

Council of Europe Convention 108+ and oversight on national security

Review Committee on the Intelligence and Security Services (CTIVD)

Investigatory Powers Commission (TIB)

The Hague, February 2021.

[‘Convention 108+’](#) is the modernized version of the existing Council of Europe Convention 108 (Convention for the protection of individuals with regard to automatic processing of personal data) ETS No. 108. See:). An important addition to the amended Convention with respect to the current version is that data collection and its processing within the domain of national security (and defence) can no longer be exempted from the scope of application of the Convention. This was previously possible under Article 3.2a of the Convention. As stated in the Explanatory Report to Convention 108+, the Convention also codifies the rich body of case-law of the European Court of Human Rights (ECtHR).

The process to ratify the Protocol CETS No. 223 amending the Convention that will result in the entry into force of Convention 108+ has now been initiated or is already ongoing in several signatory countries (to date, 33 signatures and 10 ratifications out of the 55 Parties to Convention 108). The new Convention could enter into force and thus become binding as early as October 2023.

Convention 108+ has several implications for oversight in the context of national security. A number of observations in this respect are specified below. This memo is not intended to exhaustively consider all relevant aspects of the Convention for oversight related to national security, but it

attempts to create further awareness of the relevance of the Convention to regulating and oversight of the intelligence and security services.¹

It should be noted that although the Convention sets new minimum standards, states Parties are free and should be encouraged to set higher norms.

1. Scope of Convention 108+

Convention 108+ is fully applicable to the national security domain. This means that national security regulations must be checked article by article against the Convention to establish whether existing national security regulations are consistent with Convention 108+. This not only applies to the area of oversight but also to the requirements (principles and rules) in the Convention that apply to the collection and processing of personal data.

The Convention takes a conceptual/holistic approach when it refers to ‘national security and defence’. National legislative frameworks do not always take that approach and sometimes exclude certain areas, for example limiting the scope of oversight to certain intelligence and security organizations or to domestic activities or national citizens). However, Convention 108+ does not allow that type of exclusion. When implemented nationally, the entire security domain must therefore be included, i.e. it must be all-inclusive. That means that when appointing the oversight body/supervisory authority (i.e. Article 11.3, 15, and 16(2) of the Convention), it must be clear that the entire national security domain falls under the responsibility of the oversight body or bodies to be appointed.

2. Limited exceptions and restrictions

Article 11 of Convention 108+ (Exceptions and restrictions) regulates the authorized (lawful) exceptions and restrictions to a limited number of provisions of the Convention (specified in article

¹ The CTIVD and TIB are grateful for the helpful comments they received on the draft versions of this memo, including those made by the secretariat of the Council of Europe and the members of the CTIVD-knowledge network.

11, paragraph 1 and 3) notably to the rights of individuals (data subjects), but also to the international transfers of data, the set-up and investigatory powers of oversight.

The exceptions and restrictions further specified and limited in this Article are only permitted when they are in accordance with the requirements referred to in that article. This means that when implementing Convention 108+, each specific exception and restriction must be provided for by law, must respect the essence of the fundamental rights and freedoms and must justify that it ‘constitutes a necessary and proportionate measure in a democratic society’ for one of the legitimate grounds listed in Article 11. This assessment is provided for in the case law of the European Court of Human Rights (ECtHR) that lays the burden of proof with the State/legislator.

A full assessment of an exception of restriction along the above mentioned lines is therefore by no means optional and in this assessment, the existing normative framework must also be taken into account. That framework can be found for example in the ECtHR’s case law, which must be considered to have been incorporated in the Convention (see, e.g., the ECtHR [factsheet of the on Mass surveillance](#)).

For EU member states, it is also important that both the General Data Protection Regulation (GDPR, 2016/679) and the Police Directive (2016/680) incorporated standards for data collection and data processing, as well as standards for oversight. The same applies to the European Court of Justice’ case law. Recent case law uses the strengthened term ‘strictly necessary’ where it concerns the necessity requirement (see: [ECLI:EU:C:2020:790](#) [*Privacy international*] and [ECLI:EU:C:2020:791](#) [*La Quadrature du Net*]).

3. Role and competence of independent and effective oversight

Convention 108+ pays particular attention to oversight in the context of national security when formulating the exceptions and restrictions. Based on Article 11(3), exceptions and restrictions concerning oversight are only permitted in regard to Articles 4(3), 14(5) and (6), and 15 (2)(a)-(d). That means that the aforementioned necessity and proportionality assessments also apply in a strict/narrow sense to these provisions. Furthermore, exceptions and restrictions may never affect the independence and effectiveness of the oversight as prescribed by Article 11.3: ‘This is without

prejudice to the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party'. Relevant ECtHR case law on independent and effective oversight includes cases such as [\[ECLI:CE:ECHR:2015:1204JUD004714306\]](#) [*Roman Zakharov v. Russia*] and [\[ECLI:CE:ECHR:2016:0112JUD003713814\]](#) [*Szabó and Vissy v. Hungary*].

Article 15(2)(a) lays down that the oversight 'shall have powers of investigation and intervention'. Effective review and supervision implies binding powers where the impact on the fundamental rights is the greatest, particularly in the accessing, analysis and storage phases of processing personal data. Binding powers must deal with the restriction/termination of data processing including data minimisation/deletion. In this respect it should be noted that these oversight powers are also required under the current EU standards in the GDPR and Police Directive. From the perspective of protecting the rule of law as effectively as possible, the lack of binding powers within the domain of national security is incompatible with the criterion that this 'constitutes a necessary and proportionate measure in a democratic society'. In principle the same applies to the other elements of Article 15.2 where restrictions are allowed (under b to d).

Convention 108+ does not allow exceptions where it concerns the other elements of Article 15, namely littera e of paragraph 2 [awareness raising duties], paragraph 3 [consultation on legislative and administrative measures, paragraph 4 [requests and complaints by individuals], paragraph 5 [independence and impartiality], paragraph 6 [necessary resources for effective performance of tasks], paragraph 7 [periodic reporting], paragraph 8 [confidentiality], paragraph 9 [possibility of appeal], and paragraph 10 [no power regarding bodies when acting in their juridical capacity].

4. Transborder flows of personal data

Chapter III/Article 14 looks in greater detail at the transborder flows of personal data. As general restrictions and exceptions are not allowed, this Article also applies in full to the security domain.

This provision has at least two implications for oversight. Firstly, Article 14(5) imposes on the state Parties an obligation to require that data controllers provide to the oversight body all relevant information concerning the transfer of personal data referred to in paragraph 3.b and, upon request,

paragraphs 4.b and 4.c. The information obligation relates to virtually all personal data transfers. Secondly, Paragraph 6 further stipulates that the reasons for the transborder exchange of data must be substantiated. This includes the obligation to allow the oversight body the power to prohibit or suspend the exchange of data, or subject it to conditions.

Article 14 is one of the articles that allows for exceptions or restrictions. This follows from Article 11 in conjunction with Article 15(2)(b). Any exception and restriction must therefore meet the same requirements regarding proportionality and necessity.

5. Co-operation in oversight

The Convention stipulates in Article 17 that oversight bodies must cooperate with one another 'to the extent necessary for the performance of their duties and exercise of their powers'. Article 17 is not one of the articles that allows exception or restrictions.

The Article refers in particular to forms of cooperation: mutual assistance [sub a], coordinating investigations and interventions, and conducting joint actions [sub b] and providing information and documentation on their law and administrative practice relating to data protection [sub c]. Within the context of this cooperation no personal data can be exchanged, unless this is essential to that cooperation or when the individuals involved have granted authorization (explicit, specific, free and informed consent). Finally, paragraph 3 of the Article provides for the setting up of a network of oversight bodies. This obligation mainly falls on the oversight bodies. The State parties will in this case - as applies in principle to all other aspects of the Convention - have to create the conditions which enable this so that this obligation can be implemented.