COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 6 October 2022 T-PD(2022)5

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Modernised Convention 108 – Article 11 Guidance Document

Working Draft Legal Instrument on Government-Led Surveillance and Oversight

Modernised Convention 108 – Article 11 Guidance Document

Working Draft Legal Instrument on Government-Led Surveillance and Oversight

Including the Explanatory Memorandum

Version 0.4

PREFACE TO FIRST DRAFT PRESENTED FOR DISCUSSION BY THE T-PD in NOVEMBER 2022

When researching the best way to approach the creation of an interpretative document to Article 11 of Convention 108+, it was immediately clear that this provision is a wide-ranging one which is best tackled by dividing it into its main constituent elements:

i) the 'Protection of National Security';
ii) the 'Protection of National Defence';
iii) the 'Protection of Public Safety';
iv) the 'Protection of Important Economic and Financial Interests of the State';
v) the 'Impartiality and Independence of the Judiciary';
vi) the 'Prevention, Investigation and Prosecution of Criminal Offences and Execution of Criminal Penalties' (including information concerning various courts' proportionality assessment, and the retention of various forms of data);
vii) and 'Other Essential Objectives of General Public Interest'.

When contrasting the above with current legislative provisions both inside and outside Europe it was likewise clear that elements i-iii above could, in some circumstances, be usefully categorised together with element vi. and occasionally even iv. but less often with element (v). Additionally, element vii. is such a catch-all phrase that it is perhaps best dealt with separately at a later stage, benefitting from more desk research as well as discussions with and between contracting states and observers at the T-PD.

At the same time, it was apparent that the discussion is not altogether a new one and that the debate within the T-PD may benefit from consultations and research which have taken place in other fora notably over the last nine years since June 2013, when the first revelations by Edward Snowden started to achieve international impact. This document attempts to bring together the results of relevant consultations with key stakeholders in the sectors covered by elements i., ii., iii and vi. which were held by the Lead Expert both within and outside Europe during the period 2015-2022.

When discussing the matter with stakeholders within countries already signatory to Convention 108+ as well as those potentially ratifying the Convention over the coming 5-10 years to 2032, one functional requirement immediately emerged. Rather than vague and loose wording, contracting states would prefer to have something which would enable the government and other stakeholders to clearly visualise what it would mean, in concrete terms, for their country to have to do in order to claim compliance with Article 11. In order to achieve this aim, the Lead Expert appointed by the Council of Europe is hereby recommending to the T-PD that it undertake a preliminary exploration of the most appropriate format to achieve this aim. It is also recommended that this could take the form of a model law or of a Council of Europe Recommendation fleshing out the principles that would need to be included in a model

law which could complement or constitute a substantial part of any interpretative document pertinent to Article 11. Over the past four decades, the Council of Europe achieved notable success through the development of data protection safeguards through a sectoral approach. Thus, recommendations on medical data, insurance data, statistical data and social security data, to mention but a few of the sectors tackled, were produced in such a way that they provided the guidance necessary for each sector. Many CoE member states used these Recommendations as reference points when devising their own internal legislation about a specific subject. A Recommendation is a legal instrument which is flexible and capable of enabling organic growth within different member states where the extent of data processed for national security or defence or law enforcement could be hugely different to that of a neighbouring European state. At this very preliminary stage of the work on the best way to interpret and implement Article 11 of Convention 108+, the Lead Expert is offering the following text which could give the T-PD an idea of what a potential Recommendation could look like. In Council of Europe tradition, a Recommendation is normally set one step above that of a Model Law, outlining many of the principles in detail, but without tailoring the contents to the exact legal traditions of each member state. In the past, some EU member states have even transposed Recommendations (eg 1987 (15)) lock, stock and barrel into their substantive law.

In order to be of concrete practical use, the text contained in this draft legal instrument/Recommendation is largely focused on the privacy-intrusive activity most linked to elements i-iii and element vi. of Article 11 of Convention 108+ i.e. surveillance.

It will be up to the T-PD to decide, after the necessary discussion, as to whether a new Recommendation or a Model Law would be the most appropriate way to complement an interpretative document in best explaining to the world how Article 11 of Convention 108 should be understood. While the header very tentatively suggests a Recommendation format for the interim, the following draft uses the term “Legal Instrument” or abbreviation “LI” as a generic term since, given the preliminary nature of the work, it is not yet definitive what such a Legal Instrument could be, though a standard Council of Europe Recommendation would certainly qualify as one such legal instrument.

This draft Legal Instrument should not be read in isolation. It is designed to be compatible with and indeed to implement the spirit and the word of the most recent relevant jurisprudence[1] of the European Court of Human Rights, the European Court of Justice, leading case law from across Europe as well as the findings and recommendations of the UN’s Special Rapporteur on the right to Privacy.

[1] For more details see the document “Article 11 Convention 108+ - Compendium of Jurisprudence and Legislation” prepared by the teams from the University of Malta and the University of Groningen under the guidance of Prof. J. A. Cannataci.

Part I – Introduction

a. Background

States have long recognised the need to collect personal data from their citizens and residents. For an equally long time, the importance of the need to reconcile this collection of data with the protection of human rights and fundamental freedoms of individuals has also been recognised. As far back as 1981, the explanatory report for the original Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) notes the existence of a number of national legislations in Europe on the subject of general data protection.[2] Since that date, several advances have been made in both technology and the understanding of the nuances of a rules-based regime geared towards the protection of human rights and fundamental freedoms.

The original Convention was based on the twin principles of publicity ("the existence of automated data files should be publicly known") and control ("public supervisory authorities as well as the individuals directly concerned by the information can require that the rights and interests of those individuals are respected by the data users").[3] One of the driving needs for modernising the Convention, apart from these principles and the right to privacy, was the inclusion of the need to safeguard human dignity, "in order for individuals not to be treated as mere objects".[4]

Apart from these considerations, the Explanatory Report to the modernised convention identified three key aspects of the Convention that must be reinforced: "the general and technologically neutral nature of the Convention's provisions must be maintained; the Convention's coherence and compatibility with other legal frameworks must be preserved; and the Convention's open character, which gives it a unique potential as a universal standard, must be reaffirmed."[5]

One of the critical sections of Convention 108 revolves around the creation of exceptions and restrictions to the protections afforded by the Convention. At the same time, it was important to establish minimum safeguards for the protection of rights and freedoms of individuals even within those exceptions and restrictions. Encapsulated within Article 9 of the original Convention and Article 11 of the modernised Convention are provisions that allow a State to almost entirely bypass an individual's rights regarding their personal data, but only for specific purposes and with some major caveats. In the original Convention 108, States could utilise the exceptions in Article 9 to enact any measure by law that was deemed necessary for a democratic society. The modernised Convention, in line with rulings from the European Court of Human Rights, recognised the necessity to curtail the breadth of exceptions this language provided. Article 11 of the modernised Convention further restricts a State's power to ensure that such measures, apart from (i) being necessary in a democratic society, also (ii) respect the essence of the fundamental rights and freedoms and (iii) are proportionate to the legitimate aim being pursued – aims which cannot be achieved by less intrusive means.

Apart from reinforcing the test of necessity and explicitly introducing that of proportionality, Article 11 also adds language absent from Article 9 of the original Convention that ensures the creation of independent and effective oversight mechanisms, even when a State utilises the exceptions and restrictions provided by the Article 11 paragraph 3 when processing

[2] p. 2, Explanatory Report – ERS 108 – Automatic Processing of Personal Data (Convention)
[3] p. 3, Explanatory Report – ERS 108 – Automatic Processing of Personal Data (Convention)
[4] p. 2, Explanatory Report – ERS 108 – Automatic Processing of Personal Data (Convention)
[5] p. 1, Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)

personal data for national security and defence purposes.[6] This was because of the expansion of another exception created under Article 11 paragraph 3 which allows States to create exceptions to certain clauses when processing activities for national security and defense purposes dealing with the review of a law for effectiveness (Article 4 paragraph 3), on transborder data flows (Article 14 paragraphs 5 and 6) and the creation of supervisory authorities (Article 15, paragraph 2, litterae a, b, c and d). This makes it even more important to keep in mind that the same paragraph reinforces the need for safeguards by ensuring that such exceptions are provided by law and may be deployed only to the extent that they constitute a necessary and proportionate measure in a democratic society to fulfil such an aim.

Several smaller, but no less impactful, changes were also made to the specific purposes for which States could utilise the exceptions and restrictions under Article 11: (a) the original wording of "State security" was expanded to national security and defense; (b) "monetary interests" was expanded to "important economic and financial interests" of the State; (c) a new purposes of the protection of "the impartiality and independence of the judiciary" was added; (d) "suppression of criminal offences" was changed to "the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties"; and finally (e) a catch-all purpose of "other essential objectives of general public interest" was added.

In sum, the language of Article 11 is complex and carries multiple interpretations, while also making reference to broader principles present throughout Convention 108. When read within the context of a Convention that is technologically neutral, works well with other legal frameworks, and has an open character, it is easy to see why States may have difficulty putting the Convention into practice in national law. Especially given the open nature of Convention 108 which aspires to be a universal standard, and the delicate subject matters of national security, public safety and defense, the bedrock upon which a nation's autonomy is founded, the need for a model law or a recommendation outlining detailed principles on which a model law can be based, cannot be understated.

The drafters of this legal instrument (LI) posit that the protection of human rights and fundamental freedoms of individuals, along with human dignity, within the context of the State's processing of personal data for purposes including national security and defense, must be outlined in a more detailed and comprehensive manner. Convention 108, and specifically Article 11, have shown that it is possible for democratic nations to agree to curtail their own broad surveillance powers in a rules-based framework that protects human rights and fundamental freedoms. The need for a universal standard continues to grow as countries around the world continue to grapple with protecting human rights and ensuring public health and safety, particularly when fighting global threats such as the COVID-19 pandemic.

The most privacy-intrusive measure pertinent to data protection law undertaken by all states in pursuit of many of the main exceptions outlined in Article 11 is that of surveillance. This draft legal instrument therefore focuses on measures relevant to surveillance and another key principle established by Article 11 i.e. that of independent oversight. The provisions are developed thanks to extensive consultations with stakeholders over the period 2013-2022 in the light of evolving case-law at both the European and national level.

[6] Article 11 paragraph 3, Convention 108+

b. Methodology

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

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

This draft has been developed with a strong focus on substance and irrespective of any particular institutional or legislative framework. This draft draws substantively on sources developed through stakeholder consultations co-organised by the EU-funded MAPPING project (Grant Agreement No.612345) and the UN Special Rapporteur on the Right to Privacy (SRP) during the period 2015-2018. Further consultations held and observations made by the UN SRP until July 2021 were then reviewed and relevant provisions integrated into this September 2022 version of this draft legal instrument in the light of the evidence base contained in the document designated Article 11 Convention 108+ - Compendium of Jurisprudence and Legislation.

Part II – Text, Context and Commentary

Preamble

(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.*

(2) *The right to private and family life, as enshrined in Art. 8 of the European Convention on Human Rights and amplified further by the various cases decided by the European Court of Human Rights has, since 1981, been specifically protected in the field of digital data by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) as revised and modified by the Protocol Council of Europe Treaty Series - No. 223.*

(3) *All human rights are rooted in human dignity as also recognised by Article 1 of the European Charter of Fundamental Rights. 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 or regulations.*

(4) *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.[7] Only if all these criteria are met, a necessary measure is proportionate and can therefore be taken.*

(5) *Many international and regional systems of law explicitly lay down that in order to restrict, limit, or interfere with an individual's enjoyment of the right to privacy a measure, which shall be subjected to independent prior authorization and targeted by nature, must*
a. be provided for by a law,
b. pursue a legitimate aim,
c. be necessary and proportionate to the pursued aim
d. while providing appropriate safeguards specified within the law.
e. Furthermore, surveillance activities should be authorized by an independent judiciary or authority whose activities are governed by the rule of law and
f. overseen by at least one legitimate body.

(6) *Recognizing that privacy online is essential for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of*

[7] This last step could also be described as a "cost-benefit" analysis.

peaceful assembly and association, the States which sign this legal instrument declare the following:

EXPLANATORY NOTE TO PREAMBLE

Convention 108 has always had a global vocation, a key characteristic further entrenched in Convention 108+. It was always intended to be open for signature to all member states of the United Nations (UN). Thus, it is both fortunate and important that Article 11 of Convention 108+ is demonstrably 100% compatible with legal principles embraced globally and especially within the context of global institutions such as the UN. The preamble therefore mainly refers to wording that was developed by the United Nations (UN) following the resolution on the Right to Privacy in the Digital Age which also established the mandate of the Special Rapporteur on the Right tp Privacy (SRP).[8] It particularly reflects language which can be found in a resolution of the UN Human Rights Council of 27th of June 2016 on the promotion, protection, and enjoyment of human rights on the internet.[9]

Paragraph 2 refers specifically to Art. 8 of the European Convention of Human Rights which broadly covers the same scope and intent of Art 12 of the UN's 1948 Declaration of Human Rights and Art. 17 of the 1966 International Covenant on Civil and Political Rights.

Paragraph (par.) 3 contains a commitment to a holistic approach to human rights which are rooted in human dignity. Ultimately, the entirety of human rights should result in the protection, respect and promotion of human dignity. This is important when considering privacy and other human rights relating to personal development, the right to live in security and the rights of victims of a crime. It is an opportunity to introduce the term dignity into the discourse of the Council of Europe, emulating the example set by the European Charter of Fundamental Rights and thus filling a lacuna still present in the ECHR which does not explicitly mention dignity unlike most other international legal instruments purporting to protect human rights.

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

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

Par. 5 also adds the requirement in lit. c for any limitation of a right to be necessary and proportionate. This reflects the explicit inclusion of proportionality by Art. 11 of Convention 108+ which had been previously absent in Art. 9 of Convention 108.Here, as everywhere in this text those terms should be understood in the following way: Necessity is referring to the specific end or purpose ("telos") of a measure. Necessity should be prescribed by law which itself must be the result of a legitimate legislative process. Typically, necessity is a purpose that is legitimate in a society which is based on values such as human rights, rule of law and democracy.

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

[9] United Nations, Human Rights Council, A/HRC/32/L.20.

To learn further about regional examples mentioned in par.5 one can consult the case of the European Court of Human Rights (ECtHR) in the case of Zakharov vs. Russia.[10] Particularly, the notions of the abstract nature of surveillance and the requirement of the foreseeability of surveillance have been discussed.[11] Another regional example to be considered is the judgment of the Court of Justice of the European Union (CJEU) in the joined cases C-203/15 and C-698/15 Tele 2 Sverige and Watson.[12]

Further cases that should be considered from the Inter-American System of Human Rights are Donoso v. Panama and Escher et al. v. Brazil.[13] This section and others may be further substantiated using European cases cited in the "evidence-base document" Compendium of Jurisprudence and Legislation.

Article 1

Subject matter and objectives

(1) The subject matter of this legal instrument is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy where exceptions to data protection law permit surveillance through digital technology.

(2) The purpose of this legal instrument is to establish the independent and effective review and supervision of the processing of personal data through digital technology for those purposes recognised by Article 11 of Convention 108+. Through independent and effective supervision, this legal instrument aims to safeguard the rights and fundamental freedoms of persons with regard to the use of personal data for the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties and other essential objectives of general public interest.

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

(4) *In accordance with this legal instrument and without exception, the processing of personal data for those purposes specified in Art 1 (2) above, should be provided for by law, respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society.*

---

[10] 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.

[11] Ibidem.

[12] CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970,

[13] 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.

EXPLANATORY NOTE TO ARTICLE 1

The formulation "legal instrument" (LI) is an interim one and is capable of being substituted by the term "Recommendation", "Act", "Regulation", "Law" or "Directive" depending on the binding force that parties may wish to accord the instrument. It is intended that the LI is capable of being used in part or in whole by Member States party to Convention 108+ or indeed by other States that wish to adopt the set of principles enshrined in Article 11 of Convention 108+ as a model for their domestic law. This objective is being proposed for the Council of Europe since it is consistent with the MAPPING project's finding that, when it came to surveillance through digital technologies, there was no discernible difference between the concerns of stakeholders inside Europe and of those outside Europe. The concerns were as universal as the right to privacy set out in Art 12 UDHR/Art 17 ICCPR, Art 8 of the European Convention on Human Rights and Art 7/8 of the EU Charter of Fundamental Rights as well as similar provisions laid down in equally relevant regional protection mechanisms such as Art 11 of the American Convention on Human Rights.

Article (Art.) 1 defines the subject matter of this legal instrument. It addresses surveillance carried out by using or manipulating digital technologies. Such activities are carried out by States on their behalf or at their order. While most of these activities will be carried out online using the Internet, it is also possible that other electronic technologies are being used. The LI is not aiming at covering conventional surveillance in the physical world (i.e. one person physically observing another unaided by technology), but surveillance using or facilitated by digital technologies and typically over the Internet. It tries to provide an answer to the issues raised in instances such as the revelations of Edward Snowden, the blocking of Internet services by governments with little or no justifiable arguments, and the questions that arise while studying cases such as Apple vs the FBI.[14] However, not only direct efforts of States to gather information electronically are covered. Information received from other States or data repurposed from parties in other countries beyond their jurisdiction are subject to this text, too. Furthermore, the LI is drafted to tackle these challenges from a perspective which has international human rights protection and human dignity at its centre.

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

Par. 3 should not be read as balancing security against privacy or any other fundamental human right. In the view of the drafters it is necessary that fundamental human rights are promoted in a comprehensive manner. Rather than a trade-off between rights, ways should be sought to strengthen them collectively and to ultimately promote human dignity. Hence, it is necessary to provide both privacy and security rather than the one or the other.

Article 2

Definitions

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

[14] 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.

(1) “personal data” means any information relating to an identified or identifiable individual (“data subject”);
(2) “data processing” means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data, in particular for the purpose of surveillance;
(3) “data processing” means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria, in particular for the purpose of surveillance;
(4) “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;
(5) “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
(6) [“person” describes any natural individual with the capability to have rights or duties, particularly including data subjects.]
(7) “surveillance” is any monitoring or observation of persons, including their conversations or other activities, or any other collection of personal data for the purposes of protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties and other essential objectives of general public interest.
(8) “surveillance system” refers to any organised means or resources designed or intended to be used for surveillance.
(9) “surveillance data” is data that is acquired, retained, analysed, shared or otherwise used for surveillance. This includes data gathered as a result of acts by a State or on its behalf or at its order without the use of a dedicated surveillance system.
(10) “non-surveillance data” is data the primary purpose for the creation or collection of which is not surveillance, but which could be searched or interrogated because the data contained therein may, through either pattern recognition or applied search methods, yield personal data which is used for surveillance.
(11) “competent authority” means:
(a) any public authority competent for the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security, defense, or public safety; or
(b) any other body or entity entrusted by State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security, defense, or public safety;
(12) [“national security”] includes, *inter alia*, the protection of state security and constitution democracy from, *inter alia*, espionage, terrorism, support for terrorism and separatism.
(13) [“defence”]
(14) [“public safety”]
(15) [“important economic and financial interests of the State”] covers, *inter alia*, tax collection requirements and exchange control.
(16) [“general public interest”] covers, *inter alia*, public health including preparations for and measures taken during pandemics as well as the prevention, investigation,

detection and prosecution of breaches of ethics for regulated professions and the enforcement of civil law claims.

EXPLANATORY NOTE TO ARTICLE 2

The definition in par. 1 (personal data), par. 2 and 3 (data processing), par. 4 (controller), and par. 5 (processor) are the same as in Article 2 of the modernised Convention 108.

While Par. 6 currently refers exclusively to natural persons, it may be amended if the definition of "person" is to be based on the choice of including legal entities within the definition similar to the definition of "processor" and "recipient" under the modernised Convention 108, or excluding legal entities based on the approach taken by the General Data Protection Regulation of the European Union.[15] This is because it is possible that legal persons (like corporations) are entitled to fundamental rights like privacy or similar rights in different States. Since the situation differs from State to State and because of different legal traditions in different states it is left to them to decide whether they choose to extend protection to legal persons or not.

Par. 7 defines surveillance as an act of government or entities which act on behalf of the government. The term "surveillance" includes all forms of bulk acquisition of personal data,[16] all forms of "mass surveillance" and targeted surveillance. This sentence is also intended to cover all those instances where the surveillance activity is carried out by non-state actors acting on behalf of or at the order of any form of state authority.

Surveillance is only acceptable if it is based on reasonable suspicion.[17] However, reasonable suspicion is not a standard that is defined in international law outside Europe. When deciding

[15] EU, Official Journal L 119/33, 04.05.2016

[16] 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.

[17] 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 […]."

whether reasonable suspicion exists, it is necessary to demonstrate that the specific anticipated surveillance will yield evidence of a serious crime or help mitigate the threat.

Most of the time surveillance might be carried out through the collection and processing of data as referred to in par. 9 (*'surveillance data' is data the primary purpose for the creation of which is surveillance and/or non-surveillance data actually being used for surveillance).*

Nevertheless, the LI also refers to data which was originally collected for other purposes and is being re-used for surveillance as defined in par. 9. In such cases data, which was originally non-surveillance data, also becomes surveillance data according to par. 10. The main characteristic to distinguish surveillance and non-surveillance data is the original purpose for the creation of the data.

Both, the definition of surveillance data in par. 9 and non-surveillance data in par. 10 include not only the actual content of conversations, messages, activities etc., but also metadata generated about it.

The definition of par. 11 (competent authority) is based on the definition of Art. 3(7) of the Directive (EU) 2016/680[18] aligned with the wording provided in the modernised Convention 108.

The definition of par. 12 (national security), para. 15 (important economic and financial interests of the State) and par. 16 (general public interest) are based on the Explanatory Report to the modernised Convention 108.

Article 3

Basic requirements for surveillance

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

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

(3) Any law regulating surveillance shall limit the purposes to:

- *a. the prevention, investigation, detection or prosecution of criminal offences;*
- *b. public safety;*
- *c. protecting national security;*
- *d. defense;*
- *e. important economic and financial interests of the State;*
- *f. the impartiality and independence of the judiciary; or*
- *g. other essential objectives of general public interest.*

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

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

[18] EU, Official Journal L 119/89, 04.05.2016

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

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

- *a. Legislative oversight on a regular basis and at least quarterly, by a Committee of the regional or national elected legislative body responsible for the entity funding and tasked for the purpose by law, of the budgetary and operational performance of all LEAs, SIS and PMEs authorized by law to carry out surveillance, both domestic and foreign, with the authority to temporarily or permanently withhold, suspend, grant or cancel the funding of any surveillance program or activity;*
- *b. A Pre-Authorisation authority, completely independent from the entity and the executive or legislative branches of government, composed of one or more members with the security of tenure of, or equivalent to, that of a permanent judge which is tasked by law to evaluate ex-ante requests from and grant permission to LEAs, SIS and PMEs as shall be required under law prior to the conduct of lawful surveillance;*
- *c. An Operational Oversight authority, completely independent from the entity, the Pre-Authorisation Authority and the executive or legislative branches of government, composed of one or more members with the security of tenure of, or equivalent to, that of a permanent judge which is tasked by law to exercise ex-post oversight over and exercise accountability of LEAs, SIS and PMEs as shall be required under law especially for the conduct of lawful surveillance;*
- *d. Inter-institutional whistle-blower mechanisms that allow for anonymity of the whistle-blower(s), protection from retaliation and include extra-authoritarian or extra-institutional review of the process including remedies;*
- *e. Wherever practical and possible, providing, at public expense, an independent advocate/defender of the rights of the person subjected to a surveillance system, who would be able to defend and promote the right to privacy of such person in front of the Pre-Authorisation and Operational Oversight Authorities while that person would not be aware of having been placed under surveillance;*
- *f. except as may be otherwise provided for by law in the interests of operational integrity, the presentation and publication of reports, at minimum on an annual basis, by the Legislative, Pre-Authorisation and Operational Oversight Authorities*

(8) Any LEA, SIS or PME carrying out surveillance must be explicitly authorized to do so and regulated by a specific law defining the

- *a. exact Purposes.*
- *b. tasks.*
- *c. objectives.*
- *d. activities.*
- *e. basic administrative functions and setup.*

(9) Any surveillance activity must only be carried out for concretely defined specific and legitimate purpose and in response to a concrete and legitimate need. Except in those cases where it concerns serving foreign military personnel, serving foreign LEA, SIS or PME officers, all surveillance, domestic and foreign, shall be carried out only provided that a relative warrant is obtained ex-ante from the regional or national pre-authorisation agency in the case of persons or data located within the regional or

national jurisdiction or provided that a valid legal request is obtained ex-ante under a legal framework for cross-border requests that includes the relevant regional or national government authorities recognized as being competent for the task..

(10) When any form of warrant for surveillance is requested, the only criteria that may be taken into account is that of reasonable suspicion. The race, colour, gender, language, religion, political or other opinion, national or social origin, citizenship, property, birth or other status of the suspect cannot be advanced or accepted as being adequate or relevant grounds for the issue of any form of surveillance warrant.

(11) Any law authorising surveillance must include intelligible, accessible and effective procedural remedies for persons whose rights may have been violated.

(12) The budget of any entity carrying out surveillance must be defined clearly and subject to review on the executive, political and judicial level, albeit when necessary and appropriate the review process may be carried out in camera.

EXPLANATORY NOTE TO ARTICLE 3

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

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

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

A specific law is also required to regulate activities for PMEs. For example, the ECtHR made clear that the State cannot absolve itself from responsibility by delegating its obligations to private bodies or persons.[19]

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

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

The specific law provides increased legitimacy for surveillance activities. It enables a better understanding for the need to carry out surveillance. Additionally, it becomes more likely that the general scope of activities is subject to a broad discussion while details regarding individual operations must not necessarily be disclosed. Such a law should also be containing

[19] ECtHR, Wos v Poland, App.No. 22860/02, 01.03.2005.

which kind of information is being collected and which authorities can access the data under which circumstances. Additionally, it should be laid down how the data is being managed once it has lost relevance.

According to par. 3 the specific law supports States in their efforts to maintain the basic order of a society. The purposes of surveillance are therefore limited to the three mentioned in lit. a – g. These purposes are based on Article 11 of the modernised Convention 108. It is important that the definition of surveillance in Art. 2 is considered together with the legitimate purposes in this paragraph.

The terms necessity and proportionality as well as the criteria to establish them have already been discussed and described in the explanatory memorandum of the preamble. They may be further expanded, should members of the T-PD deem it desirable, using examples from the case law outlined in the "Compendium of Jurisprudence and Legislation".

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

Those LEAs, SIS or PMEs which carry out surveillance should only do so in an environment with adequate safeguards including a system of checks and balances. This system (par. 7) consists of regular and effective legislative oversight (lit. a), an independent pre-authorisation authority (ex-ante oversight, lit. b), an independent operational oversight authority (ex-post oversight including accountability of LEAs, SIS and PMEs, lit. c), inter-institutional whistle-blower mechanisms (lit. d). On the latter, there are situations where internal channels will not be effective at calling attention to systemic tolerance of wrongdoing, and public disclosure should be either protected, or at least potentially defensible.[20] Following the best practices noted in the Swedish system and parts of the US system, provision is made in lit. e) for an independent defender of the person who is the target of surveillance especially when such a person is understandably not aware that he or she is being subjected to surveillance by the state. The presentation and publication of separate reports compiled by the legislative oversight, independent pre-authorisation and independent operation oversight authority (lit. f). These measures are supposed to reinforce each other and are a complete system. In the understanding of the drafters of this document, oversight is not a finished product. Rather it is constant work in progress.

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

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

[20] 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.

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

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

Article 4

General Principles

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

(1) States shall provide that surveillance systems shall be authorised by law prior to their use. This law shall:

a. identify the purposes and situations where the surveillance system is to be used.

b. define the category of serious crimes or threats for which the surveillance system is to be used.

c. state that the agency using the surveillance system should only use the system in cases where a reasonable suspicion exists that a serious crime may be committed or a genuine threat to security exists;

d. define and provide the least intrusive measures which potentially might be suitable to achieving the aim.

e. demand from the authority to justify that each single measure envisaged is necessary and proportionate for the obtaining of vital intelligence in an individual operation as well as considering the overall impact of this and such measures on the right to privacy of persons irrespective of whether this is a citizen or resident of that state.[21]

f. provide that any final decision on enacting the surveillance system shall be subjected to independent prior authorization before actual surveillance takes place.

g. provide that the deliberate monitoring of an individual's behaviour or other information by the State should only be targeted surveillance carried out on the basis of reasonable suspicion.

[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

h. *provide that the individual concerned is likely to have committed a serious crime or is likely to be about to commit a serious crime. Such domestic law shall establish that an independent authority, having all the attributes of permanent independent judicial standing, and operating from outside the law enforcement agency or security or intelligence agency concerned, shall have the competence to authorise targeted surveillance using specified means for a period of time limited to what is appropriate to the case.*[22]

i. *state that the authority carrying out the surveillance shall, unless an independent authority has adjudicated that it would not be appropriate or feasible to do so or this would be prejudicial to the completion of ongoing or future investigations or the prevention, detection or prosecution of a specific criminal offence or threat, without undue delay [within a period of time established by law] explain in writing the use of the surveillance system in the particular situation to any person who was directly or indirectly subject to such surveillance.*

j. *set the length of time information obtained from the surveillance system should be kept and by whom it may be accessed at each stage as well as requirements for permanent deletion or destruction upon the expiration of the relevant period.*

k. *set up an independent surveillance oversight authority to monitor the conduct of surveillance and ensure that the provisions of the law are followed.*

l. *provide for an individual right to redress for subjects of surveillance.*

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

a. *Publicly available, periodic reports allowing for a substantive and comprehensive review of the activities of relevant agencies to other State entities such as the legislative branch and/or the judicial branch of a State.*

b. *Publicly available transparency reports by the State itself in respect to all requests made to corporations and other non-state actors with regard to the provision of personal data including categories, and frequency.*

c. *Provide for transparency regarding surveillance law regulations and the power of agencies who carry out surveillance.*

d. *Setting up of a documented, regular and ongoing process of dialogue with civil society and academia and other stakeholders on the purpose and design of surveillance systems and the use of non-surveillance data for surveillance purposes.*

e. *Support and encouragement of publicly available transparency reports by corporations and other non-State entities which provide personal data if the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. States must not prohibit corporations from publishing transparency reports.*

(3) When considering the use of surveillance systems, as well as the use of non-surveillance data for surveillance purposes, States should respect and protect the free flow of information and the stability of information and communication technologies and

[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."

services. Particularly, States are prohibited from directly or indirectly ordering or compelling

a. *service providers in their jurisdiction to disconnect, shut down access or otherwise broadly disrupt or block flows of information.*
    i. *States shall respect the secrecy of telecommunications in accordance with both their own laws and the laws of the State of the originator of such correspondence, applying whichever has the stronger privacy protections.*
    ii. *If in an individual case a State agency has reasonable suspicion that a particular service was set up and/or is being used substantively for an illegal purpose a service provider may be required to deny that service on the presentation of a legal request issued pursuant to applicable laws in accordance with the rule of law. Any such limitation must be necessary and proportionate as well as strictly limited to the extent of such illegal use.*
    iii. *States shall issue publicly available annual reports on such individual cases describing the frequency and extent of the interruption.*
b. *service and hardware providers to take measures which negatively impact the security – including the security of technologies such as encryption – of digital services or products.*
c. *that actions are taken which require data localization.*
d. *that agency carrying out an investigation and seek to use information held by private entities give false, misleading or incomplete explanations of the reason for their request or the legal authority for their making it.*
e. *a lowering of standards through legislative or other measures of the protection of privileged communications and records of privileged communications.*

(4) *When setting up and operating surveillance systems, as well as while using non-surveillance data for surveillance purposes, States shall*

a. *not assert extra-territorially jurisdiction over data or persons in contravention of relevant treaties and principles of international mutual legal assistance.*
b. *seek to establish appropriate bilateral and/or multilateral international legal frameworks to facilitate cross-border requests for data in a manner that adheres to the rule of law and is consistent with international human rights law.*

(5) *If States share intelligence*

a. *such activities shall be subject to an oversight regime equivalent to and as effective as described in Art. 3 par. 7.*
b. *they are required to ensure that oversight authorities have access to any relevant information necessary to evaluate the legality, necessity and proportionality of the sharing and the agreements that form the basis of such activities.*
c. *they shall empower oversight authorities to review decisions and/or undertake independent investigations concerning the activities.*
d. *they shall ensure that this information is only shared with states that have equivalent, effective and adequate mechanisms in place to guarantee similar standards and safeguards.*

.

EXPLANATORY NOTE TO ARTICLE 4

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

The phrase in par. 1 "*authorised by law"* should be interpreted with reference to the categories laid down in European Court of Human Rights (ECtHR) judgment in the case of Roman Zakharov vs. Russia.[23] Particularly, authorised by law means that there is an actual request for surveillance, a certain level of suspicion (e.g. reasonable suspicion), impartial and effective oversight of the activities, authorization by judicial warrants and no bulk collection of information. The latter principle of no bulk collection has since been very strongly entrenched in European law by the decision of the European Court of Justice in Sverige2 and Watson of 21 December 2016.[24]

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

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

Targeted surveillance is only acceptable if is based on reasonable suspicion as mentioned in par.1 lit. c.[25] However, reasonable suspicion is not a standard that is sufficiently defined in international law except possibly outside European Law. When deciding about whether reasonable suspicion exists, it is necessary to demonstrate that the specific anticipated surveillance will yield evidence of a crime or help mitigate the threat.

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

In par. 1 lit. j a time limit is mentioned. Here, as well as in the rest of this legal instrument, time limits are set in square brackets as an indication of urgency of a procedure. However, each time limit may have to be amended to address the special circumstance and criminal procedural law in the respective State. The time limits need to fit the operational and managerial practices of a State. Nevertheless, time in most of the procedures covered by this

[23] ECtHR, App. No. 47143/06, Zakharov vs. Russia, via http://hudoc.echr.coe.int/eng?i=001-159324 – accessed on 22.09.2016. This 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.

[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 […]."

legal instrument is of the essence. Large delays in action may result to delays in justice and hence reduced effectiveness of safeguards ("Justice delayed is justice denied.")

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

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

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

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

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

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

Par. 3 lit. b refers to the need to guarantee the security of information products and services. States are banned from trying to weaken the development of security standards by requiring developers and/or engineers to intentionally weaken the implementation of protective technologies. This specifically prohibits states from banning any forms of encryption, requiring a service provider to maintain keys or the ability to decrypt data, and requiring a service provider to weaken encryption. It also prohibits states from requiring that a service provider

[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.

create so-called "backdoors" and/or any other technological measures designed to circumvent security measures that are intended to protect the users of the service.

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

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

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

Par. 4 makes it clear that States should not try to impose territorial restrictions through regulatory measures when technologies are cross-border in nature. States should not try to get access to data not stored on their territory by putting persons under pressure because they or their offices are physically located on their territory. In general, States should aim at establishing an international framework of cooperation in those cases where law enforcement or information gathering is needed in a cross-border scenario. This framework should be based on human rights principles and should allow for technology to develop its full potential.

Par. 5 addresses the issue of intelligence sharing between countries. At the time of drafting this LI this seemed to be an increasingly relevant activity to protect public order and safety and to protect the rights of victims of crime. Hence, it should be ensured that the same standards and principles are relevant for cross-border surveillance as for national surveillance activities.[27]

[27] „In 2016, 2017 and 2018, the oversight bodies of Belgium, Denmark, Norway, Switzerland and the Netherlands shared experiences obtained from their own national investigations into this topic, which resulted in a more in-depth understanding and a more complete overview of the international cooperation between intelligence and security services. The five oversight bodies established the risk of an 'oversight gap' because the oversight of international cooperation is still national in nature. In a joint statement the oversight bodies therefore called on national legislators to lower the main obstacle to cooperation, which is the secrecy regarding the activities of intelligence and security services in this area.

The five oversight bodies will continue to cooperate closely with each other, sharing best practices in oversight and discussing the current topics that affect each of them.

In 2019, the British Investigatory Powers Commissioner's Office (IPCO) joined the cooperative partnership. The meetings of this partnership are aimed at discussing current legal and technical issues that are relevant to each of the participating oversight bodies and at sharing best practices in oversight. The priority in this area is improvement of each body's oversight methods.

In December 2019, six oversight bodies signed a so-called charter, that consolidates the cooperation under the name Intelligence Oversight Working Group" abstracted from https://english.ctivd.nl/about-ctivd/international-cooperation last accessed on 19th September 2022

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

Article 5

Domestic Measures related to the deployment of surveillance systems

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

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

i. necessity and proportionality of the surveillance system;

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

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

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

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

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

vii. safeguards in place to protect privileged communications.

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

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

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

(2) For existing surveillance systems, a human rights impact assessment which fulfils and is equivalent to the requirements for new surveillance systems as laid down in par. 1 of this provision has to be finalized no later than 24 months after the introduction of the measures outlined in this Article.

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

EXPLANATORY NOTE TO ARTICLE 5

This article refers to states and the measures they need to take if they want to carry out surveillance activities when introducing new surveillance systems.

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

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

Par. 1 lit. a iii could include measures relating to the use and development of data mining algorithms. Such activities should be subject to regular assessments of the likely impact of the data processing on the rights and fundamental freedoms of data subjects. The basic structure of the analysis should be based on predefined risk indicators which have been clearly identified in advance. The relevance of individual results of such automatic assessments should be carefully examined on a case-by-case basis, by a person in a non-automated manner.[28]

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

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

Whereas Par. 1 deploys safeguards for the introduction of new systems, Para 2 introduces safeguards for systems already in place at the time of adoption of new domestic legislation introducing safeguards in compliance with this legal instrument. This provision needs to be read together with Article 6 below. It may possibly also be deleted if its objectives are reached through the existence of Article 6 alone.

Par. 3 may require more clarification following further discussion in keeping with the understanding of the term judicial warrant by different European states.

[28] Council of Europe, T-PD(2016)18rev, 19.08.2016.

Article 6

Domestic Measures related to the use of surveillance systems

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

a. before a human rights impact assessment is carried out by an independent external assessment body with the objective of ensuring that privacy and other human rights are protected in accordance with the provisions of this instrument. The human rights impact assessment body must be satisfied that, inter alia,

i. The use of the surveillance system is necessary and proportionate;
ii. effective actions have been taken to minimise the risks on the enjoyment of rights of persons while operating the surveillance system;
iii. the surveillance system is designed and operated to comply with privacy by design and privacy by default principles;
iv. processes that reflect the operational needs are in place to inform the data subject that his/her personal data is being kept;
v. personal data collected during surveillance is not kept when no longer necessary for the purposes for which it was collected, nor is it kept for longer than the time allowed for by law;
vi. personal data kept is accurate and current;
vii. use of the personal data is for a lawful purpose under international human rights law, and is necessary and proportionate to that purpose;
viii. the sharing of the personal data with other authorities is carried out only as permitted by law, limited to what is necessary and proportionate and in compliance with international human rights law;
ix. systems of redress for data subjects are in place;
x. safeguards which protect privileged communications are in place;
xi. adequate security means have been put in place to prevent illegal access to the personal data, and to the algorithms of a smart surveillance system by unauthorised persons or systems;
xii. social and ethical costs of deploying the surveillance system have been considered. Such costs must have been given due consideration and mitigation measures be sought where appropriate.

b. unless the report of the annual human rights impact assessment is to be submitted to the applicable competent authority, which can require additional measures to be introduced for the continuation of the deployment and use of the surveillance system.

(2) In the case of smart surveillance systems, States shall provide that the use of surveillance systems will not continue unless annual testing of the system shows that the error rate is below the threshold established for similar systems by a technical

advisory body set up for this purpose or submitted for human assessment in terms of Article 9.

EXPLANATORY NOTE TO ARTICLE 6

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

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

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

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

Article 7

Domestic Measures related to the use of non-surveillance data

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

- *a. identify the purposes and situations where non-surveillance data are to be used.*
- *b. ensure that the data was originally produced for purposes compatible with the purposes.*
- *c. define the category of serious crimes and/or threats for which the non-surveillance data are to be used.*
- *d. ensure that the agency using the non-surveillance data should use data in cases where reasonable suspicion exists that a serious crime may be committed or that a serious threat may exist.*
- *e. ensure that the agency carrying out the surveillance shall, unless it would not be appropriate or feasible to do so and/or this would be prejudicial to the completion of ongoing or future investigations or the prevention, detection or prosecution of a specific criminal offence or adequate mitigation of threat,*

without undue delay [within a period of time established by law] explain in writing the use of the non-surveillance data in the particular situation to the person who was directly or indirectly subject to such surveillance.

f. set the length of time information obtained from non-surveillance data should be kept.

g. set up an independent and adequately resourced oversight body to monitor that the provisions of the law are followed.

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

a. the risks on the enjoyment of rights of persons are in place regulating the way non-surveillance data is accessed and used.

b. privacy enhancing technologies are being used and documented.

c. processes that reflect the operational needs, are in place to inform the data subject that his/her personal data is being processed and stored.

d. non-surveillance data is not kept when no longer necessary for the purposes for which it was collected or for the time allowed by law.

e. personal data kept is accurate and current.

f. use of the non-surveillance data follows the purposes permitted by law.

g. only proportional and necessary sharing of non-surveillance data with other agencies is taking place or could take place and in all such cases only as provided for by law.

h. systems of redress for any person whose rights may be harmed are in place.

i. adequate security means have been put in place to prevent illegal or unauthorized access to the non-surveillance data.

j. social and ethical costs of using the non-surveillance data are being given due consideration and mitigation measures sought.

(3) The report of the annual human rights impact assessment of par. 2 is to be submitted to the applicable competent authority, which can ask for additional measures to be introduced for the continuation of the deployment and use of non-surveillance data.

(4) *States shall provide that access or use of non-surveillance data must not have the effect of singling out persons on the basis of race, colour, gender, language, religion, political or other opinion, national or social origin, citizenship, property, birth or other status, data concerning health or data concerning a natural person's sexual activity or gender the controller shall implement effective protection to minimize impact and introduce adequate safeguards in accordance with the achieved state of technological knowledge as well as additionally requiring, where appropriate, judicial authorisation.*

EXPLANATORY NOTE TO ARTICLE 7

This Art. clarifies that there must be a specific law in place in a State that allows for the request of such information from private entities. States should provide adequate resources to ensure that LEA and SIS are educated and remain informed about the current state of technology and potential impacts on human rights.

Allowing authorities to always ask for information should not become a standard routine. While, LEAs and SIS are, potentially, interested in proving that they have not missed out on anything in the course of an investigation, the request for information should always be based

on a standard consistent with international laws and norms (including international human rights laws and norms -e.g., reasonable suspicion).

Targeted surveillance is only acceptable if is based on reasonable suspicion.[29] However, reasonable suspicion is not a standard that is sufficiently defined in international law. When deciding about whether reasonable suspicion exists, it is necessary to demonstrate that the specific anticipated surveillance will yield evidence of a crime or help mitigate the threat against public safety.

The "*independent external assessment body"* mentioned in par. 2 should have the same basic qualities as mentioned in the commentary on Art. 5. States are free to choose whether this can be the same body or not. However, members of the body must have formal independence and the substantial knowledge required to carry out the assessment as well as the resources required to do so effectively.

Article 8

Right to notification

(1) States shall provide that where a surveillance system or non-surveillance data is used for surveillance purposes, the individual subject of the surveillance, whether directly or incidentally, has a right to notification.

(2) States shall provide that the authority carrying out the surveillance shall, unless an independent authority has adjudicated that such notification constitutes an abuse of this provision or that this would be prejudicial to the completion of ongoing or future investigations or the prevention, detection or prosecution of a specific criminal offence or threat, without undue delay [a period between four hours and seven days] explain in writing to the individual subject of the surveillance, the use of the surveillance system in the particular situation.

(3) States shall provide that the explanation should

- *a. contain in clear and plain language meaningful information about the logic used in the surveillance system and/or smart surveillance system;*
- *b. contain the reasons for which the individual has been subject to surveillance;*
- *c. mention the existence of the right to request from the data controller the rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;*
- *d. mention the right to lodge a request for human assessment referred to in Article 9 and the details of the office responsible for processing the request.*

(4) States shall provide appropriate safeguards where the person subjected to surveillance is a minor. These safeguards may include that the parents or guardians of the minor are to be informed on behalf of the minor and may exercise any rights in his/her name.

(5) Where, pursuant to par. 2, a State does not notify an individual, it must ensure that there is a redress procedure in place to enable persons to contest surveillance without having to first establish that they had been subject to a surveillance measure.

[29] CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970, „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 […]."

(6) If States have decided that monitoring by private entities falls under the definition on surveillance for the purposes of this legal instrument, potential subjects of surveillance have the right

a. to be informed when entering the area. A notification or sign must contain clear and meaningful information about the logic used in the system;

b. to know the reasons and legal basis upon which the individual is subject to surveillance;

c. to be informed about the right to lodge a request for human assessment referred to in Article 9 as well as about the details of the office responsible for processing the request.

EXPLANATORY NOTE TO ARTICLE 8

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

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

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

In par. 2 the phrase "*that such notification constitutes an abuse of this provision"* refers to potential cases where such notifications will be abused to intentionally overburden the system or where persons intentionally abuse this right to gain a better understanding of the strategic setup of state authorities carrying out surveillance without being predominantly interested in a specific case which is the cause for surveillance. However, it is crucial that such a decision is taken by an independent authority which is not directly responsible for issuing the notification. Additionally, some countries issue notifications to people who are not named in the order legitimizing surveillance, but if it is in the interests of justice. This is a good practice for States to follow.

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

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

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

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

Article 9

Right to Human assessment

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

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

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

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

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

(3) The officer appointed for this purpose shall initiate the process of human assessment without undue delay [a period between four hours and seven days] from when such a request is made.

(4) The officer appointed for carrying out the human assessment shall within a reasonable period [between four hours and seven days] examine the use of the surveillance systems and shall, unless an independent authority has adjudicated that a written explanation of the outcome of the human assessment would be prejudicial to the completion of an ongoing investigation or the prevention, detection or prosecution of a specific criminal offence or threat, without undue delay explain in writing the outcome of the human assessment carried out.

(5) In cases where the officer comes to a beneficial conclusion for the individual concerned immediately, States restore the original condition effectively and promptly.

(6) *In cases where a decision is taken in accordance with par. 5 and* restoration to original condition is *impossible*, States shall provide for adequate, prompt and effective compensation for the infringements suffered.

EXPLANATORY NOTE TO ARTICLE 9

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

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

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

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

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

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

Article 10

Right to appeal

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

(2) States shall provide that as far as practicable, the Appeals Board will give its decision without undue delay [a period between seven days and three months] from the moment when the request was submitted.

(3) States shall provide that the burden of proof lies on the controller of the personal data, who must prove that the surveillance system or non-surveillance data was used in accordance with laws, regulations, rules or procedures in force and in line with fundamental rights protection.

(4) States shall provide that where the controller cannot without undue delay [a period between eight hours and one month] prove that the surveillance system or non-surveillance data was used in accordance with laws, regulations, rules and procedures

in force and in line with fundamental rights protection, then the appeals board shall order:

a. *the reversal of the effects, as far as practicable.*
b. *compensations for any damages, including moral damages, suffered by the data subject.*
c. *the data held about the data subject upon whom the effect of the surveillance system was based to be rectified or deleted. The data controller responsible for carrying out the rectification or deletion is to carry out the decision forthwith and inform the individual in writing on the action that was taken.*
d. *if appropriate, the review of the deployment of a surveillance system or the non-surveillance data practices.*

(5) States shall provide that within 24 hours from the lodging of an appeal, the competent authority which has the authority over the processing of personal data by the controller shall be notified of the on-going appeal. The competent authority has the right to intervene in the proceedings.

(6) States shall provide that appeals against the decision of the Appeals Board can be made to the competent court.

(7) In cases where restoration to original condition is impossible, States shall provide for adequate, prompt and effective compensation for the infringements suffered.

EXPLANATORY NOTE TO ARTICLE 10

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

Given that, different jurisdictions have different Appeals Boards/Courts, it is up to each State to set up an Appeals Board in line with the legal culture and preferences in that State. However, the appeals board must be capable and resourced in a way that allows a fair trial.[30] The members of such a board must have the necessary training to understand the technological background of the surveillance system and the impact the produced data might have on the subjects of surveillance.

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

The size of the board and its composition depend on the surveillance technology that is being overseen. While the members of the board have to be free and independent in their individual decision making, they do not have to fulfil the same criteria of institutional independence as judges. However, the decisions of an appeals board must be based upon the existing legal framework which needs to be in accordance with international human rights standards, including the holding of fair hearings as part of the appeal process.

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

[30] 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.

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

Article 11

Right to an effective remedy and independent assessment mechanism

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

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

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

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

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

EXPLANATORY NOTE TO ARTICLE 11

The wording of this art. par. 1 is inspired by Art. 13 of the European Convention of Human Rights. Moreover, the UN Special Rapporteur on the right to privacy, also stressed the importance of "safeguards without borders and remedies across borders" in his first report to the UN Human Rights Council in March 2016.[31]

The term "everyone" at the start of this article makes clear that infringed rights do not depend on the citizenship of a person. For example, the European Convention of Human Rights rather uses the notion of controlled territory as reference point.[32] This is also in the spirit of the decision by the German Constitutional Court

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

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

Article 12

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

[32] 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."

Surveillance system security

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

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

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

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

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

EXPLANATORY NOTE TO ARTICLE 12

This article relates to the technical aspects of system security for surveillance systems. States shall ensure that the systems are secure and in compliance with *"internationally accepted standards"* (par. 2) which also includes that they are in accordance with the achieved state of technological knowledge, in other words that they are state of the art. For example, relevant ISO standards might be used for guidance.[33]

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

Article 13

Supervision of users of surveillance systems

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

(2) States shall provide that the relevant competent authority has the power to supervise the activities of controllers of surveillance systems and can carry out spot checks and checks of processing incidents.

(3) States shall provide that the controller shall take all necessary measures to correct or to ensure the correction of possible processing errors.

(4) States shall provide that any abuse of a surveillance system by the user should be considered as an aggravated offence.

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

EXPLANATORY NOTE TO ARTICLE 13

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

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

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

Article 14

Monitoring the use of surveillance systems

(1) States shall provide that the relevant competent authority may request from the controller any information on the use of each individual surveillance system being deployed by the controller.

(2) States shall provide that a controller subject to such monitoring must provide the requested data.

EXPLANATORY NOTE TO ARTICLE 14

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

Article 15

Multi-Stakeholder Approach, and Collaboration

(1) States shall provide for shared learning, public policy engagement and other multi-stakeholder collaboration to advance the promotion and protection of fundamental rights and freedoms in the digital age in connection with surveillance.

(2) In order to facilitate this process States shall support permanent fora for international dialogue to maintain and develop common standards, practices and technological safeguards relating to the protection of fundamental rights and fundamental freedoms in the digital age in connection with surveillance. This shall also include fora for exchange between state authorities carrying out surveillance and all stakeholder groups who shape the development of DTs.

EXPLANATORY NOTE TO ARTICLE 15

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

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

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

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

Article 16

Application to public and private entities

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

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

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

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

EXPLANATORY NOTE TO ARTICLE 16

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

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

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

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

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

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

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

Further discussion is required as to the feasibility of extending this provision to all the purposes listed in Art. 11 of Convention 108