

3 **A message from the United Nations Special Rapporteur on the right to**
4 **privacy, Prof. Joseph A. Cannataci:**

5 **“This is the basic text that has been discussed during the joint public events**
6 **which were held in Rome on 18-19 January 2018 and Malta on 12-14 February**
7 **2018. Further consultation sessions may be announced in the future. This text**
8 **also includes some amendments that were suggested in submissions received**
9 **after these meetings.**

10 **This text attempts to reflect and put up for discussion the many views received**
11 **by the Special Rapporteur to date.**

12 **The Special Rapporteur does not necessarily agree with all parts of the text**
13 **which are included. He is presenting them in the spirit of open discussion. An**
14 **annotated version containing comments received in an anonymized form will**
15 **be made available separately in order to further facilitate further in-depth**
16 **discussion.”**

17

MAPPING WP4

Working Draft Legal Instrument on Government-led Surveillance and Privacy Including the Explanatory Memorandum

Ver 0.7

PREFACE

The issue of surveillance is an extremely sensitive one. Some experts have described the current situation in the area as one where most states have either resisted legalization or have been ambivalent about prioritizing rights where national security threats are politically resonant. There is significant concern that states are far from ready to move in a rights-positive direction on surveillance, and that a draft legal instrument – such as this one – could indeed be an opportunity for regressive negotiation.

The terms and concepts used in this text depend on effectively working state institutions, operating on the basis of the rule of law and ultimately drawing from a culture which is fully committed to respecting, protecting and promoting human rights. The Special Rapporteur on the right to privacy recognizes and understands concerns that if these preconditions are not met in a state, any new international agreement on the subject could effectively lower the protection of rights.

Nevertheless, the Special Rapporteur also identified the need for more guidance and standardization of the subject. Since the work on the mandate started, many representatives of governments, corporations, civil society actors and experts from other parts of the multi-stakeholder community shaping Digital Technologies have requested a document offering detailed guidance for the area of surveillance. While International Law provides a general framework for the protection of human rights including privacy, freedom of expression and the right to information, the rapid technological development and the transition to the digital age make it necessary to develop more. This complex and demanding challenge is difficult to address. The Special Rapporteur has made more remarks on this issue in his report to the UN Human Rights Council in March 2018.

It is the intention of the Special Rapporteur on the right to privacy to keep developing this text which has become a useful basis for informed discussion of the subject. Hopefully, this working draft provides the opportunity for decision-makers in public or private capacities to develop and create better policies which respect, protect and promote human rights and human dignity in the sense of the holistic approach used to develop this document. Surveillance needs to be limited to what is necessary and proportionate while states need to be able to guarantee a safe and secure environment.

The Special Rapporteur remains open for any suggestions on how this initiative might contribute to positively influence the field of surveillance. Such suggestions might relate to the further process as well as feedback on the substantive core of this text. **In no way should this initiative and any concepts herein be understood as a platform to allow states to legitimize or develop questionable and bad practices.** Such practices ultimately weaken human rights, the national and international legal order and result in a situation which threatens to lower human dignity and cause physical harm to persons all over the world.

While the issue of surveillance is sensitive and changes in the normative framework come with risks, this cannot lead to abandonment of the task. The topic reflects many aspects – such as jurisdiction in cyberspace, development of trust, effective safeguards and remedies – which require a solution for the further development of the international community and people all across the world in order to make the transition to the digital age a fruitful endeavor.

61 **I. Introduction**
62 **a. Background**

63 This draft text for a Legal Instrument (LI) on Government-led Surveillance and Privacy is the result of
64 meetings and exchanges between the MAPPING project¹ and several categories of stakeholders
65 shaping the development and use of digital technologies (DTs). These include leading global technology
66 companies, experts with experience of working within civil society, law enforcement, intelligence
67 services, academics and other members of the multi-stakeholder community shaping DTs and the
68 transition to the Digital Age.

69 The provisions have been developed using the results of multiple research projects (including
70 MAPPING, RESPECT and SMART).² Additionally, international and national best-practices have been
71 taken in account. These insights were combined with the experiences and expertise of all parties
72 involved in contributing to drafting the text which was facilitated by members of the Security,
73 Technology & e-Privacy Research Group (STeP) at the University of Groningen in the Netherlands.

74 The provisions of the LI are based on international human rights law. Ultimately, this draft should aid
75 states and the multi-stakeholder community to protect, respect and promote human dignity. The LI
76 aims at giving detailed guidance for government-led or organized surveillance using electronic means.
77 This is necessary for both human rights and the responsible and dignified conduct of state authority
78 and powers.

79 In the view of the drafters of this document human dignity should be protected, respected and
80 promoted with a holistic approach. In other words, Human Rights ought to be considered as one
81 functional entity. Together they attempt to raise the level of human dignity, which is the root and
82 ultimate cause for the existence of modern, international human rights law. Those rights include but
83 are not limited to the rights of people to develop their lives and personalities, the rights of victims of
84 crime and of persons to live in a safe and secure environment.

85 Privacy and other rights related to the development of personality shall only be limited when
86 necessary. If a measure is necessary, a proportionality assessment shall be carried out following a
87 three-step test: First, the measure which is taken must be potentially capable of realizing the aim.
88 Secondly, the measure which is taken is required to reach the aim (in other words it must be the least-
89 intrusive measure). Thirdly, the measure which is taken must be proportionate “strictu sensu”. This
90 means that it is not only a capable measure which is the least intrusive one (steps 1 and 2), but also
91 legitimate considering its impact on the overall situation and particularly other human rights
92 potentially infringed during the process.³ Only if all these three criteria are met, a necessary measure
93 is proportionate and can therefore be taken.

94 During the first meetings it transpired that there was a desire for a new legal instrument covering
95 several problematic issues in the area of government-led or organized surveillance that could form the
96 basis of a new global consensus between states. The LI was drafted as a blueprint for any form of soft
97 law or hard law, anything ranging from a non-binding recommendation to a (global or regional)

¹ The MAPPING acronym stands for “Managing Alternatives for Privacy, Property and Internet Governance”. This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345. More information can be found via <https://mappingtheinternet.eu/> - accessed on 22.09.2016.

² The RESPECT acronym stands for “Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies”. This project has received funding from the European Union’s Seventh Framework Programme. More information can be found via http://www.rug.nl/rechten/organization/vakgroepen/eer/step-research-group/respect_description - accessed on 22.09.2014; The SMART acronym stands for “Scalable Measures for Automated Recognition Technologies”, <http://smartsurveillance.eu/> accessed on 13.06.2017.

³ This last step could also be described as a “cost-benefit” analysis.

98 international treaty, that would allow states to join the consensus and form a new group which puts
99 emphasis on the promotion and protection of human rights in the Digital Age.

100 While the infringement of privacy and other rights relating to the development of personality (e.g.
101 freedom of expression) are not new concerns, the violation of these rights in the context of growing
102 use of DTs is new, global, complex and constantly evolving. For this reason, States shall provide for
103 shared learning, public policy engagement and other multi-stakeholder collaboration to advance the
104 promotion and protection of these principles and the enjoyment of these rights.

105 However, such measures and general guidance are not sufficient. It is the position of the drafters of
106 this legal instrument that the protection of human rights by states in the Digital Age must also be
107 outlined in a more detailed and comprehensive way. One of the means for such protection of human
108 rights is through a comprehensive and innovative LI on governmental surveillance, which would assist
109 in establishing safeguards without borders and effective legal remedies across borders.⁴

110 This instrument is intended to apply to all Law Enforcement Agencies (LEA) and Security & Intelligence
111 Services (SIS) and public-mandated entities acting on their behalf. While LEA and SIS are organized
112 differently from state to state and the tasks and operational requirements as well as their capabilities
113 differ, the impact of their activities on human dignity and fundamental rights are often similar in
114 nature. Nevertheless, LEAs and SIS have separate functions.

115 Despite this clarification, DTs used to carry out surveillance become increasingly similar. Sometimes
116 they are provided by third-party vendors and used by multiple agencies of a state which will be either
117 part of the LEA or the SIS community. The drafters of the LI aimed at developing provisions that fully
118 respect, protect and promote not only privacy and personality rights, but also public safety, the right
119 to a fair trial and the rights of victims. The impact of surveillance activities on the dignity of humans,
120 regardless of their race, colour, gender, language, religion, political or other opinion, national or social
121 origin, citizenship, property, birth or other status (including age) is at the core of the LI.

122 To ensure its flexibility when integrated in a specific institutional framework the draft LI is focusing
123 mainly on substantive provisions. Hence, essential procedural provisions relating to a broader legal
124 framework of potentially supranational/national/multilateral nature need to be added if the LI is to
125 become more than a role model or “international gold-standard”. This instrument can also be
126 understood to complement the Council of Europe’s Cybercrime convention⁵ and vice-versa.

127 **b. Methodology**

128 After the introduction and presentation of methodology in Section I., Section II. of this document is
129 divided in two parts.

130 The following pages include the different sections of the LI, with the text written in *Italic*. Underneath
131 each section follows the text of the proposed explanatory memorandum relevant for that section. The
132 explanatory memorandum was created to provide context and hopefully facilitate the understanding
133 of the intent of the authors of the LI.

134 Section III. contains the main sources of the document.

135 This draft has been developed with a strong focus on substance and irrespective of any institutional or
136 legislative framework. Hence, many procedural provisions (such as the ones referring to signature and
137 entry into force) are not included.

⁴ Cf. First Report of the UN SRP to the Human Rights Council, A/HRC/31/64 via
<http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc> - accessed on 22.09.2016, p.4.

⁵ Council of Europe, Convention on Cybercrime, Treaty No. 185 via
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> - accessed on 22.09.2016.

138

II. Text, Context and Commentary

139

Preamble

140

(1) Human rights and fundamental freedoms that people enjoy offline, as enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, must equally be guaranteed and protected online.

145

(2) The exercise of human rights in the Digital Age, in particular the right to privacy and freedom of expression, is an issue of increasing interest and importance as the rapid pace of technological development allows persons all over the world to use digital technologies (DTs). The access to and use of these technologies is crucial to enable development, especially the development of personality in the digital age. Children, minors and persons developing a gender identity benefit to a very high degree from these new capabilities and opportunities. However, these groups are particularly dependent on efficient safeguards and effective remedies.

153

(3) DTs can be an important tool for fostering individual and civil society participation. They can be useful in bridging many forms of the digital divide. They contribute to the development of knowledge societies, to the empowerment of women and assist persons with disabilities in participating more comprehensively in public, social, economic and private life. While DTs enable an unprecedented flow of information and create tremendous potential for social and economic development, they also pose new risks and demand concrete actions to transform the essence of human rights to the digital age.

160

(4) All human rights are rooted in human dignity. Human dignity must be respected, protected and promoted using a holistic approach. Human Rights must be considered as one entity, which include the rights of people to develop their lives and personalities as much as the rights of victims of crime and of persons to live in a safe and secure environment, as well as the right to a fair trial. Each of these rights shall only be limited if necessary and in a proportionate manner while restrictions imposed on rights shall not impair the essence of the right. The impact of the legal framework on the enjoyment of any of these rights should be assessed in its entirety and not limited to specific laws and/or regulations.

168

(5) If there is a legitimate aim to carry out government-led surveillance, as described and provided for by national and international human rights law, a necessary measure can be taken if a proportionality assessment is carried out following a three-step test: First, the measure which is taken must be potentially capable of realizing the legitimate aim. Secondly, the measure which is taken is required to reach the legitimate aim (in other words it must be the least-intrusive measure). Thirdly, the measure which is taken must be proportionate “strictu sensu”. This means that it is not only a capable measure which is the least intrusive one (steps 1 and 2), but also justified considering its impact on the overall situation and particularly other human rights potentially infringed during the implementation process.⁶ Only if all these criteria are met, a necessary measure is proportionate and can therefore be taken.

178

(6) It has become increasingly important to build confidence and trust in the Internet, not least with regard to freedom of expression, privacy and other human rights so that the potential of the Internet as, inter alia, an enabler for development and innovation can be realized, with full cooperation between governments, international organisations, civil society, the private sector, the technical community and academia. These stakeholders as well as persons have a

182

⁶ This last step could also be described as a “cost-benefit” analysis.

183 *responsibility to respect and protect freedom of expression and the right to privacy within their*
184 *means, particularly in cases where they are controllers and/or processors of personal data.*
185 *(7) While concerns about public security may justify the gathering and protection of certain*
186 *information, States must ensure full compliance with their obligations under international*
187 *human rights law. Surveillance, including interception of communications, as well as collection*
188 *of personal data, are highly intrusive acts and when conducted in violation of human rights*
189 *standards can jeopardize privacy and freedom of expression, and are inconsistent with a*
190 *democratic society founded on the rule of law and human rights.*
191 *(8) Many international and regional systems of law explicitly lay down that in order to restrict,*
192 *limit, or interfere with an individual's enjoyment of the right to privacy a measure, which shall*
193 *be subjected to independent prior authorization and targeted by nature, must*
194 *a. be provided for by a law,*
195 *b. pursue a legitimate aim,*
196 *c. be necessary and proportionate to the pursued aim*
197 *d. while providing appropriate safeguards specified within the law.*
198 *e. Furthermore, surveillance activities should be authorized by an independent judiciary or*
199 *authority whose activities are governed by the rule of law and*
200 *f. overseen by a at least one legitimate body.*
201 *(9) Recognizing that privacy online is essential for the realization of the right to freedom of*
202 *expression and to hold opinions without interference, and the right to freedom of peaceful*
203 *assembly and association, the States which sign this legal instrument declare the following:*

204 -----

205 The preamble mainly refers to wording that was developed by the United Nations (UN) following the
206 resolution on the Right to Privacy in the Digital Age which also established the mandate of the SRP.⁷ It
207 particularly reflects language which can be found in a resolution of the Human Rights Council of 27th
208 of June 2016 on the promotion, protection, and enjoyment of human rights on the internet.⁸

209 Paragraph (par.) 4 contains a commitment to a holistic approach to human rights which are rooted in
210 human dignity. Ultimately, the entirety of human rights should result in the protection, respect and
211 promotion of human dignity. This is important when considering privacy and other human rights
212 relating to personal development, the right to live in security and the rights of victims of a crime.

213 Furthermore, this is also important when considering the overall impact of laws relating to
214 governmental surveillance in one country, one region or globally. Such laws and provisions ought to
215 be considered in their entirety and not one by one. The rights concerned in a specific case or situation
216 (apart from absolute human rights like the prohibition of torture or ius cogens rules of international
217 law like the prohibition of genocide) must be considered together and ultimately a solution sought
218 which respects, protects and promotes all human rights – security and privacy, freedom of expression
219 and privacy, etc. LEA and SIS must have the capacity, with appropriate safeguards and oversight, to
220 develop appropriate surveillance to ensure public safety and preserve the right to life and security.

221 Hence, the focus on freedom of expression and privacy is deliberate, since it allows any
222 (inter)governmental organization to relate to the right to privacy as construed and constructed in the
223 respective binding legal framework. This also allows the text to be flexible.

⁷ United Nations, Human Rights Council Resolution 28/16. For more sources see the sources provided at the end of this document.

⁸ United Nations, Human Rights Council, A/HRC/32/L.20.

224 While all stakeholders have a responsibility to respect and protect fundamental rights also in a digital
225 context it remains clear that this can only happen within their means. Among the stakeholders
226 mentioned, states clearly have the responsibility of controlling law enforcement requests and national
227 security agencies practices. States should not only refrain from infringing these rights on a domestic
228 and international level, they should also protect and promote them domestically and internationally
229 and support an environment which enables the development of personality freely and positively.

230 The term “measure” relates to an act by a state or on its behalf or at its order which as an effect
231 restricts the right to privacy of an individual.

232 Par. 8 also adds the requirement in lit. c for any limitation of a right to be necessary and proportionate.
233 Here, as everywhere in this text those terms should be understood in the following way: Necessity is
234 referring to the specific end or purpose (“telos”) of a measure. Necessity should be prescribed by law
235 which itself must be the result of a legitimate legislative process. Typically, necessity is a purpose that
236 is legitimate in a society which is based on values such as human rights, rule of law and democracy.

237 To learn further about regional examples mentioned in par.8 one can consult the case of the European
238 Court of Human Rights (ECtHR) in the case of Zakharov vs. Russia.⁹ Particularly, the notions of the
239 abstract nature of surveillance (mn. 171) and the requirement of the foreseeability of surveillance (mn.
240 229) have been discussed.¹⁰ Another regional example to be considered is the judgment of the Court
241 of Justice of the European Union (CJEU) in the joined cases C-203/15 and C-698/15 Tele 2 Sverige and
242 Watson.¹¹ The targeting of a surveillance measure has been discussed in mn. 109 - 111. Necessity is
243 discussed in mn. 118 – 121.

244 Further cases that should be considered from the Inter-American System of Human Rights are Donoso
245 v. Panama and Escher et al. v. Brazil.¹²

246 -----

247 *Article 1*

248 *Subject matter and objectives*

249 *(1) The subject matter of this legal instrument is surveillance through digital technology. It aims at*
250 *safeguarding the fundamental rights and freedoms of persons with regard to the deployment*
251 *and use of surveillance systems, as well as non-surveillance data when used for surveillance*
252 *purposes.*

253 *(2) In accordance with this legal instrument, States shall ensure the implementation of the*
254 *measures herein to protect the fundamental rights and freedoms of persons when a*
255 *surveillance system is used, as well as when non-surveillance data are used for surveillance*
256 *purposes.*

257 *(3) Surveillance systems as well as the use of non-surveillance data should be designed and*
258 *function to ensure the right to privacy, notably through the use of privacy-enhancing*

⁹ ECtHR, Roman Zakharov v. Russia, App. No. 47143/06 via <http://hudoc.echr.coe.int/eng?i=001-159324> accessed on 28 February 2017; General principles are being discussed in mn. 227 -234.

¹⁰ Ibidem.

¹¹ CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970,

¹² Inter-American Court of Human Rights, Case of Tristán Donoso v. Panamá, Judgment of 27.01.2009 also available via http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_ing.pdf - accessed 25.10.2017; Ibid., Case of Escheret al. v. Brazil, Judgment of 20.11.2009 also available via http://www.corteidh.or.cr/docs/casos/articulos/seriec_208_ing.pdf - accessed 25.10.2017.

259 *technologies and in accordance with the achieved state of technological knowledge and*
260 *operational capabilities.*

261 -----

262 The formulation “legal instrument” is an interim one and is capable of being substituted by the term
263 “Treaty”, “Convention”, “Recommendation” or “Directive” depending on the binding force that parties
264 may wish to accord the instrument. It is intended that the LI is capable of being used in part or in whole
265 by regional intergovernmental organisations such as the European Union (EU) or the Council of Europe
266 (CoE) or indeed even at the global level by the UN. This is consistent with the MAPPING project’s
267 finding that, when it came to surveillance through DTs, there was no discernible difference between
268 the concerns of stakeholders inside Europe and of those outside Europe. The concerns were as
269 universal as the right to privacy set out in Art 12 UDHR/Art 17 ICCPR, Art 8 of the European Convention
270 on Human Rights and Art 7/8 of the EU Charter of Fundamental Rights as well as similar provisions laid
271 down in equally relevant regional protection mechanisms such as Art 11 of the American Convention
272 on Human Rights. It may also be used by States wishing to have a set of principles on which to model
273 their domestic law until a regional or global agreement is reached and to which they could conceivably
274 adhere.

275 Article (Art.) 1 defines the subject matter of this legal instrument. It addresses surveillance carried out
276 by using or manipulating digital technologies. Such activities are carried out by States on their behalf
277 or at their order. While most of these activities will be carried out online using the Internet, it is also
278 possible that other electronic technologies are being used. The LI is not aiming at covering
279 conventional surveillance in the physical world, but surveillance using or facilitated by digital
280 technologies and typically over the Internet. It tries to provide an answer to the issues raised in
281 instances such as the revelations of Edward Snowden, the blocking of Internet services by governments
282 with little or no justifiable arguments, and the questions that arise while studying cases such as Apple
283 vs the FBI.¹³ However, not only direct efforts of States to gather information electronically are covered.
284 Information received from other States or data repurposed from parties in other countries beyond
285 their jurisdiction are subject to this text, too. Furthermore, the LI is drafted to tackle these challenges
286 from a perspective which has international human rights protection and human dignity at its centre.

287 Par. 1 is concerning the right of all persons in the jurisdiction of a State, not only citizens.

288 Par. 2 should not be read as balancing security against privacy or any other fundamental human right.
289 In the view of the drafters it is necessary that fundamental human rights are promoted in a
290 comprehensive manner. Rather than a trade-off between rights, ways should be sought to strengthen
291 them collectively and to ultimately promote human dignity. Hence, it is necessary to provide both
292 privacy and security rather than the one or the other.

293 Par. 3 refers to the basic setup of technologies of surveillance which should follow an approach where
294 the purpose and aim of the activities are clearly laid out before information is gathered. Information
295 gathering should be strictly limited to what is necessary and proportionate.

296 -----

297 *Article 2*

298 *Definitions*

299 *For the purpose of this legal instrument, the following definitions shall apply:*

¹³ More information on this and encryption is in the First report of the SRP to the UN General Assembly, available via <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx> - accessed on 22.09.2016.

- 300 (1) *'surveillance'* is any monitoring or observing of persons, listening to their conversations or
301 other activities, or any other collection of data referring to persons regardless whether this is
302 content data or metadata. Surveillance is carried out by a state, or on its behalf, or at its order.
- 303 (2) *'surveillance system'* refers to any organised means or resources designed, and/or intended to
304 be used for surveillance.
- 305 (3) *'smart system'* refers to a system which incorporates functions of sensing, autonomous
306 decision-making and actuation.
- 307 (4) *'smart surveillance system'* means a smart system used for surveillance.
- 308 (5) *'surveillance data'* is data the primary purpose for the creation of which is surveillance and/or
309 non-surveillance data that is acquired, retained, analyzed, shared or otherwise used for
310 surveillance. This includes data the primary purpose for the creation of which is surveillance
311 and gathered as a result of acts by a State or on its behalf or at its order without the use of a
312 dedicated surveillance system.
- 313 (6) *'non-surveillance data'* is data the primary purpose for the creation or collection of which is not
314 surveillance, but which could be searched or interrogated because the data contained therein
315 may, through either pattern recognition or applied search methods yield personal data which
316 may be useful for the prevention, detection, investigation and prosecution of crime and/or for
317 increasing public safety and/or protecting state security.
- 318 (7) *'personal data'* is any information relating to an identified or identifiable natural person (*'data*
319 *subject'*); an identifiable natural person is one who can be identified, directly or indirectly, in
320 particular by reference to an identifier such as a name, an identification number, location data,
321 an online identifier or to one or more factors specific to the physical, physiological, genetic,
322 mental, economic, cultural or social identity of that natural person.
- 323 (8) *'controller'* is the competent public authority, agency or other body or natural or legal person
324 which alone or jointly with others determines the purposes and means of the processing of
325 personal data; where the purposes and means of such processing are determined by domestic
326 law, the controller or the specific criteria for its nomination may be provided for by domestic
327 law.
- 328 (9) *'competent authority'* means any public authority competent for the prevention, detection,
329 investigation and prosecution of crime and/or for increasing public safety and/or protecting
330 state security; or any other body or entity entrusted by State law to exercise public authority
331 and public powers for these purposes.
- 332 (10) *'processor'* means a natural or legal person, public authority, agency or other body which
333 processes personal data on behalf of the controller.
- 334 (11) *'processing'* means any operation or set of operations which is performed on personal data or
335 on sets of personal data, whether or not by automated means, such as collection, creation,
336 recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation,
337 use, disclosure by transmission, dissemination or otherwise making available, alignment or
338 combination, restriction, erasure, destruction, or the carrying out of logical and/or arithmetical
339 operations on such data.
- 340 (12) *'person'* describes any entity with the capability to have rights and/or duties. Parties to this
341 agreement notify on signature whether they wish to extend the scope of protection to legal
342 persons or keep it restricted to natural persons.

343 -----

344 Par. 1 defines surveillance as an act of government or entities which act on behalf of the government.
345 This is reflected in the wording "*by a state or on its behalf or at its order*". The definition is kept broad
346 intentionally to cover all possible aspects of governmental surveillance.

347 The term "surveillance" includes all forms of bulk acquisition of personal data,¹⁴ all forms of "mass
348 surveillance" and targeted surveillance. This sentence is also intended to cover all those instances
349 where the surveillance activity is carried out by non-state actors acting on behalf of or at the order of
350 any form of state authority.

351 Surveillance is only acceptable if it is based on reasonable suspicion.¹⁵ However, reasonable suspicion
352 is not a standard that is defined in international law outside Europe. When deciding whether
353 reasonable suspicion exists, it is necessary to demonstrate that the specific anticipated surveillance
354 will yield evidence of a serious crime or help mitigate the threat.

355 Most of the time surveillance might be carried out through the collection and processing of data as
356 referred to in par. 5 (*'surveillance data' is data the primary purpose for the creation of which is*
357 *surveillance and/or non-surveillance data actually being used for surveillance*).

358 Nevertheless, the LI also refers to data which was originally collected for other purposes and is being
359 re-used for surveillance as defined in par. 5. In such cases data, which was originally non-surveillance
360 data, also becomes surveillance data according to par. 6. The main characteristic to distinguish
361 surveillance and non-surveillance data is the original purpose for the creation of the data.

362 Both, the definition of surveillance data in par. 5 and non-surveillance data in par. 6 include not only
363 the actual content of conversations, messages, activities etc., but also metadata generated about it.

364 The definition in par. 7 (personal data), par. 10 (processor) and par. 11 (processing) are the same as in
365 the General Data Protection Regulation of the European Union (GDPR) and its Article 4.¹⁶

366 The term "*natural person*" was used therefore in par. 7. It is possible that legal persons (like
367 corporations) are entitled to fundamental rights like privacy or similar rights in different States. This
368 aspect is covered in the definition of person in par. 12. Since the situation differs from State to State

¹⁴ As adapted from the UK Government's Operational case for bulk powers (2016 – see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf :

Through the bulk interception of communications . This involves intercepting international communications as they travel across networks.

Through bulk equipment interference. This involves the acquisition of communications and equipment data directly from computer equipment overseas. Historically, this data may have been available during its transmission through bulk interception. The growing use of encryption has made this more difficult and, in some cases, equipment interference may be the only option for obtaining crucial intelligence.

As bulk communications data, obtained from communications service providers. Communications data can be invaluable in identifying the links between subjects of interest and uncovering networks.

As bulk personal datasets. This involves the use of datasets such as travel data or Government databases. Like communications data, the information included in those datasets is generally less intrusive than data acquired through equipment interference or interception.

¹⁵ CJEU, *Tele 2 Sverige*, C-203/15, ECLI:EU:C:2016:970, mn. 103: "Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight [...]."

¹⁶ EU, Official Journal L 119/33, 04.05.2016

369 and because of different legal traditions in different states it is left to them to decide whether they
370 choose to extend protection to legal persons or not.

371 The definition in par. 8 (controller) is similar to the one in Art. 4 (7) of the GDPR. It has been modified
372 to be consistent with the rest of the legal instrument.

373 The definition of par. 9 (competent authority) is based on the definition of Art. 3 (7) of the Directive
374 (EU) 2016/680.¹⁷

375 -----

376 *Article 3*

377 *Basic requirements for government-led surveillance*

378 (1) *No surveillance, domestic or foreign, civil or military, may be carried out except by a law*
379 *enforcement agency (LEA) or a Security and Intelligence Service (SIS) or any public-mandated*
380 *entity (PME) tasked by a specific law.*

381 (2) *This law shall be publicly available. The provisions shall meet a standard of clarity and precision*
382 *that is sufficient to ensure that persons can foresee its application.*

383 (3) *Any law regulating surveillance shall limit the purposes to*
384 *a. the prevention, investigation, detection or prosecution of crime and/or*
385 *b. increasing public safety and/or*
386 *c. protecting state security.*

387 (4) *The surveillance itself must be provided for by law which respects, protects and promotes the*
388 *essence of human rights. Any surveillance shall be necessary and proportionate which includes*
389 *that the least intrusive means shall be used.*

390 (5) *LEAs and PMEs shall include tax, revenue, customs and anti-corruption authorities. SIS shall*
391 *include all forms of intelligence and security services, whether civil, military or signals*
392 *intelligence, foreign or domestic.*

393 (6) *No surveillance, except that of foreign military personnel, serving members of LEAs, SIS and*
394 *PMEs may be carried out by any entity the existence of which is secret. All LEA, SIS and other*
395 *PME authorized by law to conduct surveillance shall be created and governed by laws which*
396 *shall also provide adequate safeguards against the abuse of powers and particularly*
397 *surveillance.*

398 (7) *These safeguards shall include but shall not be restricted to a system of checks and balances*
399 *consisting of:*

400 *a. Legislative oversight on a regular basis and at least quarterly, by a Committee of the*
401 *regional or national elected legislative body responsible for the entity funding and*
402 *tasked for the purpose by law, of the budgetary and operational performance of all*
403 *LEAs, SIS and PMEs authorized by law to carry out surveillance, both domestic and*
404 *foreign, with the authority to temporarily or permanently withhold, suspend, grant or*
405 *cancel the funding of any surveillance program or activity;*

406 *b. A Pre-Authorisation authority, completely independent from the entity and the*
407 *executive or legislative branches of government, composed of one or more members*
408 *with the security of tenure of, or equivalent to, that of a permanent judge which is*
409 *tasked by law to evaluate ex-ante requests from and grant permission to LEAs, SIS and*
410 *PMEs as shall be required under law prior to the conduct of lawful surveillance;*

¹⁷ EU, Official Journal L 119/89, 04.05.2016.

- 411 c. *An Operational Oversight authority, completely independent from the entity, the Pre-*
412 *Authorisation Authority and the executive or legislative branches of government,*
413 *composed of one or more members with the security of tenure of, or equivalent to, that*
414 *of a permanent judge which is tasked by law to exercise ex-post oversight over and*
415 *exercise accountability of LEAs, SIS and PME as shall be required under law especially*
416 *for the conduct of lawful surveillance;*
417 d. *Inter-institutional whistle-blower mechanisms that allow for anonymity of the whistle-*
418 *blower(s), protection from retaliation and include extra-authoritarian and/or extra-*
419 *institutional review of the process including remedies;*
420 e. *The presentation and publication of reports, at minimum on an annual basis, by the*
421 *Legislative, Pre-Authorisation and Operational Oversight Authorities.*
422 (8) *Any LEA, SIS or PME carrying out surveillance must be explicitly authorized to do so and*
423 *regulated by a specific law defining the*
424 a. *exact Purposes.*
425 b. *tasks.*
426 c. *objectives.*
427 d. *activities.*
428 e. *basic administrative functions and setup.*
429 (9) *Any surveillance activity must only be carried out for concretely defined specific and legitimate*
430 *purpose and in response to a concrete and legitimate need. Except in those cases where it*
431 *concerns serving foreign military personnel, serving foreign LEA, SIS or PME officers, all*
432 *surveillance, domestic and foreign, shall be carried out only provided that a relative warrant is*
433 *obtained ex-ante from the regional or national pre-authorisation agency in the case of persons*
434 *or data located within the regional or national jurisdiction, or that an International Data Access*
435 *Warrant (IDAW) is obtained from the International Data Access Commission (IDAC) as created*
436 *in terms of Article 16 of this legal instrument, or provided that a valid legal request is obtained*
437 *ex-ante under a legal framework for cross-border requests that includes the relevant regional*
438 *or national government authorities.*
439 (10) *When any form of warrant for surveillance is requested, the only criteria that may be taken*
440 *into account is that of reasonable suspicion. The race, colour, gender, language, religion,*
441 *political or other opinion, national or social origin, citizenship, property, birth or other status of*
442 *the suspect cannot be advanced or accepted as being adequate or relevant grounds for the*
443 *issue of any form of surveillance warrant.*
444 (11) *Any law authorising surveillance must include intelligible, accessible and effective procedural*
445 *remedies for persons whose rights may have been violated.*
446 (12) *The budget of any entity carrying out surveillance must be defined clearly and subject to review*
447 *on the executive, political and judicial level, albeit when necessary and appropriate the review*
448 *process may be carried out in camera.*

449 -----

450 This article defines the basic requirements a government must fulfil when carrying out surveillance
451 (as defined for the purposes of this text).

452 Par. 1 states that any surveillance activity must be based on a specific law. The term surveillance
453 shall be understood broadly since it includes domestic and foreign oriented activities and includes
454 civil and military actions.

455 There are overall three types of entities that are potentially able to carry out surveillance: LEAs
456 (typically providing inner security and stability), SIS (typically providing external security and
457 stability) and public mandated entities (PMEs; can be private contractors).

458 A specific law is also required to regulate activities for PMEs. For example, the ECtHR made clear
459 that the State cannot absolve itself from responsibility by delegating its obligations to private
460 bodies or persons.¹⁸

461 When surveillance is carried out through PMEs the government always remains in full control of,
462 and fully responsible for, the entire surveillance process, data, and use and further processing of
463 data. The outsourcing of surveillance activities to PMEs may divert responsibility away from police,
464 judicial or national security departments and onto small companies that cannot be held
465 accountable to constitutional prohibitions. Therefore, private entities that are involved in the
466 surveillance process must be subject to stringent deontological rules and confidentiality
467 requirements and be under a contractual obligation to provide full transparency and governmental
468 access to their technical and organisational arrangements governing the surveillance activities.
469 State entities must be provided with sufficient expertise and resources in order to be able to
470 remain in full control of any surveillance activities that are outsourced to private entities.

471 Furthermore, “LEAs and PMEs shall include tax, revenue, customs and anti-corruption authorities”
472 which suggests a broad understanding which is also applicable to SIS.

473 The specific law provides increased legitimacy for surveillance activities. It enables a better
474 understanding for the need to carry out surveillance. Additionally, it becomes more likely that the
475 general scope of activities is subject to a broad discussion while details regarding individual
476 operations must not necessarily be disclosed. Such a law should also be containing which kind of
477 information is being collected and which authorities can access the data under which
478 circumstances. Additionally, it should be laid down how the data is being managed once it has lost
479 relevance.

480 According to par. 3 the specific law supports States in their efforts to maintain the basic order of a
481 society. The purposes of surveillance are therefore limited to the three mentioned in lit. a – c. It is
482 important that the definition of surveillance in Art. 2 is considered together with the legitimate
483 purposes in this par.

484 It is not necessary to separately include “the economic interest of the State” since serious crimes
485 relating to it can legitimize surveillance per se. Industrial espionage or other activities that enable
486 the unauthorized use of intellectual property are not legitimate purposes to carry out surveillance.

487 The terms necessity and proportionality as well as the criteria to establish them have already been
488 discussed and described in the explanatory memorandum of the preamble. See there for more
489 information.

490 Par. 6 clarifies that there are no secret parts of a State which carry out any kind of surveillance.
491 Those LEAs, SIS or PMEs who carry out surveillance do so in an environment with safeguards
492 including a system of checks and balances.

493 This system (par. 7) consists of regular and effective legislative oversight (lit. a), an independent
494 pre-authorisation authority (ex-ante oversight, lit. b), an independent operational oversight
495 authority (ex-post oversight including accountability of LEAs, SIS and PMEs, lit. c), inter-

¹⁸ ECtHR, *Wos v Poland*, App.No. 22860/02, 01.03.2005.

496 institutional whistle-blower mechanisms (lit. d). On the latter, there are situations where internal
497 channels will not be effective at calling attention to systemic tolerance of wrongdoing, and public
498 disclosure should be either protected, or at least potentially defensible.¹⁹ The presentation and
499 publication of separate reports compiled by the legislative oversight, independent pre-
500 authorisation and independent operation oversight authority (lit. e). These measures are supposed
501 to reinforce each other and are a complete system. In the understanding of the drafters of this
502 document, oversight is not a finished product. Rather it is constant work in progress.

503 On the notion of independence in this section and other sections of the text see also the “Basic
504 Principles on the Independence of the Judiciary” and numerous treaty-based standards and
505 comments on this subject that are collected by the Office of the High Commissioner for Human
506 Rights.²⁰

507 Par. 9 forbids any surveillance measures that are being carried out without a legitimate aim. It is
508 forbidden to carry out any surveillance for the mere collection of information or potential future
509 use apart from any concrete threat or case.

510 Par. 10 forbids any surveillance based on discriminatory motives. Any surveillance must be based
511 on reasonable suspicion and leave out any other motives to start an investigation. Reasonable
512 suspicion must be particular to the target of the surveillance, rather than simply a reasonable
513 suspicion that exists generally. It refers to the “*race, colour, gender, language, religion, political or
514 other opinion, national or social origin, citizenship, property, birth or other status*” of a person. The
515 term political or other opinion also includes philosophical beliefs. The term other status can be
516 read as also referring to age, sexual orientation, or other characteristics that are integral to human
517 identity. This also applies to other sections of the text where this list of characteristics is used.

518 Par. 11 establishes remedies for any individual concerned by a surveillance measure. Furthermore,
519 the phrasing persons makes clear that such a person need not be a citizen of a particular country.
520 While the detailed circumstances of such a (often judicial) review procedure must not necessarily
521 be disclosed any party to this agreement must guarantee that a meaningful review that fully
522 protects the right to a remedy for violations of human rights takes place and that individual human
523 rights are being protected, respected and promoted when carrying out surveillance activities.

524 Par. 12 refers to the budget of entities carrying out surveillance. The budget need not be disclosed
525 in detail necessarily, but it must be subject to checks and balances, external evaluation and review.
526 In many countries this will be done through legislative control such as parliamentary control.

527 -----

528 *Article 4*

529 *General Principles*

530 *When considering the use of surveillance systems, as well as the use of non-surveillance data for*
531 *surveillance purposes, States shall adhere to the following principles:*

532 *(1) States shall provide that surveillance systems shall be authorised by law prior to their use. This*
533 *law shall,*

¹⁹ Also compare the “Tshwane Principles”, particularly 38-43; United Nations, Special Rapporteur on the freedom of expression, David Kaye Sept. 2015 report via

http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361 - accessed 22.02.2018.

²⁰ For an online version of the UN Basic Principles on the Independence of the Judiciary see:

<http://www.ohchr.org/EN/ProfessionalInterest/Pages/IndependenceJudiciary.aspx> - accessed 25.10.2017.

- 534 a. *identify the purposes and situations where the surveillance system is to be used.*
535 b. *define the category of serious crimes and/or threats for which the surveillance system*
536 *is to be used.*
537 c. *state that the agency using the surveillance system should only use the system in cases*
538 *where a reasonable suspicion exists that a serious crime may be committed or a*
539 *genuine threat to security exists;*
540 d. *define and provide the least intrusive measures which potentially might be suitable to*
541 *achieving the aim.*
542 e. *demand from the authority to justify that each single measure envisaged is necessary*
543 *and proportionate for the obtaining of vital intelligence in an individual operation as*
544 *well as considering the overall impact of this and such measures on the right to privacy*
545 *of persons irrespective of whether this is a citizen or resident of that state.²¹*
546 f. *provide that any final decision on enacting the surveillance system shall be subjected*
547 *to independent prior authorization before actual surveillance takes place.*
548 g. *provide that the deliberate monitoring of an individual's behaviour or other*
549 *information by the State should only be targeted surveillance carried out on the basis*
550 *of reasonable suspicion.*
551 h. *provide that the individual concerned is likely to have committed a serious crime or is*
552 *likely to be about to commit a serious crime. Such domestic law shall establish that an*
553 *independent authority, having all the attributes of permanent independent judicial*
554 *standing, and operating from outside the law enforcement agency or security or*
555 *intelligence agency concerned, shall have the competence to authorise targeted*
556 *surveillance using specified means for a period of time limited to what is appropriate*
557 *to the case.²²*
558 i. *provide that where the person to be subjected to targeted surveillance and personal*
559 *data pertaining to that individual are to be found outside the jurisdiction of the state*
560 *then the law enforcement agency or the security service or intelligence agency*
561 *concerned would be empowered to apply for an International Data Access Warrant*
562 *(IDAW) to the International Data Access Authority (IDAA) set up in terms of this legal*
563 *instrument.*
564 j. *ensure that all public and private entities within the jurisdiction of the State would*
565 *comply with the requirements of a properly constituted International Data Access*
566 *Warrant (IDAW) immediately with the same effect as if that warrant had been issued*
567 *by a court established within that particular State. In such cases the domestic law*
568 *should provide that territoriality or jurisdiction cannot be raised as a reason or a*
569 *defence for the public or private entity concerned not complying with an IDAW request*
570 *to hand over or otherwise make accessible the personal data requested.*
571 k. *state that the authority carrying out the surveillance shall, unless an independent*
572 *authority has adjudicated that it would not be appropriate or feasible to do so and/or*

²¹ This provision can be understood in connection with the ECtHR judgment in Szabo and Vissy v Hungary, App. No. 37138/14, para. 73. The second part is inspired by the German constitutional court's development of a holistic approach ("Überwachungsgesamtrechnung") to the extent of surveillance in society declaring that a measure of precautionary surveillance cannot be examined in isolation, but must always be seen in the context of the totality of the existing collections of data on the persons as established in BVerfG, 1 BvR 256/08 [2010], paragraph 218

²² ECtHR, App. No. 47143/06, Zakharov vs. Russia, via <http://hudoc.echr.coe.int/eng?i=001-159324> – accessed on 22.09.2016. Mn. 264: "[...] it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such information may be made by names, addresses, telephone numbers or other relevant information."

573 *this would be prejudicial to the completion of ongoing or future investigations or the*
574 *prevention, detection or prosecution of a specific criminal offence or threat, without*
575 *undue delay [within a period of time established by law] explain in writing the use of*
576 *the surveillance system in the particular situation to any person who was directly or*
577 *indirectly subject to such surveillance.*

- 578 *l. set the length of time information obtained from the surveillance system should be*
579 *kept and by whom it may be accessed at each stage as well as requirements for*
580 *permanent deletion or destruction upon the expiration of the relevant period.*
- 581 *m. set up an independent surveillance oversight authority to monitor the conduct of*
582 *surveillance and ensure that the provisions of the law are followed.*
- 583 *n. provide for an individual right to redress for subjects of surveillance.*

584
585 *(2) States should set up and promote procedures to ensure transparency about and accountability*
586 *for government demands for surveillance data and non-surveillance data for surveillance*
587 *purposes. Such procedures should include, but are not limited to:*

- 588 *a. Publicly available, periodic reports allowing for a substantive and comprehensive*
589 *review of the activities of relevant agencies to other State entities such as the legislative*
590 *branch and/or the judicial branch of a State.*
- 591 *b. Publicly available transparency reports by the State itself in respect to all requests*
592 *made to corporations and other non-state actors with regard to the provision of*
593 *personal data including categories, and frequency.*
- 594 *c. Provide for transparency regarding surveillance law regulations and the power of*
595 *agencies who carry out surveillance.*
- 596 *d. Setting up of a documented, regular and ongoing process of dialogue with civil society*
597 *and academia and other stakeholders on the purpose and design of surveillance*
598 *systems and the use of non-surveillance data for surveillance purposes.*
- 599 *e. Support and encouragement of publicly available transparency reports by corporations*
600 *and other non-State entities which provide personal data if the core activities of the*
601 *controller or the processor consist of processing operations which, by virtue of their*
602 *nature, their scope and/or their purposes, require regular and systematic monitoring*
603 *of data subjects on a large scale. States must not prohibit corporations from publishing*
604 *transparency reports.*

605 *(3) When considering the use of surveillance systems, as well as the use of non-surveillance data*
606 *for surveillance purposes, States should respect and protect the free flow of information and*
607 *the stability of information and communication technologies and services. Particularly, States*
608 *are prohibited from directly or indirectly ordering or compelling*

- 609 *a. service providers in their jurisdiction to disconnect, shut down access or otherwise*
610 *broadly disrupt or block flows of information.*
 - 611 *i. States shall respect the secrecy of telecommunications in accordance with both*
612 *their own laws and the laws of the State of the originator of such*
613 *correspondence, applying whichever has the stronger privacy protections.*
 - 614 *ii. If in an individual case a State agency has reasonable suspicion that a*
615 *particular service was set up and/or is being used substantively for an illegal*
616 *purpose a service provider may be required to deny that service on the*
617 *presentation of a legal request issued pursuant to applicable laws in*
618 *accordance with the rule of law. Any such limitation must be necessary and*
619 *proportionate as well as strictly limited to the extent of such illegal use.*

- 620 iii. *States shall issue publicly available annual reports on such individual cases*
621 *describing the frequency and extent of the interruption.*
- 622 b. *service and hardware providers to take measures which negatively impact the security*
623 *– including the security of technologies such as encryption – of digital services or*
624 *products.*
- 625 c. *that actions are taken which require data localization.*
- 626 d. *that agencies carrying out an investigation and seek to use information held by private*
627 *entities give false, misleading or incomplete explanations of the reason for their*
628 *request or the legal authority for their making it.*
- 629 e. *a lowering of standards through legislative or other measures of the protection of*
630 *privileged communications and records of privileged communications.*
- 631 (4) *When setting up and operating surveillance systems, as well as while using non-surveillance*
632 *data for surveillance purposes, States shall*
- 633 a. *not assert extra-territorially jurisdiction over data or persons in contravention of*
634 *relevant treaties and principles of international mutual legal assistance.*
- 635 b. *seek to establish appropriate bilateral and/or multilateral international legal*
636 *frameworks to facilitate cross-border requests for data in a manner that adheres to the*
637 *rule of law and is consistent with international human rights law.*
- 638 (5) *If States share intelligence*
- 639 a. *such activities shall be subject to an oversight regime equivalent to and as effective as*
640 *described in Art. 3 par. 7.*
- 641 b. *they are required to ensure that oversight authorities have access to any relevant*
642 *information necessary to evaluate the legality, necessity and proportionality of the*
643 *sharing and the agreements that form the basis of such activities.*
- 644 c. *they shall empower oversight authorities to review decisions and/or undertake*
645 *independent investigations concerning the activities.*
- 646 d. *they shall ensure that this information is only shared with states that have equivalent,*
647 *effective and adequate mechanisms in place to guarantee similar standards and*
648 *safeguards.*

649 -----

650 This Art. defines the General principles states should be adhering to when carrying out surveillance
651 activities.

652 The phrase in par. 1 “*authorised by law*” should be interpreted with reference to the categories laid
653 down in European Court of Human Rights (ECtHR) judgment in the case of Roman Zakharov vs. Russia.²³
654 Particularly, authorised by law means that there is an actual request for surveillance, a certain level of
655 suspicion (e.g. reasonable suspicion), impartial and effective oversight of the activities, authorization
656 by judicial warrants and no bulk collection of information. The latter principle of no bulk collection has
657 since been very strongly entrenched in European law by the decision of the European Court of Justice
658 in Sverige² and Watson of 21 December 2016.²⁴

²³ ECtHR, App. No. 47143/06, Zakharov vs. Russia, via <http://hudoc.echr.coe.int/eng?i=001-159324> – accessed on 22.09.2016. Mn. 260 defines that an independent authority charged with authorising surveillance “must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.”

²⁴ CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970.

659 Furthermore, States must identify the purposes and situations where the surveillance system may be
660 used to a degree of granularity beyond the general purposes of national security or crime prevention.

661 Par. 1 was created to contain a proportionality assessment, but reaches further than that. It
662 additionally contains provisions on how to handle a case where surveillance was used after the
663 information was gathered.

664 Targeted surveillance is only acceptable if is based on reasonable suspicion as mentioned in par.1 lit.
665 c.²⁵ However, reasonable suspicion is not a standard that is sufficiently defined in international law
666 except possibly outside European Law. When deciding about whether reasonable suspicion exists, it is
667 necessary to demonstrate that the specific anticipated surveillance will yield evidence of a crime or
668 help mitigate the threat. This also applies to the level of suspicion that must exist to act in accordance
669 with par. 4 lit. a.

670 The requirement in par. 1 lit. d that the surveillance system defines the least intrusive measures has
671 to be interpreted as being the “least intrusive means for achieving the legitimate aim in the particular
672 circumstances.” To make sure this is the case other less invasive techniques should have been
673 considered or it must be obvious from the outset that they are futile.

674 In par. 1 lit. k a time limit is mentioned. Here, as well as in the rest of this legal instrument, time limits
675 are set in square brackets as an indication of urgency of a procedure. However, each time limit may
676 have to be amended to address the special circumstance and criminal procedural law in the respective
677 State. The time limits need to fit the operational and managerial practices of a State. Nevertheless,
678 time in most of the procedures covered by this legal instrument is of the essence. Large delays in action
679 may result to delays in justice and hence reduced effectiveness of safeguards (“Justice delayed is
680 justice denied.”)

681 Par. 2 makes it mandatory for states to be transparent about the surveillance systems they employ.
682 They should also be required to explain how they are using them in principle. In this way, an ordinary
683 person should be able to understand the potential scope of surveillance activities. Without such
684 transparency the activities of LEAs and SIS cannot be legitimated in the context of a democratic society.
685 Par. 2 lit. a and b oblige States to setup a transparency report system both internally (checks and
686 balances) as well as externally for the public record. When doing so - as mentioned in 4.2.7. of the
687 Council of Europe Recommendation on Internet Freedom - oversight bodies involved in the process
688 should be empowered to obtain access to all relevant information held by public authorities, including
689 information provided by foreign bodies.²⁶ Furthermore, States should periodically evaluate their
690 implementation of human rights standards, including with respect to surveillance activities.

691 This should be augmented through broader exchanges with civil society and relevant stakeholders (lit.
692 c).

²⁵ CJEU, *Tele 2 Sverige*, C-203/15, ECLI:EU:C:2016:970, mn. 103: „Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight [...].“

²⁶ Council of Europe, Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom, via https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2016-5-of-the-committee-of-ministers-to-member-states-on-internet-freedom?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/ accessed 31.07.2017.

693 According to lit. e States must support/encourage private entities to report on the requests made to
694 them. This applies to all relevant private entities as long as the “*core activities of the controller or the*
695 *processor consist of processing operations which, by virtue of their nature, their scope and/or their*
696 *purposes, require regular and systematic monitoring of data subjects on a large scale.*” This exemption
697 typically removes this obligation for small and medium sized corporations or other small-scale private
698 entities as long as these do not carry out activities which are of particular interest to the state and the
699 public in the context of passing on private data to public entities for the purpose of surveillance.

700 Par. 3 is an obligation for States to create an environment which promotes the development of the
701 potential of DT regardless of territorial or protectionist considerations.

702 Par. 3 lit. a refers to shutting off the access to information networks broadly and indiscriminately. The
703 formulation also refers to a situation where the network is slowed down on purpose and becomes
704 practically useless. The phrase “limited to the extent of such illegal use” can refer to the suspension of
705 a specific user account or similar measures.

706 If State authorities reasonably believe that a particular service or site was setup for illegitimate
707 purposes or is being used substantively for an illegal purpose then it might be justified to shut down
708 that specific service. However, this must only be done *to the extent of such illegal use and* upon the
709 “*presentation of a legal request*” or in other words in the context of a fair procedure which is governed
710 by the principle of the rule of law, subject to independent and impartial oversight and respecting the
711 “equality of judicial arms” principle.

712 Par. 3 lit. b refers to the need to guarantee the security of information products and services. States
713 are banned from trying to weaken the development of security standards by requiring developers
714 and/or engineers to intentionally weaken the implementation of protective technologies. This
715 specifically prohibits states from banning any forms of encryption, requiring a service provider to
716 maintain keys or the ability to decrypt data, and requiring a service provider to weaken encryption. It
717 also prohibits states from requiring that a service provider create so-called “backdoors” and/or any
718 other technological measures designed to circumvent security measures that are intended to protect
719 the users of the service.

720 Par. 3 lit. c focuses on the issue of data localization and retention. States should be obliged to refrain
721 from ordering other entities to locate or store data.

722 Par. 3 lit. d makes it mandatory for State authorities to make their intentions clear when they interact
723 with persons, corporations and other private entities. This serves to reinforce the principles by which
724 the purpose and aim of an operation should be clearly set out before personal data is gathered.

725 Par 3 lit. e obliges States to not lower the standards of protection of “*privileged communications*”.
726 States should not pressure journalists or members of the press to disclose sources or limit the freedom
727 of press in an unjustified manner. States should establish specific legal procedures to safeguard the
728 professional privilege of groups such as members of parliament, members of the judiciary, lawyers and
729 media professionals. More on the nature and circumstances of privileged communications can be
730 found in the explanatory memorandum to Art. 5 par. 1 lit. a vii.

731 Par. 4 makes it clear that States should not try to impose territorial restrictions through regulatory
732 measures when technologies are cross-border in nature. States should not try to get access to data not
733 stored on their territory by putting persons under pressure because they or their offices are physically
734 located on their territory. In general, States should aim at establishing an international framework of
735 cooperation in those cases where law enforcement or information gathering is needed in a cross-

736 border scenario. This framework should be based on human rights principles and should allow for
737 technology to develop its full potential.

738 Par. 5 addresses the issue of intelligence sharing between countries. At the time of drafting this LI this
739 seemed to be an increasingly relevant activity to protect public order and safety and to protect the
740 rights of victims of crime. Hence, it should be ensured that the same standards and principles are
741 relevant for cross-border surveillance as for national surveillance activities.

742 The term “intelligence sharing” refers to (1) sharing of “processed” intelligence, (2) sharing of “raw”
743 personal and/or meta-data, (3) direct access to data, (4) joint operations of states to collect
744 intelligence.

745 -----

746 *Article 5*

747 *Domestic Measures related to the deployment of surveillance systems*

748 *(1) States shall provide that no new surveillance system can be deployed:*

749 *a. before an initial human rights impact assessment is carried out by an independent*
750 *external assessment body with the objective of ensuring that privacy and other human*
751 *rights are protected in accordance with the provisions of this instrument. The human*
752 *rights impact assessment must include analysis of:*

753 *i. necessity and proportionality of the surveillance system;*

754 *ii. technological security and state of art of the technology used;*

755 *iii. actions taken to minimise the risks to the enjoyment of rights of persons;*

756 *iv. compliance with privacy by design and privacy by default principles;*

757 *v. safeguards to ensure that personal data collected during surveillance is not kept*
758 *when no longer necessary for the purposes for which it was collected;*

759 *vi. social and ethical costs of deploying the surveillance system. Such costs must be*
760 *given due consideration and mitigation measures have to be sought where*
761 *appropriate;*

762 *vii. safeguards in place to protect privileged communications.*

763 *b. before the report of the initial human rights impact assessment in par. 1 was submitted*
764 *to the applicable competent authority, which can ask for additional measures to be*
765 *introduced before the deployment of the surveillance system can start.*

766 *c. unless an initial testing of the surveillance system, carried out by an independent*
767 *external assessment body, shows that adequate security means have been put into*
768 *place to prevent illegal access to the personal data, and to the algorithms of the smart*
769 *surveillance system by unauthorised persons or systems.*

770 *d. in the case of smart surveillance systems, the error rate is below the threshold*
771 *established for similar systems by a technical advisory body set up for this purpose or*
772 *submitted for human assessment in terms of Article 9.*

773 *(2) For existing surveillance systems, a human rights impact assessment which fulfils and is*
774 *equivalent to the requirements for new surveillance systems as laid down in par. 1 of this*

775 *provision has to be finalized no later than 12 months after the ratification of this agreement by*
776 *a state party.*

777 (3) *Any surveillance measure using systems that comply with this article is subject to a judicial*
778 *warrant.*

779 -----

780 This article refers to states and the measures they need to take if they want to carry out surveillance
781 activities.

782 Par. 1 lays down the detailed criteria of a “human rights impact assessment” which is mandatory before
783 the deployment of surveillance systems. Par. 2 mirrors the same criteria for existing surveillance
784 systems.

785 Par. 1 lit. a refers to an “*independent external assessment body*”. Such a body should consist of formally
786 independent experts from different parts of the domestic stakeholder community (civil society,
787 government, corporations, data protection authorities, etc.) who have access to all information
788 necessary to evaluate the deployment of a concrete surveillance system. These experts also have to
789 have the necessary qualification and assistance (resources) to effectively evaluate the system and
790 report to the authority responsible for the deployment of the system. The competent authority
791 responsible for the deployment of the system itself has to subject to political and/or judicial oversight
792 (checks and balances).

793 Par. 1 lit. a iii could include measures relating to the use and development of data mining algorithms.
794 Such activities should be subject to regular assessments of the likely impact of the data processing on
795 the rights and fundamental freedoms of data subjects. The basic structure of the analysis should be
796 based on predefined risk indicators which have been clearly identified in advance. The relevance of
797 individual results of such automatic assessments should be carefully examined on a case-by-case basis,
798 by a person in a non-automated manner.²⁷

799 Par. 1 lit. a vii refers to “*privileged communications*”. There is a variety of such relations that various
800 legal systems may recognize (e.g. spousal relations, caregiver or guardian relations, parent-child
801 relations, parliamentary privilege, clerical relations, journalist-source, etc.). This also includes
802 specifically protected professions and the privileged communications they might have with patients or
803 clients (such as doctors or lawyers). The protections are to be defined in detail by a member states
804 domestic law. Only communications falling outside the scope of the privilege may be intercepted.

805 Par. 1 lit. d sets up a similar requirement to that established in Par. 1 lit. a, but for smart surveillance
806 systems. A “*technical advisory body*” should have the same basic qualities as an independent external
807 assessment body. More emphasis has to be set however, on the qualification of members since smart
808 surveillance systems typically require more specific, technical and contextual knowledge than is
809 needed for the evaluation of the deployment of surveillance systems in general.

810 -----

811 *Article 6*

812 *Domestic Measures related to the use of surveillance systems*

813 (1) *States shall provide that the use of surveillance systems will not continue:*

814 a. *before a human rights impact assessment is carried out by an independent*
815 *external assessment body with the objective of ensuring that privacy and other*

²⁷ Council of Europe, T-PD(2016)18rev, 19.08.2016.

816 *human rights are protected in accordance with the provisions of this instrument.*
817 *The human rights impact assessment body must be satisfied that, inter alia,*

- 818
- 819 *i. The use of the surveillance system is necessary and proportionate;*
 - 820 *ii. effective actions have been taken to minimise the risks on the enjoyment of*
821 *rights of persons while operating the surveillance system;*
 - 822 *iii. the surveillance system is designed and operated to comply with privacy by*
823 *design and privacy by default principles;*
 - 824 *iv. processes that reflect the operational needs are in place to inform the data*
825 *subject that his/her personal data is being kept;*
 - 826 *v. personal data collected during surveillance is not kept when no longer necessary*
827 *for the purposes for which it was collected, nor is it kept for longer than the time*
828 *allowed for by law;*
 - 829 *vi. personal data kept is accurate and current;*
 - 830 *vii. use of the personal data is for a lawful purpose under international human rights*
831 *law, and is necessary and proportionate to that purpose;*
 - 832 *viii. the sharing of the personal data with other authorities is carried out only as*
833 *permitted by law, limited to what is necessary and proportionate and in*
834 *compliance with international human rights law;*
 - 835 *ix. systems of redress for data subjects are in place;*
 - 836 *x. safeguards which protect privileged communications are in place;*
 - 837 *xi. adequate security means have been put in place to prevent illegal access to the*
838 *personal data, and to the algorithms of a smart surveillance system by*
839 *unauthorised persons or systems;*
 - 840 *xii. social and ethical costs of deploying the surveillance system have been*
841 *considered. Such costs must have been given due consideration and mitigation*
842 *measures be sought where appropriate.*
- 843
- 844 *b. unless the report of the annual human rights impact assessment is to be submitted*
845 *to the applicable competent authority, which can require additional measures to*
846 *be introduced for the continuation of the deployment and use of the surveillance*
847 *system.*

848 *(2) In the case of smart surveillance systems, States shall provide that the use of surveillance*
849 *systems will not continue unless annual testing of the system shows that the error rate is below*
850 *the threshold established for similar systems by a technical advisory body set up for this*
851 *purpose or submitted for human assessment in terms of Article 9.*

852 -----

853 The “*independent external assessment body*” mentioned in Par. 1 lit. a should have the same qualities
854 as mentioned in the commentary on Art. 5. States are free to choose whether this can be the same
855 body or not. However, members of the body must have formal independence and the substantial
856 knowledge required to carry out the assessment as well as the resources required to do so effectively.

857 Par. 1 lit. a x. refers to “*privileged communications*”. Such communications are to be defined by a
858 member states domestic law and have already been described in the explanatory memorandum to
859 Art. 5 par. 1 lit. a vii. These laws typically include lawyers, doctors and other professions which rely on
860 confidentiality between a client and the protected professional. Only communications falling outside
861 the privilege may be intercepted.

862 Referring to the communications between lawyers and their clients specifically, it is being added that
863 the right to a fair trial of any client is closely connected to the confidentiality of this type of
864 communication.

865 The “*technical advisory body*” mentioned in Par. 2 is similar as described in the commentary on Art. 5.
866 States are free to choose whether this can be the same body or not. However, members of the body
867 must have formal independence and the substantial knowledge (particular emphasis on this criteria)
868 required to carry out the assessment as well as the resources required to do so effectively.

869 -----

870 *Article 7*

871 *Domestic Measures related to the use of non-surveillance data*

872 (1) *States shall provide legislation identifying the conditions for any use of non-surveillance data*
873 *for the purposes of surveillance. This law should, inter alia, as appropriate:*

- 874 *a. identify the purposes and situations where non-surveillance data are to be used.*
- 875 *b. ensure that the data was originally produced for purposes compatible with the*
876 *purposes.*
- 877 *c. define the category of serious crimes and/or threats for which the non-surveillance*
878 *data are to be used.*
- 879 *d. ensure that the agency using the non-surveillance data should use data in cases where*
880 *reasonable suspicion exists that a serious crime may be committed or that a serious*
881 *threat may exist.*
- 882 *e. ensure that the agency carrying out the surveillance shall, unless it would not be*
883 *appropriate or feasible to do so and/or this would be prejudicial to the completion of*
884 *ongoing or future investigations or the prevention, detection or prosecution of a*
885 *specific criminal offence or adequate mitigation of threat, without undue delay [within*
886 *a period of time established by law] explain in writing the use of the non-surveillance*
887 *data in the particular situation to the person who was directly or indirectly subject to*
888 *such surveillance.*
- 889 *f. set the length of time information obtained from non-surveillance data should be kept.*
- 890 *g. set up an independent and adequately resourced oversight body to monitor that the*
891 *provisions of the law are followed.*

892 (2) *States shall provide that access by law enforcement agencies and security and intelligence*
893 *services to and use of non-surveillance data may not continue for surveillance purposes unless*
894 *an annual human rights impact assessment, including an assessment on proportionality and*
895 *necessity of the access and use of non-surveillance data is carried out by an independent*
896 *external assessment body and the assessment body is satisfied that, inter alia,*

- 897 *a. the risks on the enjoyment of rights of persons are in place regulating the way non-*
898 *surveillance data is accessed and used.*
- 899 *b. privacy enhancing technologies are being used and documented.*
- 900 *c. processes that reflect the operational needs, are in place to inform the data subject*
901 *that his/her personal data is being processed and stored.*
- 902 *d. non-surveillance data is not kept when no longer necessary for the purposes for which*
903 *it was collected or for the time allowed by law.*
- 904 *e. personal data kept is accurate and current.*
- 905 *f. use of the non-surveillance data follows the purposes permitted by law.*
- 906 *g. only proportional and necessary sharing of non-surveillance data with other agencies*
907 *is taking place or could take place and in all such cases only as provided for by law.*

- 947 (2) States shall provide that the authority carrying out the surveillance shall, unless an independent
948 authority has adjudicated that such notification constitutes an abuse of this provision or that
949 this would be prejudicial to the completion of ongoing or future investigations or the
950 prevention, detection or prosecution of a specific criminal offence or threat, without undue
951 delay [a period between four hours and seven days] explain in writing to the individual subject
952 of the surveillance, the use of the surveillance system in the particular situation.
- 953 (3) States shall provide that the explanation should
- 954 a. contain in clear and plain language meaningful information about the logic used in the
955 surveillance system and/or smart surveillance system;
 - 956 b. contain the reasons for which the individual has been subject to surveillance;
 - 957 c. mention the existence of the right to request from the data controller the rectification
958 or erasure of personal data concerning the data subject or to object to the processing
959 of such personal data;
 - 960 d. mention the right to lodge a request for human assessment referred to in Article 9 and
961 the details of the office responsible for processing the request.
- 962 (4) States shall provide appropriate safeguards where the person subjected to surveillance is a
963 minor. These safeguards may include that the parents or guardians of the minor are to be
964 informed on behalf of the minor and may exercise any rights in his/her name.
- 965 (5) Where, pursuant to par. 2, a State does not notify an individual, it must ensure that there is a
966 redress procedure in place to enable persons to contest surveillance without having to first
967 establish that they had been subject to a surveillance measure.
- 968 (6) If States have decided that monitoring by private entities falls under the definition on
969 surveillance for the purposes of this legal instrument, potential subjects of surveillance have
970 the right
- 971 a. to be informed when entering the area. A notification or sign must contain clear and
972 meaningful information about the logic used in the system;
 - 973 b. to know the reasons and legal basis upon which the individual is subject to surveillance;
 - 974 c. to be informed about the right to lodge a request for human assessment referred to in
975 Article 9 as well as about the details of the office responsible for processing the request.

976 -----

977 This article provides an individual right that any subject of surveillance is entitled to know that it has
978 been the target of governmental surveillance. It supports ‘a right to know’ of the individual unless an
979 independent authority (e.g., an independent judicial authority) has adjudicated pursuant to the rule of
980 law that disclosure would prejudice the operation of law enforcement. In some cases, there may be
981 an issue with notifying persons that they are under surveillance as this may lead to compromising an
982 investigation. A delay in disclosure may be needed to protect officers from harm or may be needed to
983 enable LEAs and/or SIS to establish the identities of other perpetrators.

984 The wording “specific” points to the fact that the potential harm must be tangible or relating to an
985 actual and known event which is likely to occur. Potential dangers, which cannot be linked to an
986 existing set of facts, are not sufficient to justify the delay of the notification.

987 As is outlined in par. 2 such a notification shall be phrased in a clear language, detailed (par. 3) and
988 delivered close to the actual event.

989 In par. 2 the phrase “that such notification constitutes an abuse of this provision” refers to potential
990 cases where such notifications will be abused to intentionally overburden the system or where persons
991 intentionally abuse this right to gain a better understanding of the strategic setup of state authorities

992 carrying out surveillance without being predominantly interested in a specific case which is the cause
993 for surveillance. However, it is crucial that such a decision is taken by an independent authority which
994 is not directly responsible for issuing the notification. Additionally, some countries issue notifications
995 to people who are not named in the order legitimizing surveillance, but if it is in the interests of justice.
996 This is a good practice for States to follow.

997 Par. 4 relates to the surveillance of minors who also have a right to be informed. This right, however
998 might be exercised through their parents or guardians.

999 Par. 5 relates to monitoring carried out according to Art. 2 par. 2. Persons who enter an area where
1000 they are likely to be subject of monitoring should be informed of that fact. They should be made aware
1001 of the surveillance system being employed (e.g. camera system). The information might also be backed
1002 up with symbols (camera icons or images, etc.). Usually, this will be done by installing signs in the area
1003 where surveillance is carried out. If smart technology is used to interpret the pictures this should also
1004 be indicated.

1005 Additionally, persons should be provided with reasons for having been subjected to surveillance.
1006 Typically, these reasons should be based on the domestic law. However, it is also useful to give
1007 additional explanations in plain language.

1008 Any operational activity, specifically when smart surveillance systems are employed, is subject to a
1009 human assessment process as lined out in Art. 9.

1010 -----

1011 *Article 9*

1012 *Right to Human assessment*

1013 *(1) States shall provide that an individual who alleges that the use of a surveillance system or non-*
1014 *surveillance data for surveillance purposes has led to, inter alia, unjustified:*

- 1015 *a. restrictions imposed while entering the territory of a State;*
- 1016 *b. restrictions on right of free movement and/or right to assembly and association;*
- 1017 *c. limitations or restrictions on other fundamental rights or freedoms;*
- 1018 *d. detention and/or arrest;*
- 1019 *e. placing on lists which are used to monitor persons and prevent them from exercising*
1020 *certain rights (black lists/watch lists);*
- 1021 *f. awarding of fines or penalties;*

1022 *has the right to request a human assessment by an officer appointed for this purpose.*

1023 *(2) States shall provide that the aim of the human assessment is to carry out an objective*
1024 *examination, by a person not initially involved in the surveillance or the effects of the*
1025 *surveillance, of the facts used in the decision-making process. States shall provide*

- 1026 *a. how the process of human assessment will take place;*
- 1027 *b. how the rights of the individual to be informed, to be heard, to remain silent, to engage*
1028 *legal counsel as well as other basic procedural rights will be protected;*
- 1029 *c. the legal effects of the outcome of the human assessment;*
- 1030 *d. the right to lodge a complaint to the Appeals Board referred to in Article 10;*
- 1031 *e. that a human assessment will be conducted without being prejudicial to the completion*
1032 *of an ongoing investigation or future investigation or the prevention, detection or*
1033 *prosecution of a specific criminal offence or threat.*

- 1034 (3) *The officer appointed for this purpose shall initiate the process of human assessment without*
1035 *undue delay [a period between four hours and seven days] from when such a request is made.*
- 1036 (4) *The officer appointed for carrying out the human assessment shall within a reasonable period*
1037 *[between four hours and seven days] examine the use of the surveillance systems and shall,*
1038 *unless an independent authority has adjudicated that a written explanation of the outcome of*
1039 *the human assessment would be prejudicial to the completion of an ongoing investigation or*
1040 *the prevention, detection or prosecution of a specific criminal offence or threat, without undue*
1041 *delay explain in writing the outcome of the human assessment carried out.*
- 1042 (5) *In cases where the officer comes to a beneficial conclusion for the individual concerned*
1043 *immediately, States restore the original condition effectively and promptly.*
- 1044 (6) *In cases where a decision is taken in accordance with par. 5 and restoration to original*
1045 *condition is impossible, States shall provide for adequate, prompt and effective compensation*
1046 *for the infringements suffered.*

1047 -----

1048 A Human assessment is not a Human Rights Impact assessment. The more there are automated means
1049 of assessment, the more there is a need for human analysis of the outcomes. Officers appointed for
1050 this purpose must be trained to understand the system and not to rely too much on its judgement. All
1051 of this must be ensured as part of the compliance process with this system. This human assessment
1052 may, in the jurisdictions where this is applicable, be likened to ‘merits review procedures’.

1053 The list in par. 1 has to be understood as being descriptive. It is possible that States decide to add a
1054 Human Rights Assessment for similar procedures.

1055 Par. 3 identifies the process which can be set in place for these safeguards to have effect. This par. also
1056 gives a suggestion of the time period within which the procedure should take place.

1057 Another time limit is mentioned in Par. 4. When deciding on the actual time limit it may be pertinent
1058 to consider practical considerations such as language needs. In border control cases, for example, the
1059 persons concerned may require translation or other types of language services as they do not speak
1060 the language of the country on whose border they are.

1061 Par. 5 demands a possibility to give the officer making a decision also the competence to restore the
1062 original and justified state (“restitutio in integrum”) with little administrative effort. Hence, an
1063 individual concerned will have a quick and effective remedy.

1064 Par. 6 obliges states to compensate in cases where the restoration of the original condition is
1065 impossible.

1066 -----

1067 *Article 10*

1068 *Right to appeal*

- 1069 (1) *States shall provide that the human assessment taken by the officer and the facts giving rise to*
1070 *the human assessment can be subject to appeal to an Appeals Board specifically set up to*
1071 *review the effects of the surveillance system or non-surveillance data. The Appeals Board is to*
1072 *call a hearing without undue delay [a period between four hours and seven days] from the*
1073 *moment the individual submits his/her request.*

- 1074 (2) States shall provide that as far as practicable, the Appeals Board will give its decision without
1075 undue delay [a period between seven days and three months] from the moment when the
1076 request was submitted.
- 1077 (3) States shall provide that the burden of proof lies on the controller of the personal data, who
1078 must prove that the surveillance system or non-surveillance data was used in accordance with
1079 laws, regulations, rules or procedures in force and in line with fundamental rights protection.
- 1080 (4) States shall provide that where the controller cannot without undue delay [a period between
1081 eight hours and one month] prove that the surveillance system or non-surveillance data was
1082 used in accordance with laws, regulations, rules and procedures in force and in line with
1083 fundamental rights protection, then the appeals board shall order:
- 1084 a. the reversal of the effects, as far as practicable.
 - 1085 b. compensations for any damages, including moral damages, suffered by the data
1086 subject.
 - 1087 c. the data held about the data subject upon whom the effect of the surveillance system
1088 was based to be rectified or deleted. The data controller responsible for carrying out
1089 the rectification or deletion is to carry out the decision forthwith and inform the
1090 individual in writing on the action that was taken.
 - 1091 d. if appropriate, the review of the deployment of a surveillance system or the non-
1092 surveillance data practices.
- 1093 (5) States shall provide that within 24 hours from the lodging of an appeal, the competent
1094 authority which has the authority over the processing of personal data by the controller shall
1095 be notified of the on-going appeal. The competent authority has the right to intervene in the
1096 proceedings.
- 1097 (6) States shall provide that appeals against the decision of the Appeals Board can be made to the
1098 competent court.
- 1099 (7) In cases where restoration to original condition is impossible, States shall provide for adequate,
1100 prompt and effective compensation for the infringements suffered.

1101 -----

1102 If the subject of surveillance is not satisfied with the outcome of the Human assessment an appeal
1103 might be made to an “Appeals Board specifically set up to review the effects of the surveillance system
1104 or non-surveillance data”. The appeal can be made regardless of the original result. However, the
1105 findings of the appeals board must not lead to a decision which is worse for the individual concerned
1106 than the one taken by the officer who did the human assessment (no “reformatio in peius”).

1107 Given that different jurisdictions have different Appeals Boards/Courts, it is up to each State to set up
1108 an Appeals Board in line with the legal culture and preferences in that State. However, the appeals
1109 board must be capable and resourced in a way that allows a fair trial.²⁹ The members of such a board
1110 must have the necessary training to understand the technological background of the surveillance
1111 system and the impact the produced data might have on the subjects of surveillance.

1112 This board will most likely be a quasi-judicial body consisting of experts (selected on criteria of
1113 qualification and seniority) on the surveillance system which is subject to review. The appeals board
1114 should consist of members from the state (LEAs and/or SIS community) and data protection specialists
1115 (academia and/or data protection officers).

1116 The size of the board and its composition depend on the surveillance technology that is being
1117 overseen. While the members of the board have to be free and independent in their individual decision

²⁹ For guidance on the notion of a fair trial see Council of Europe, Guide on Article 6 of the ECtHR via
http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf - accessed on 13.03.2017.

1118 making, they do not have to fulfil the same criteria of institutional independence as judges. However,
1119 the decisions of an appeals board must be based upon the existing legal framework which needs to be
1120 in accordance with international human rights standards, including the holding of fair hearings as part
1121 of the appeal process.

1122 The decision of the Appeals Board can be appealed against to the competent court.

1123 Compensation provided following par. 4 lit. b shall be adequate, prompt and effective. Restoration to
1124 original condition should be sought where possible.

1125 -----

1126 *Article 11*

1127 *Right to an effective remedy and independent assessment mechanism*

1128 *(1) Everyone whose rights and freedoms as set forth in this legal instrument are violated shall have*
1129 *an effective remedy before an authority notwithstanding that the violation has been*
1130 *committed by persons acting in an official capacity.*

1131 *(2) Any state which is party to this legal instrument can request an independent assessment of its*
1132 *own surveillance activities and institutions carrying out surveillance. This assessment will focus*
1133 *on compliance with the provisions of the legal instrument.*

1134 *a. This assessment is carried out by an independent body of internationally renowned and*
1135 *highly qualified experts with different professional backgrounds. The findings of the*
1136 *assessment are non-legally binding.*

1137 *b. The assessment is coordinated by the International Data Access Authority which is*
1138 *established in Article 16.*

1139 *c. The state which is requesting the assessment shall make any relevant information*
1140 *available to the experts. The state shall provide the resources necessary to carry out*
1141 *the assessment comprehensively, effectively and without any undue delay.*

1142 *d. Upon completion of the assessment a public report shall be issued which is presenting*
1143 *the main findings of the assessment as well as the recommendations made by the*
1144 *group of experts.*

1145 -----

1146 The wording of this art. par. 1 is inspired by Art. 13 of the European Convention of Human Rights.
1147 However, the Special Rapporteur on the right to privacy, Prof. Joseph Cannataci, also stressed the
1148 importance of “safeguards without borders and remedies across borders” in his first report to the UN
1149 Human Rights Council in March 2016.³⁰

1150 The term “everyone” at the start of this article makes clear that infringed rights do not depend on the
1151 citizenship of a person. For example, the European Convention of Human Rights rather uses the notion
1152 of controlled territory as reference point.³¹

1153 While effective remedies are typically guaranteed by national authorities, this must not necessarily be
1154 the case to fulfil this duty. Hence, also an international body could be setup for this purpose.

³⁰ United Nations, Report of the Special Rapporteur on the right to privacy to the Human Rights Council A/HRC/31/64, p.3.

³¹ Art. 1 ECHR states: “The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.”

1155 Par. 2 is containing a mechanism for an independent review of the surveillance system. This external
1156 assessment mechanism should facilitate for states to improve their surveillance mechanisms and at
1157 the same time increase public trust.

1158 -----

1159 *Article 12*

1160 *Surveillance system security*

1161 *(1) States shall provide that adequate safeguards are put in place to protect the data collected,*
1162 *retained, or processed by a surveillance system against risks violating its integrity,*
1163 *confidentiality, availability and resilience.*

1164 *(2) States shall provide that the controller shall be responsible for establishing an information*
1165 *security management system based on internationally accepted standards and based on a risk*
1166 *assessment conducted for the establishment of the information security management system*
1167 *for this purpose.*

1168 *(3) States shall provide that the controller shall be responsible for developing the communication*
1169 *infrastructure and databases in order to preserve the security of data, in compliance with a*
1170 *security policy established for this purpose.*

1171 *(4) States shall provide that the controller is responsible for defining authorization or security-*
1172 *clearance procedures for its staff for each level of data confidentiality.*

1173 *(5) States shall provide that the controller is responsible for notifying the relevant competent*
1174 *authority, without undue delay, when a data breach of a surveillance system has taken place.*
1175 *This notification must be provided in a manner not prejudicial to the completion of an ongoing*
1176 *investigation or the prevention, detection or prosecution of a specific criminal offence or threat.*

1177 -----

1178 This article relates to the technical aspects of system security for surveillance systems. States shall
1179 ensure that the systems are secure and in compliance with “*internationally accepted standards*” (par.
1180 2) which also includes that they are in accordance with the achieved state of technological knowledge,
1181 in other words that they are state of the art. For example, relevant ISO standards might be used for
1182 guidance.³²

1183 The security aspect does not include hardware and software considerations, but refers mainly to the
1184 challenges of proper management of these systems. Hence, there is a need for education and training
1185 of the staff involved in their operation (par. 4).

1186 -----

1187 *Article 13*

1188 *Supervision of users of surveillance systems*

1189 *(1) States shall provide that controllers regularly ensure that their users observe all the relevant*
1190 *legal rules related to the use of surveillance systems including those assuring the quality,*
1191 *accuracy and time limitation placed upon data.*

³² More information on the International Organization for Standardization (ISO) is at
<https://www.iso.org/standards.html> - accessed 27.10.2017.

- 1192 (2) States shall provide that the relevant competent authority has the power to supervise the
1193 activities of controllers of surveillance systems and can carry out spot checks and checks of
1194 processing incidents.
1195 (3) States shall provide that the controller shall take all necessary measures to correct or to ensure
1196 the correction of possible processing errors.
1197 (4) States shall provide that any abuse of a surveillance system by the user should be considered
1198 as an aggravated offence.

1199 -----

1200 This provision relates to the administrative supervision of surveillance systems. Authorities and entities
1201 involved in surveillance must make sure that there are internal procedures in place which ensure
1202 compliance with substantive legal provisions.

1203 In relation to par. 1 it must be assured that data is only accessed for a limited amount of time and only
1204 as long as necessary and proportionate to comply with the goal of this Art.

1205 States shall develop additional training standards in compliance with international reference
1206 frameworks. Limited access to data could be assured according to the Standard ISO/IEC 29115:2013,
1207 which provides a framework for managing entity authentication assurance in a given context.

1208 -----

1209 *Article 14*

1210 *Monitoring the use of surveillance systems*

- 1211 (1) States shall provide that the relevant competent authority may request from the controller any
1212 information on the use of each individual surveillance system being deployed by the controller.
1213 (2) States shall provide that a controller subject to such monitoring must provide the requested
1214 data.

1215 -----

1216 States should not only setup an internal compliance procedure but also ensure that there are checks
1217 and balances across the institutions of the State. Hence, the relevant competent authority has the
1218 obligation to setup a procedure which reviews the activities of SIS and LEAs.

1219 -----

1220 *Article 15*

1221 *Multi-Stakeholder Approach, and Collaboration*

- 1222 (1) States shall provide for shared learning, public policy engagement and other multi-stakeholder
1223 collaboration to advance the promotion and protection of fundamental rights and freedoms in
1224 the digital age in connection with surveillance.
1225 (2) In order to facilitate this process States shall support permanent fora for international dialogue
1226 to maintain and develop common standards, practices and technological safeguards relating
1227 to the protection of fundamental rights and fundamental freedoms in the digital age in
1228 connection with surveillance. This shall also include fora for exchange between state authorities
1229 carrying out surveillance and all stakeholder groups who shape the development of DTs.

1230 -----

1231 By signing up to this legal instrument States express their commitment to support Human Rights in the
1232 Digital Age. This means that they will not only refrain from certain behaviour, but that they will actively
1233 contribute to creating an environment which is beneficial for the development of individuality and
1234 personality through modern DTs. As a precondition for this, fundamental rights such as privacy and
1235 freedom of expression must not only be protected and respected, but also promoted.

1236 This can only be achieved by commitment to a regular and ongoing exchange with all members of the
1237 multi-stakeholder community who shapes events in the digital age.

1238 States are free to choose whether they will set up new or adapt existing fora to achieve these aims
1239 collectively. They may choose to do so as parties to this agreement or in other appropriate contexts.

1240 States are furthermore encouraged to consider involving members of oversight bodies created by this
1241 legal instrument in the multi-stakeholder exchange fora.

1242 -----

1243 *Article 16*

1244 *Mechanisms for transborder access to personal data*

1245 *(1) States shall establish an International Data Access Authority with the purpose of protecting*
1246 *personal data, privacy, freedom of expression and other fundamental human rights while*
1247 *facilitating the timely exchange of personal data across borders as may be required for the*
1248 *legitimate purposes of law enforcement agencies, intelligence and security services.*

1249 *(2) The International Data Access Authority (IDAA) shall be comprised of:*

- 1250 *a. The Surveillance Legal Instrument Consultative Committee (SCC),*
1251 *i. comprising of one member nominated by each contracting party;*
1252 *ii. which shall meet at least twice a year at the Headquarters of the International*
1253 *Data Access Authority;*
1254 *iii. monitor the workings of this legal instrument;*
1255 *iv. make recommendations as to the acceptance of new parties to the legal*
1256 *instrument;*
1257 *v. make recommendations on the interpretation and eventual amendment of the*
1258 *legal instrument.*

- 1259 *b. The International Data Access Commission (IDAC),*
1260 *i. comprising of a number of independent judges nominated by each of the*
1261 *contracting parties;*
1262 *ii. shall decide upon all requests for the granting of an International Data Access*
1263 *Warrant (IDAW) which may be submitted by law enforcement agencies,*
1264 *security or intelligence services of a contracting State;*
1265 *iii. When carrying out the function of par. 2 lit. b ii the IDAC shall decide in the*
1266 *following way,*

- 1267 *1. each request for an IDAW shall be heard by a panel of three judges*
1268 *each from separate jurisdictions one of whom should be a judge in the*
1269 *jurisdiction from where the request originated;*
1270 *2. Except for the judge from the jurisdiction originating a request, all*
1271 *judges on a panel will be assigned to adjudicate each request for an*
1272 *IDAW at the initial request stage, through automated random*
1273 *allocation;*

- 1274 3. *The Chair of the Panel should always be a judge from a jurisdiction*
1275 *other than that from the one where the request for the IDAW*
1276 *originated from;*
- 1277 4. *Where the request impacts more than three jurisdictions or where, in*
1278 *the opinion of the Panel Chair, the complexity of the case so merits,*
1279 *the Panel shall, at the request of the Panel Chair, be composed of five*
1280 *Judges each from different jurisdictions;*
- 1281 5. *All decisions of the Panel shall be taken by simple majority. Dissenting*
1282 *opinions may be recorded at the express wish of the dissenting Judge*
1283 *or Judges.*
- 1284 c. *The International Committee of Human Rights Defenders (ICHRD),*
- 1285 i. *compromising of eminent independent human rights experts, one from each*
1286 *contracting party or more pro rata if the workload so requires;*
- 1287 ii. *whose member experts (HRD) shall be nominated by contracting States and be*
1288 *able to demonstrate excellent knowledge in the fields of human rights*
1289 *including privacy, freedom of expression and freedom of association;*
- 1290 iii. *whose member experts (HRD) shall be assigned to monitor the proceedings*
1291 *followed by the International Data Access Commission and the International*
1292 *Data Access Tribunal where such proceedings are carried out in camera;*
- 1293 iv. *shall, once a year, after internal meetings and deliberations, present to the*
1294 *Consultative Committee a report on the number of cases monitored, the*
1295 *difficulties encountered in such cases and include in such annual report*
1296 *recommendations on bad practices to be avoided and best practices to be*
1297 *followed in the protection of human rights and the authorisation and carrying*
1298 *out of surveillance;*
- 1299 v. *A Human Rights Defender (HRD) will be assigned to monitor each request for*
1300 *an IDAW at the initial request stage,*
- 1301 1. *the selection of the HRD shall be based on automated random*
1302 *allocation;*
- 1303 2. *A HRD shall have the right of audience and to present arguments on*
1304 *behalf of but unknown to the data subject concerned, where it is felt*
1305 *that such surveillance requested is unnecessary, disproportionate or in*
1306 *any way breaches that individual's fundamental human rights.*
- 1307 d. *The International Data Access Tribunal (IDAT),*
- 1308 i. *comprising of a number of judges nominated by each of the contracting*
1309 *parties;*
- 1310 ii. *which shall decide upon any and all appeals resulting from the refusal of the*
1311 *International Data Access Commission to grant an IDAW;*
- 1312 iii. *an appeal may be submitted in exceptional circumstances, such as the*
1313 *availability of new evidence by law enforcement agencies, security or*
1314 *intelligence services of a contracting State;*
- 1315 iv. *each appeal shall be heard by a panel of five judges each from separate*
1316 *jurisdictions one of whom should be a judge in the jurisdiction from where the*
1317 *request originated;*
- 1318 v. *except for the judge from the jurisdiction originating a request, all judges on a*
1319 *panel of the IDAT will be assigned to adjudicate each request for an IDAW at*
1320 *the initial appeal stage, through automated random allocation;*

- 1321 vi. *the Chair of the Panel should always be a judge from a jurisdiction other than*
1322 *that from the one where the request for the IDAW originated from;*
1323 vii. *where the request impacts more than three jurisdictions or where, in the*
1324 *opinion of the Panel Chair, the complexity of the case so merits, the Panel shall,*
1325 *at the request of the Panel Chair, be composed of seven Judges each from*
1326 *different jurisdictions;*
1327 viii. *all decisions of the Panel shall be taken by simple majority. Dissenting opinions*
1328 *may be recorded at the express wish of the dissenting Judge or Judges.*
1329 e. *The International Data Access Authority Administration (IDAAA) which shall provide all*
1330 *the administrative, logistical and other support services required for the Authority to*
1331 *carry out its functions in a timely and efficient manner.*
1332 (3) *The International Data Access Authority (IDAA) shall model itself on best practices especially*
1333 *those utilised to deliver cost-effective dispute resolution in an on-line environment:*
1334 a. *Any and all proceedings of the IDAA may and should wherever possible and*
1335 *appropriate be carried out on-line.*
1336 b. *Proceedings carried out in person at the Headquarters of the IDAA will only be*
1337 *permissible in those exceptional instances where the Panel Chair obtains the explicit*
1338 *written permission from the Chair of the Surveillance Legal Instrument Consultative*
1339 *Committee.*
1340 c. *Secure video-conferencing and other communications facilities shall be provided by the*
1341 *IDAAA in order to enable the judges and Human Rights Defenders to carry out their*
1342 *duties.*
1343 (4) *The contracting parties to this legal instrument shall provide the adequate resources for the*
1344 *efficient working of the IDAA;*
1345 a. *Human Rights Defenders and Judges nominated by States shall, for the period of their*
1346 *service to the IDAA, be remunerated directly by the Authority under such terms and*
1347 *conditions to be established by the Consultative Committee.*
1348 b. *The financial contribution of each contracting State shall be determined by the*
1349 *Consultative Committee in accordance with the GDP, size of population and number of*
1350 *requests for IDAW originating from or directed to a particular State.*
1351 (5) *Any contracting State which does not make its financial contribution, or nominate its Judges,*
1352 *or Human Rights Defenders in a timely manner shall be automatically suspended from the*
1353 *membership and benefits of this legal framework for a period of two years from the due date*
1354 *of payment of contribution or nomination.*
1355 (6) *Any contracting State which carries out surveillance upon the activities of or otherwise*
1356 *attempts to interfere with the workings of the IDAA is automatically suspended from the*
1357 *membership and benefits of this legal framework for a period of five years from the discovery*
1358 *of such surveillance or interference.*
1359 (7) *Any State applying to become a party to this legal framework which carries out surveillance*
1360 *upon the activities of or otherwise attempts to interfere with the workings of the IDAA is hereby*
1361 *automatically determined to be ineligible for the membership and benefits of the legal*
1362 *framework for a period of five years from the discovery of such surveillance or interference.*

1363 -----

1364 This mechanism is intended to create an alternative to existing Mutual Legal Assistance Frameworks.
1365 When it comes in existence, it will not replace such existing mechanisms. It is at the discretion of states
1366 which framework they prefer in each individual case that requires the sharing of information.

1367 States and other stakeholders should work together to develop legal frameworks that (a) provide for
1368 governments' cross-border requests for user data between or among relevant regional or national
1369 governments, (b) respect the sovereignty and jurisdiction of each State, (c) adhere to the rule of law,
1370 and (d) protect human rights and public safety. Proposals for such legal frameworks have included bi-
1371 lateral and multilateral agreements. This provision outlines, for further multi-stakeholder discussions,
1372 one approach for such a legal framework.

1373 This Art. creates the cost-effective, privacy-friendly mechanisms which would enable States to request
1374 and receive access to personal data held in other States, but which could be important to the detection,
1375 investigation and prosecution of serious crimes including terrorism and organised crime. The creation
1376 of the International Data Access Authority (IDAA) created by this Art. would facilitate cross-border
1377 investigation and surveillance through the International Data Access Warrant (IDAW) contemplated
1378 earlier in this text. This would be complementary to mechanisms existing within States to grant
1379 authorisation for surveillance and would kick in at the request of the law enforcement agency or the
1380 security or intelligence service of a contracting party once it was clear that there is – as is now very
1381 often the case – a transborder, multiple jurisdiction dimension to the location where personal data
1382 may be held. The mechanism created by this legal instrument could notionally create a privacy-friendly
1383 one-stop shop for LEAs and SIS to apply for the IDAW which could greatly reduce costs and delays in
1384 data transfers at both the domestic and international levels. The request would be speedily dealt with
1385 by a panel of 3-5 judges in an on-line manner. Each request would be monitored and assured by an
1386 independent human rights defender, this measure partially inspired by the innovative practice
1387 introduced by the USA's FISA court.

1388 In a world where personal data is increasingly held by private companies in data centres which are
1389 established in accordance with rules dictated by technical and financial expediency, it would also
1390 become much simpler for a company to handle a request for personal data coming from a law
1391 enforcement or national security or intelligence agency located outside a particular jurisdiction: if the
1392 company is presented with an IDAW it can rest assured that such a warrant was issued in full protection
1393 of human rights and authorised by the law of the State where its data centres are located – which
1394 would presumably be a party to this legal instrument.

1395 The creation of such a mechanism would, if the IDAA is properly resourced and staffed, cut down
1396 waiting times for transfer of personal data required by law enforcement, prosecutors and intelligence
1397 services by weeks and often by an average of up to eleven months. With panels of judges working
1398 world-wide in a secure on-line manner, on a rota 24/7, urgent requests for access to personal data,
1399 whether in real-time or historical, for legitimate surveillance purposes could be handled quickly and
1400 efficiently.

1401 -----

1402 *Article 17*

1403 *Application to public and private entities*

1404 *(1) The controller and the processor shall be bound by the provisions of this instrument if the*
1405 *processing is carried out by a competent authority, any other public authority or body, or on*
1406 *behalf of or at the order of any of these public entities.*

1407 *(2) States may determine that monitoring by private entities using electronic means falls*
1408 *under the definition of surveillance in Art. 2 par. 1, if such monitoring is in place for the*
1409 *purposes of the prevention, detection, investigation and prosecution of crime and/or for*
1410 *increasing public safety and/or protecting State security.*

1411 *(3) In cases where a State decides to expand this legal instrument to monitoring by private*
1412 *entities in alignment with the definition Art. 16 par. 2, such entities shall be bound if the core*
1413 *activities of the controller or the processor consist of processing operations which, by virtue of*
1414 *their nature, their scope and/or their purposes, require regular and systematic monitoring of*
1415 *data subjects on a large scale.*

1416 *(4) If a State decides to make use of the option in Art. 16 par. 2 of this legal instrument, it*
1417 *shall notify the other parties of this legal instrument after signing and before domestic*
1418 *ratification of this legal instrument takes place.*

1419 -----

1420 This clause emphasizes the focus of the provisions of this legal instrument which is surveillance carried
1421 out through or on behalf of the government.

1422 Par. 2 provides an addition that States can opt-for when joining this agreement. It refers to monitoring
1423 by private entities that States might choose to regulate as ‘surveillance’. This includes but is not limited
1424 to Closed Circuit Television (CCTV), any class of sensors/actuators that are not smart (e.g. gunshot
1425 detector or the sound of glass cracking/breaking, etc.) as well as the collection of information
1426 emanating from portable telephones, or internet use.

1427 Such monitoring must only be included if the intent to carry it out is surveillance for “*the prevention,*
1428 *detection, investigation and prosecution of crime and/or for increasing public safety and/or protecting*
1429 *State security.*” Hence, such surveillance must have the same purpose as the surveillance activities
1430 described in par. 1. Additionally, it must be carried out on a scale that is meaningful to contribute to
1431 the four aims mentioned in par. 1 and par. 2.

1432 As an example, the contributors to this document have discussed the cooperation among private
1433 operators of CCTVs in shopping malls and their cooperation with law enforcement, in cases where the
1434 decision on how to de-escalate critical situations rests with the private operators. (In case of an
1435 incident they could ask themselves: “Should we call the police or leave the issue for the local security
1436 service or some special social workers who know the perpetrators better?” The choice of the action
1437 which is leading to resolving the situation quickly and most efficiently is left to the private entity
1438 carrying out the monitoring.)

1439 However, since the situation in certain States is different, parties to the legal instrument may choose
1440 on their behalf whether or not to extend the provisions of the legal instrument to these technologies
1441 and scenarios.

1442 However, as pointed out in par. 3, this is not true in all cases. That is why this legal instrument covers
1443 only private entities “*if the core activities of the controller or the processor consist of processing*
1444 *operations which, by virtue of their nature, their scope and/or their purposes, require regular and*
1445 *systematic monitoring of data subjects on a large scale.*” For example, a small shop which uses 5
1446 cameras to avoid shoplifting would not fall under this definition, while a large regional shopping mall
1447 or department store with a large number of cameras would.

1448 Par. 3 sets a timeframe for States on when to communicate their intention to apply this legal
1449 instrument, including to private CCTV operators.

1450 -----

1451 *Article 18*

1452 *Extended protection*

1453 (1) *None of the provisions of this legal instrument shall be interpreted as limiting or otherwise*
1454 *affecting the possibility for a State to grant persons a wider measure of protection than that*
1455 *stipulated in this text.*

1456
1457 (2) *None of the protections identified in this document are designed to limit or derogate from the*
1458 *rights provided by the United Nations Universal Declaration of Human Rights (particularly Art.*
1459 *12) and the United Nations International Convention on Civil and Political Rights (particularly*
1460 *Art. 17) or other international treaties a State has ratified that improve the level of protection*
1461 *of a data subject within the scope of this instrument.*

1462 -----

1463 This provision is a standard clause in Human Rights Law treaties and inspired by the wording of Article
1464 11 in the modernized version of Convention 108 of the Council of Europe.³³ It defines that the
1465 provisions in the legal instrument have to be understood as setting a minimum level and that States
1466 are free to improve standards of protection if they wish.

1467 The international agreements referred to in par. 2 are the Universal Declaration of Human Rights by
1468 the United Nations as proclaimed in Paris on 10 December 1948 (General Assembly resolution 217 A)
1469 and the United Nations International Covenant on Civil and Political Rights Adopted and opened for
1470 signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966,
1471 entry into force 23 March 1976. Other noteworthy international agreements and guidelines are for
1472 example, the Convention for the Protection of Individuals with regard to Automatic Processing of
1473 Personal Data (ETS No. 108) by the Council of Europe as well as the Convention on Cybercrime of the
1474 Council of Europe (CETS No.185), the revised Guidelines on the Protection of Privacy and Transborder
1475 Flows of Personal Data (2013) of the Organisation for Economic Cooperation and Development and
1476 Privacy Framework of the Asia-Pacific Economic Cooperation.

1477

³³ Cf. Consolidated version of the modernised convention 108 (September 2016) via
<https://rm.coe.int/16806a616c> – accessed on 28.07.2017, p. 5.

1478 III. Sources

1479

1480 - UN Legal Framework (particularly Art 12 and Art 19 of the Universal Declaration of Human
1481 Rights and Art 17 and Art 19 of the International Covenant on Civil and Political Rights).

1482 - Several UN resolutions (particularly resolution 68/167 of 18th of December 2013 on the right
1483 to privacy in the digital age as well as 28/16 of 24th of March 2015; a resolution of the Human
1484 Rights Council of 27th of June 2016 on the promotion, protection, and enjoyment of human
1485 rights on the internet, A/HRC/32/L.20; Resolution A/HRC/34/L.7/Rev.1 on the right to privacy
1486 in the digital age of 22nd March 2017).

1487 - Principles from <https://www.reformgovernmentsurveillance.com/> - accessed 13.12.2017.

1488 - GNI Principles: <https://globalnetworkinitiative.org/principles/index.php> - accessed
1489 13.12.2017.

1490 - International Principles on the Application of Human Rights to Communications Surveillance
1491 from <https://necessaryandproportionate.org/principles> - accessed 13.12.2017.

1492 - Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the
1493 protection of individuals with regard to automatic processing of personal data in the context
1494 of profiling:

1495 https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00 -
1496 accessed 13.12.2017.

1497 - [Modernization process of Convention 108 of the Council of Europe;](http://www.coe.int/en/web/data-protection/modernisation-convention108)
1498 <http://www.coe.int/en/web/data-protection/modernisation-convention108> - accessed
1499 13.12.2017.

1500 - Council of Europe, Recommendation CM/Rec(2016)5 of the Committee of Ministers to
1501 member States on Internet freedom.

1502 - EU Fundamental Rights Agency (FRA) report “Surveillance by intelligence services:
1503 fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal
1504 update”, via <http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega> -
1505 accessed 13.12.2017.

1506 - Several judgments of courts like the ECtHR, Roman Zakharov v. Russia, App. No. 47143/06;
1507 Szabo and Vissy v Hungary, App. No. 37138/14; CJEU, Tele 2 Sverige, C-203/15,
1508 ECLI:EU:C:2016:970.

1509 - RESPECT Toolkit.

1510 - Input from participants received in preparation and during the MAPPING meetings in Malta
1511 (June 2016, May 2017, February 2018), Miami (February 2017), New York (September 2016),
1512 Paris (September 2017), Rome (January 2018) and Washington D.C. (April 2016),

1513 - Written submissions received from various rounds of consultation with different members of
1514 the multi-stakeholder community.