursuant to section 51, each
1475 data subject shall have the right to an effective judicial remedy where the data subject considers
1476 that the data subject's rights under this chapter have been infringed as a result of the processing
1477 of the data subject's personal data in non-compliance with this chapter. Proceedings against a
1478 controller or a processor shall be brought before the superior court.

1479 Section 54. (a) A data subject shall have the right to mandate a not-for-profit body,
1480 organization or association to lodge a complaint on behalf of the data subject, to exercise the
1481 rights referred to in sections 51 to 53, inclusive, on behalf of the data subject and to exercise the
1482 right to receive compensation referred to in section 55 on behalf of the data subject; provided,
1483 that the body, organization or association: (i) has been properly constituted in accordance with
1484 state or federal law; (ii) has statutory objectives in the public interest; and (iii) is active in the
1485 field of the protection of data subjects' rights and freedoms with regard to the protection of their
1486 personal data.

1487 (b) Any body, organization or association referred to in subsection (a), independently of a
1488 data subject's mandate, has the right to lodge a complaint with the attorney general pursuant to

1489 section 51 and to exercise the rights referred to in sections 52 and 53 if the body, organization or
1490 association considers that the rights of a data subject pursuant this chapter have been infringed as
1491 a result of the processing.

1492 Section 55. (a) Any person who has suffered material or non-material damage as a result
1493 of an infringement of this chapter shall have the right to receive compensation from the
1494 controller or processor for the damage suffered.

1495 (b) Any controller involved in processing shall be liable for the damage caused by
1496 processing which infringes this chapter. A processor shall be liable for the damage caused by
1497 processing only where it has not complied with obligations of this chapter specifically directed to
1498 processors or where it has acted outside or contrary to lawful instructions of the controller.

1499 (c) A controller or processor shall be exempt from liability as specified in subsection (b)
1500 if the controller or processor proves that the controller or processor is not in any way responsible
1501 for the event giving rise to the damage.

1502 (d) Where more than 1 controller or processor, or both a controller and a processor, are
1503 involved in the same processing and where the controller and processor are responsible for any
1504 damage caused by processing, each controller or processor shall be held liable for the entire
1505 damage in order to ensure effective compensation of the data subject. Where a controller or
1506 processor has paid full compensation for the damage suffered, that controller or processor shall
1507 be entitled to claim back from the other controllers or processors involved in the same processing
1508 that part of the compensation corresponding to their part of responsibility for the damage, in
1509 accordance with the conditions set out in subsection (b).

1510 (e) Court proceedings for exercising the right to receive compensation shall be brought
1511 before the superior court.

1512 Section 56. (a) The attorney general shall ensure that the imposition of administrative
1513 fines pursuant to this section in respect of infringements of this chapter referred to in subsections
1514 (d) to (f), inclusive, shall in each individual case be effective, proportionate and dissuasive.

1515 (b) Administrative fines shall, depending on the circumstances of each individual case, be
1516 imposed in addition to, or instead of, measures referred to in subsections (vii) to (xiv), inclusive
1517 and (xvi) of section 46. When deciding whether to impose an administrative fine and deciding on
1518 the amount of the administrative fine in each individual case due regard shall be given to:

1519 (i) the nature, gravity and duration of the infringement taking into account the nature
1520 scope or purpose of the processing concerned as well as the number of data subjects affected and
1521 the level of damage suffered by the data subjects;

1522 (ii) the intentional or negligent character of the infringement;

1523 (iii) any action taken by the controller or processor to mitigate the damage suffered by
1524 data subjects;

1525 (iv) the degree of responsibility of the controller or processor taking into account
1526 technical and organizational measures implemented by them pursuant to sections 19 and 26;

1527 (v) any relevant previous infringements by the controller or processor;

1528 (vi) the degree of cooperation with the attorney general, in order to remedy the
1529 infringement and mitigate the possible adverse effects of the infringement;

- 1530 (vii) the categories of personal data affected by the infringement;
- 1531 (viii) the manner in which the infringement became known to the attorney general, in
1532 particular whether, and if so to what extent, the controller or processor notified the infringement;
- 1533 (ix) where measures referred to in clauses (vii) to (xvi) of subsection (a) of section 46
1534 have previously been ordered against the controller or processor concerned with regard to the
1535 same subject-matter, compliance with those measures;
- 1536 (x) adherence to approved codes of conduct pursuant to section 34 or approved
1537 certification mechanisms pursuant to section 36; and
- 1538 (xi) any other aggravating or mitigating factor applicable to the circumstances of the case,
1539 such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.
- 1540 (c) If a controller or processor intentionally or negligently, for the same or linked
1541 processing operations, infringes several provisions of this chapter, the total amount of the
1542 administrative fine shall not exceed the amount specified for the gravest infringement.
- 1543 (d) Infringements of the following provisions shall, in accordance with subsection (b), be
1544 subject to administrative fines up to \$10,000,000, or in the case of an undertaking, up to 2 per
1545 cent of the total worldwide annual turnover of the preceding financial year, whichever is higher:
- 1546 (i) the obligations of the controller and the processor pursuant to subsection (e) of section
1547 5, subsection (e) of section 6, sections 19 to 33, inclusive, and sections 36 and 37;
- 1548 (ii) the obligations of the certification body pursuant to sections 36 and 37; or
- 1549 (iii) the obligations of the monitoring body pursuant to subsection(c) of section 35.

1550 (e) Infringements of the following provisions shall, in accordance with subsection (b), be
1551 subject to administrative fines up to \$20,000,000, or in the case of an undertaking, up to 4 per
1552 cent of the total worldwide annual turnover of the preceding financial year, whichever is higher:

1553 (i) the basic principles for processing, including conditions for consent, pursuant to
1554 sections 3 and 4, subsections (a) to (d), inclusive, of section 5, and subsections (a) to (c),
1555 inclusive, of section 6;

1556 (ii) the data subjects' rights pursuant to sections 7 to 17, inclusive;

1557 (iii) the transfers of personal data to a recipient in a foreign destination pursuant to
1558 sections 38 to 43, inclusive;

1559 (iv) any obligations pursuant to general or special law adopted pursuant to sections 58 to
1560 64, inclusive;

1561 (v) non-compliance with an order or a temporary or definitive limitation on processing or
1562 the suspension of data flows by the attorney general pursuant to clauses (vii) to (xvi), inclusive,
1563 of subsection (a) of section 46 or failure to provide access in violation of clauses (i) to (vi),
1564 inclusive, of said subsection (a) of said section 46.

1565 (f) Non-compliance with an order by the attorney general as referred to in clauses (vii) to
1566 (xvi), inclusive, of subsection (a) of section 46 shall, in accordance with subsection (b), be
1567 subject to administrative fines up to \$20,000,000 , or in the case of an undertaking, up to 4 per
1568 cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

1569 (g) Without prejudice to the corrective powers of the attorney general as referred to in
1570 clauses (vii) to (xvi), inclusive, of subsection (a) of section 46, the general court may enact

1571 general and special laws providing rules on whether and to what extent administrative fines may
1572 be imposed on public authorities and bodies.

1573 (h) The exercise by the attorney general of powers pursuant to this section shall be
1574 subject to appropriate procedural safeguards in accordance with state and federal law, including
1575 effective judicial remedy and due process.

1576 Section 57. The general court may enact general and special laws providing rules on
1577 other penalties applicable to infringements of this chapter, in particular for infringements that are
1578 not subject to administrative fines pursuant to section 56, and shall take all measures necessary to
1579 ensure that they are implemented. The penalties shall be effective, proportionate and dissuasive.

1580 Section 58. (a) The general court shall enact general or special laws to reconcile the right
1581 to the protection of personal data pursuant to this chapter with the right to freedom of expression
1582 and information, including processing for journalistic purposes and the purposes of academic,
1583 artistic or literary expression.

1584 (b) For processing carried out for journalistic purposes or the purpose of academic artistic
1585 or literary expression, the general court shall enact general or special laws that provide for
1586 exemptions or derogations from sections 4 to 50, inclusive, and sections 59 to 64 if exemptions
1587 or derogations are necessary to reconcile the right to the protection of personal data with the
1588 freedom of expression and information.

1589 Section 59. Personal data in official documents held by a public authority or a public
1590 body or a private body for the performance of a task carried out in the public interest may be
1591 disclosed by the authority or body in accordance with general, special or federal law in order to

1592 reconcile public access to official documents with the right to the protection of personal data
1593 pursuant to this chapter.

1594

1595 Section 60. The attorney general may further determine the specific conditions for the
1596 processing of a social security number, driver's license number or any other identifier of general
1597 application. In that case, the social security number, driver's license number or other identifier of
1598 general application shall be used only under appropriate safeguards for the rights and freedoms
1599 of the data subject pursuant to this chapter.

1600 Section 61. The general court may, by law or by collective agreements, provide for more
1601 specific rules to ensure the protection of the rights and freedoms in respect of the processing of
1602 employees' personal data in the employment context, in particular for the purposes of:
1603 (i) recruitment; (ii) the performance of the contract of employment, including discharge of
1604 obligations laid down by law or by collective agreements, management, planning and
1605 organization of work; (iii) equality and diversity in the workplace; (iv) health and safety at work;
1606 (v) protection of employer's or customer's property; (vi) the exercise and enjoyment, on an
1607 individual or collective basis, of rights and benefits related to employment; and (vii) the
1608 termination of the employment relationship. The rules shall include suitable and specific
1609 measures to safeguard the data subject's human dignity, legitimate interests and fundamental
1610 rights, with particular regard to the transparency of processing, the transfer of personal data
1611 within a group of undertakings, or a group of enterprises engaged in a joint economic activity
1612 and monitoring systems at the work place.

1613 Section 62. (a) Processing for archiving purposes in the public interest, scientific or
1614 historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in
1615 accordance with this chapter, for the rights and freedoms of the data subject. The safeguards
1616 shall ensure that technical and organizational measures are in place in particular in order to
1617 ensure respect for the principle of data minimization. The measures may include
1618 pseudonymization; provided, that the public interest, scientific or historical research purposes or
1619 statistical purposes can be fulfilled in with pseudonymization. Where said purposes can be
1620 fulfilled by further processing that does not permit or no longer permits the identification of data
1621 subjects, the purposes shall be fulfilled in that manner.

1622 (b) Where personal data is processed for scientific or historical research purposes or
1623 statistical purposes, general or special law may provide for derogations from the rights referred
1624 to in sections 10, 11, 13 and 16 subject to the conditions and safeguards referred to in subsection
1625 (a), in so far as the rights are likely to render impossible or seriously impair the achievement of
1626 the specific purposes and the derogations are necessary for the fulfilment of those purposes.

1627 (c) Where personal data is processed for archiving purposes in the public interest, general
1628 or special law may provide for derogations from the rights referred to in sections 10, 11, 13, 14,
1629 15 and 16, subject to the conditions and safeguards referred to in subsection (a), in so far as the
1630 rights are likely to render impossible or seriously impair the achievement of the specific purposes
1631 and the derogations are necessary for the fulfilment of those purposes.

1632 (d) Where processing referred to in subsections (b) and (c) serves at the same time
1633 another purpose, the derogations shall apply only to processing for the purposes referred to in
1634 said subsections (b) and (c).

1635 Section 63. The general court may enact general or special laws establishing specific
1636 rules to set out the powers of the attorney general described in clauses (v) and (vi) of subsection
1637 (a) of section 46 in relation to controllers or processors that are subject, pursuant to state or
1638 federal law or rules established by national competent bodies, to an obligation of professional
1639 secrecy or other equivalent obligations of secrecy; provided, that the rules are necessary and
1640 proportionate to reconcile the right of the protection of personal data with the obligation of
1641 secrecy. The rules shall apply only with regard to personal data which the controller or processor
1642 has received as a result of or has obtained in an activity covered by that obligation of secrecy.

1643 Section 64. Churches and religious associations or communities that apply
1644 comprehensive rules relating to the protection of natural persons with regard to processing may
1645 continue to apply said rules; provided, that the rules are brought into line with this chapter; and,
1646 provided further, that the churches and religious associations or communities shall be subject to
1647 the supervision of the attorney general.

1648 Section 65. (a) Every 4 years, the attorney general shall submit a report on the evaluation
1649 and review of this chapter to the clerks of the house of representatives and the senate and the
1650 joint committee on advanced information technology, the internet and cybersecurity. The
1651 attorney general shall make the reports available to the public on the attorney general's website.
1652 In evaluating and reviewing this chapter, the attorney general shall examine, in particular, the
1653 application and functioning of sections 38 to 44 regarding the transfer of personal data to foreign
1654 destinations, with particular regard to decisions adopted pursuant to subsection (c) of section 39.
1655 The attorney general shall take into account the positions and findings of state agencies and other
1656 relevant bodies or sources. The attorney general shall, if necessary, submit drafts of legislation to

1657 amend this chapter, in particular taking into account of developments in information technology
1658 and in the light of the state of progress in the information society.

1659 (b) The attorney general shall, if appropriate, submit legislative proposals with a view to
1660 amending other general or special laws on the protection of personal data, in order to ensure
1661 uniform and consistent protection of natural persons with regard to processing; including, but not
1662 limited to, the rules relating to the protection of natural persons with regard to processing by
1663 state institutions, bodies, offices and agencies and the free movement of data.

1664 SECTION 2. Notwithstanding chapter 93M of the General Laws, agreements involving
1665 the transfer of personal data to foreign destinations which were in place prior to the effective date
1666 of this act, and which comply with state and federal law as applicable prior to the effective date
1667 of this act, shall remain in force until amended, replaced or revoked.