Convention 108+, the GDPR and Data Processing in the National Security Domain

Jansen, R.H.T.; Reijneveld, M.D.

2022, Article / Letter to editor (European Data Protection Law Review, 8, 3, (2022), pp. 423-430)

Doi link to publisher: https://doi.org/10.21552/edpl/2022/3/14

Council of Europe

Convention 108+, the GDPR, and Data Processing in the National Security Domain

*Rowin Jansen and Minke Reijneveld**

I. Introduction

The legal order of the Council of Europe (CoE) is increasingly influencing the national security domain. This development is likely soon to receive an additional boost. On 10 October 2018, the Protocol amending the Convention for the Protection of Individuals with regard to Processing of Personal Data came into being.[1] This protocol, also known as 'Convention 108+', is the modernised and strengthened version of the existing Council of Europe Data Protection Convention 1981, also known as Convention 108.[2] Its entry into force is scheduled for October 10th 2023.[3] Close to 40 countries have already signed Convention 108+. These include both EU-Member States and non-EU states.[4] The European Union (EU) as a body is not a party to the Data Protection Convention yet, but there are plans for this accession to Convention 108+ in the near future.[5] In the meantime, the EU Member States – all already party to the Data Protection Convention (DPC) – are authorised to accede to it. The European Commission is actively encouraging EU Member States to ratify Convention 108+ as soon as possible.[6]

Convention 108+ contains principles and rules for the processing of personal data, standards regarding oversight mechanisms, and standards on the international transfer of data. The level of convergence with EU-instruments such as the General Data Protection Regulation (GDPR) and the Law Enforcement Directive is high. This implies that the implementation of Convention 108+ will have almost no impact on the European Union legal order, given that all Member States are subjected to the GDPR and most have adopted national legislation implementing the GDPR.[7]

However, there are certain areas where Convention 108+ can have an impact also on the EU legal order. An important difference between the GDPR and Convention 108+ is the scope of application. The GDPR in principle does not apply to data processing in the national security and intelligence domain, since the EU has no competence in this area accord-

DOI: 10.21552/edpl/2022/3/14

* Rowin Jansen, PhD candidate, Research Centre for State and Law & Interdisciplinary Hub for Digitalization and Society, Radboud University; for correspondence: <rowin.jansen@ru.nl>. Minke Reijneveld, PhD candidate, Radboud Business Law Institute & Interdisciplinary Hub for Digitalization and Society, Radboud University; for correspondence: <minke.reijneveld@ru.nl>.

1 See for a first overview Jörg Ukrow, 'Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108' (2018) 4 EDPL 2 239-247.

2 In this article we refer to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as Data protection convention or DPC and to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as Convention 108+.

3 Graham Greenleaf, 'Modernised' data protection Convention 108+ and the GDPR' 2018 (154) Privacy Laws & Business International Report 22-3.

4 Urszula Góral, 'The right to privacy and the protection of personal data: Convention 108 as a universal and timeless standard for policymakers in Europe and beyond' 2021(1) Acta Iuris Stetinensis 101 and Lee A Bygrave, 'The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects', 2021 (4) CLSR 105460.

5 COM (2018) 451 final 2018/0238, 2.

6 COM (2018) 451 final, 2018/0238. This position of the EC is supported by other parties, eg. the United Nations Special Rapporteur Cannataci, also pushed for a speedy ratification and entry into force of Convention 108+, cf. Joseph Cannataci, *Report of the Special Rapporteur on the right to privacy*, (Genève 2019) paras 28 and 47 <www.coe.int/en/web/data-protection/-/security-and-surveillance-un-push-for-convention-108-> accessed 27 September 2022.

7 This can be different for countries outside of the EU legal order, but these are outside of the scope of this report. See for example Eduardo Bertoni, 'Convention 108 and the GDPR: Trends and perspectives in Latin America' 2020 (29) CLSR; Colin J Bennett, 'The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession' 2020 CIGI Papers no. 246.

ing to Art. 4(2) TEU.[8] Member States have a large margin of discretion when evaluating national security threats and deciding how to combat these. Convention 108+ on the other hand explicitly applies to the area of national security – in so far that the area of national security and surveillance cannot be entirely excluded from its material scope. This means that Convention 108+ is likely to strengthen the harmonised data processing regulation in a national security context.[9]

So far, the impact of data protection legislation of both the CoE and the EU on this national security domain has not gained much attention. This report aims to do that by giving an overview of the implications of Convention 108+ for data processing in the national security domain. It first discusses what should be considered 'national security' (II.). After that, we look at the GDPR and its possible applications in the national security domain (III.) and then switch to the DPC and Convention 108+ and present how it will apply in the national security domain (IV.). Finally, we look in more detail at the legal consequences for both the EU Member States and the EU as an organisation(V.) before concluding (VI.).

II. The National Security Domain

No clear-cut definition of 'national security' exists. The Explanatory Report to Convention 108+ states that this notion must be interpreted in line with the relevant case law of the European Court of Human Rights (ECtHR). In this context, states have a possibility to invoke reasons of national security to justify certain restrictions to human rights. National security is seen as one of the legitimate aims for such restrictions.[10] However, the ECtHR does not use a very clear definition either. In fact, the Commissioner of Human Rights considered it impossible to comprehensively define the term national security.[11] The notion is related to the protection of the state, and it is interpreted in a flexible way to adapt to changing threats.[12] The ECtHR includes in particular the protection of state security and constitutional democracy from a wide range of threats such as espionage, separatism, and terrorism. However, not every serious crime is a national security threat.[13]

States have a wide margin of appreciation to decide the best way to protect their national security. The ECtHR can decide in individual cases whether or not a certain measure is in line with the European Convention on Human Rights (ECHR). It is important to mention that the ECtHR takes what one can refer to as a holistic approach when it refers to national security. It adjudicates on the basis of the (protective) system as a whole with all different facets that play a role. The ECtHR has, amongst others, referred to the possible existence of less restrictive measures,[14] the requirement of the existence of independent courts to review such measures,[15] and the level of detailedness of the (accessible and foreseeable) law that uses national security as a basis for restriction.[16]

To highlight the differences in scope of application of the GDPR and Convention 108+, we shortly focus on data processing in the domain of national security. Here, one can think of large scale data collection, interception, retention, analyses of traffic data, and other surveillance measures. Data processing in a national security context does not necessarily take place by enforcement agencies or security and intelligence agencies. Other controllers, such as businesses, can also process data for such purposes.

In its case law, the ECtHR time and again stresses the importance of the protection of privacy,[17] also in the context of interferences for national security reasons. The ECtHR assesses infringements mainly on the basis of the necessity and proportionality requirements and looks at a legislation framework as a whole, balancing this with other rights at stake. To

8 TEU, Art 4(2).

9 Jan-Jaap Oerlemans & Mireille Hagens, 'National security and the processing of personal data' (*Montaigne Centrum Blog,* 23 September 2020) <blog.montaignecentre.com/nl/blog_author/mireille-hagens/> accessed 26 January 2022.

10 E.g. Art 8 para 2, Art 10 para 2, Art 11 para 2 ECHR.

11 *Esbester/ The United Kingdom* App no 18601/91 (ECtHR, 2 April 1993).

12 *Christie/ The United Kingdom* App no 21482/93 (2ECtHR, 7 July 1994) par 12. Compare ICO, 'National security and defence', online <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/> accessed June 20 2022. See also Liz Campbell, 'Organized Crime and National Security: A Dubious Connection?' (2012) New Criminal Law Review 2, 233-234.

13 *Malone/The United Kingdom* App no 8691/79 (ECtHR, 2 August 1984) 76-79.

14 *Van Mechelen/ The Netherlands* App nos 21363/93, 21364/93, 21427/93 and 22056/93 (ECtHR, 23 April 1997).

15 *Incal/ Turkey* 41/1997/825/1031 (ECtHR, 9 June 1998).

16 *Klass and others/ Germany* no 28 (ECtHR, 6 September 1978).

17 *Amann/ Switzerland* App no 27798/95 (ECtHR,16 Februari 2000); *Rotaru/ Romania* App no 28341/95 (ECtHR, 4 May 2000).

give some examples, the ECtHR considers interferences proportionate when a state pursues a legitimate aim to prevent serious threats, for a short period, only affecting the person of interest.[18] Arbitrary and potentially limitless surveillance by intelligence agencies is not proportionate.[19] Such actions must have a legal basis in national legislation which must contain sufficient definitions of the measures taken,[20] and the national legislation must also provide for adequate judicial oversight and court reviews for renewal of orders.[21]

III. The GDPR and the National Security Domain

The GDPR applies 'to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'.[22] The GDPR contains rules on the processing of personal data and applies to private parties as well as companies, and states. The essence of the GDPR consists of the data protection principles that materialise broadly what a processing of personal data should look like. Every processing must be in line with these, openly formulated, principles.

As mentioned above, the GDPR in principle does not apply to the data processing by national security and intelligence agencies.[23] The EU legal framework thus is organised in such a way that the organisation and oversight of national security remain the responsibility of each individual EU Member State.

However, this picture is not as clear as it might seem. The national security of Member States overlaps and intersects with the internal security of the EU. In this latter area, the EU has a shared competence to adopt legislative measures in the area of Freedom, Security, and Justice (AFSJ) as governed by Title V of the TFEU. Based on articles 87 and 88 TFEU, the EU has for example the competence to adopt legislation on police cooperation, fighting organised crime, and fighting terrorism. It can be difficult to draw a strict line between national security and any of those topics. Being a shared competence, both the EU and Member States can act in this area, but Member States have to act within the EU legal framework. However, the GDPR does not apply to data processing undertaken in the domain of national security. Therefore, any data processing in that domain is exempted from the data protection principles of the GDPR as well as the rights of individual data subjects, the stricter rules on the processing of special categories of personal data, and requirements related to reporting of data breaches and impact assessments – unless there is national legislation that puts forward such requirements.

Because of the lack of a generally accepted definition it can be questionable whether an action of a Member State concerns a matter of national security, especially in the intersection of data retention and national security. In recent cases – in particular *la Quadrature du Net, Privacy International,* and *The Commissioner of the Garda Síochána*[24] – the Court of Justice of the EU (CJEU) has defined national security rather narrowly, therefore strengthening the role of EU law in the context of data retention.[25] In these cases, the CJEU held that EU law precluded the existence of national legislation that required providers of electronic communication services to carry out general and indiscriminate transmission of traffic and location data to intelligence and security agencies for the purpose of safeguarding national security. It concluded that, if such data retention is warranted in a case where there exists a serious threat to national security, the nature of the measure nonetheless must be strictly proportionate to the purpose.

18 *Uzan/ Germany* App no 35623/05 (ECtHR, 2 September 2010).

19 *Roman Zakharov/ Russia* App no 47143/06 (ECtHR, 4 December 2015); See on this Mark Cole and Annelies Vandendriessche, From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg, (2016) 2 EDPL 1, 121-129.

20 *Szabó and Vissy/ Hungary* App no 37138/14 (ECtHR, 12 January 2016).

21 *Centrum för rättvisa/ Sweden* App no 35252/08 (ECtHR, 25 May 2021).

22 GDPR, Art 2(2).

23 GDPR, Art 2(2)(a,b,d): The GDPR shall not apply to the processing of personal data in the course of activities which fall outside the scope of EU law, the processing by Member States when carrying out activities which fall within the scope of Title V, Chapter 2 of the Treaty on the European Union (TEU), and the processing by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties.

24 *Privacy International* Case C-623/17, ECL:EU:C:2020:790 (CJEU, 6 October 2020); *La Quadrature du Net and Others* Case C-512/18, ECLI:EU:C:2020 :791 (CJEU, 6 October 2020); *The Commissioner of the Garda Síochána* Case C-140/20, ECLI:EU:C:2022:258 (CJEU, 5 April 2022).

25 Monika Zalnieriute, A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union, MLR 2022 (85)1 198, 217.

IV. Convention 108+ and the National Security Domain

The assessment of application to the national security domain is different for Convention 108+ as will be shown in the following.

1. An Overview of the Original Convention and the Protocol Creating Convention 108+

The Data Protection Convention (DPC) was created within the framework of the Council of Europe with the aim of protecting the right to privacy as guaranteed by Article 8 ECHR. It has had an impact worldwide, partly due to the currently 55 countries that are party to the Convention, including nine non-CoE members.[26]

The DPC has a wide scope of application. It is relevant to any data processing carried out in both the public and the private sector. In principle, this also includes processing by the judiciary and law enforcement authorities, and data processing in the context of national security. The Convention also allows for certain restrictions and exceptions. No exceptions are allowed to the so-called basis principles for data protection, unless the breach is within certain limits and serves a legitimate purpose.[27] Exceptions to the rights regarding the quality of data, special categories of data, and data security can, for example, be made in order to protect State security or public safety.[28] Various parties to the Convention make use of these possibilities.

The DPC contains a number of principles for the processing of personal data such as the requirement that data which is processed by automated means must be obtained and processed fairly and lawfully.[29] In 2001, the Data Protection Convention was supplemented by an Additional Protocol which obliges parties to set up one or more independent supervisory authorities.[30] It also regulates the obligation to allow cross-border data traffic to states that are not party to the Data Protection Convention only if an adequate data protection regime exists in that third country.

After nearly two decades since the last protocol, the DPC was considered in need of modernisation in order to reinforce the protection of individuals and to strengthen the implementation of the Convention.[31] The main objective was 'to adapt this landmark instrument to the new realities of an increasingly connected word, and to strengthen the effective implementation of the convention'[32]. The CoE aimed to bring the Convention more in line with the GDPR.[33] The result of this modernisation process is Convention 108+.[34] Its content remains largely the same as the content of the DPC. Some changes are mainly linguistic in order to bring the terminology more in line with the GDPR.[35] But there are also a number of changes that change the Convention,[36] such as an expansion of the rights of data subjects.[37]

26 Argentina, Burkina Faso, Cape Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay. See: Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 IDPL 68. See also Sara Leonor Duque de Carvalho, 'Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108' (2019) 1 EDPL 54.

27 Data Protection Convention, art 9.

28 Art 9(2)(a) Data Protection Convention.

29 Art 8(a) Data Protection Convention.

30 Art 1 Protocol.

31 Viktor Mayer-Schönberger, 'Paradigm shift' 2021(40) CLSR 105515.

32 Alessandra Pierucci & Jean-Philippe Walter, *Joint statement 'Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services* (Strasbourg, 7 September 2020) 3.

33 EU Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, 2018 Luxemburg: Publications Office of the European Union, 11-12.

34 See for the cooperation partnership between United Kingdom and the EU David Erdos, 'The UK and the EU personal data framework after Brexit: A new trade and cooperation partnership grounded in Council of Europe Convention 108+', *Computer Law & Security Review* 44 (2022). See for the Latin American perspective Eduardo Bertoni, 'Convention 108 and the GDPR: Trends and perspectives in Latin America', *Computer Law & Security Review* 40 (2021) and for the global perspective Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 IDPL 68; Graham Greenleef, 'How far can Convention 108+ 'globalise'? Prospects for Asian accessions', *Computer Law & Security Review* 40 (2021).

35 'The modernised Convention 108: novelties in a nutshell', online via <https://www.coe.int/en/web/data-protection/convention108/modernised> Accessed 27 June 2022. See also Jörg Ukrow, 'Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108', 2018 (2) EDPL 239, 240.

36 See also Paul de Hert & Vagelis Papakonstantinou, 'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition', 2014 (3) CLSR 633.

37 Convention 108+, art 8.

2. Convention 108+ and National Security

The aim of Convention 108+ is to raise the level of data protection for individuals significantly. With this in mind, the convention reduces the number of limitations and exceptions that existed under the original regime of the DPC. Now there are fewer possibilities to exclude (parts of) the Convention by Signatories with a reference to the protection of national security as foreseen by Art. 11. In addition, Convention 108+ explicitly incorporates the processing of personal data in a national security context into the scope of application. Exceptions and restrictions based on this are only permitted when they are provided for by law, respect the essence of the fundamental rights and freedoms, and are necessary in a democratic society.[38] The state party should ensure a prescription of the measure in a sufficiently detailed, accessible, and foreseeable law. National security is regarded as a legitimate aim that can make measures necessary in a democratic society.[39]

As a consequence, in a national security context, some principles of Convention 108+ can be excluded or altered, such as restricting the application of the principles of fairness, transparency, purpose limitation, data minimisation, accuracy, and storage restriction. Also, the duty to report data breaches, the obligation to inform data subjects, and the rights of data subjects can be restricted. This can lead to data subjects not being able to invoke their right to access against intelligence or security services if this is regarded as necessary to ensure national security and there is no less intrusive means of achieving the same objective. The principle of lawfulness – which requires any processing to be based on a previously determined basis and be otherwise in accordance with the law – cannot be excluded.[40] With regard to surveillance, Convention 108+ also leaves some room for restrictions and exceptions in the context of national security and defence.

3. Specifically on the Oversight of Processing Activities

The Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe recently stated that 'there is a strong need to tackle at international level the complex and sensitive question of the democratic and effective oversight of intelligence services'.[41] It is important to recognize that the regime of Convention 108+ will indeed bolster supervision of data processing activities compared to the DPC. Convention 108+ demands that every State Party has one or more authorities responsible for ensuring compliance with the Convention. In short, those authorities shall have powers of investigation and intervention, powers to issue decisions and impose administrative sanctions, and the power to engage in legal proceedings or to bring violations to the attention of the competent judicial authorities.[42] Decisions may be subject to judicial appeal.[43]

The oversight authorities should also raise public awareness about their functions, powers and activities, about the rights of data subjects and about the responsibilities of controllers and processors.[44] Furthermore, the supervisory authorities must be consulted regarding legislative proposals concerning the processing of personal data and they have to deal with requests and complaints lodged by data subjects.[45] Finally, those authorities must publish a periodical report outlining their activities.[46] To ensure that supervisory authorities are able to fulfil this duties, State Parties need to take a number of measures. Foremost, State Parties must make sure that the supervisory authorities can act with complete independence and impartiality. Therefore the supervisory au-

38 Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para 91.

39 Other legitimate aims are (a) defence, 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 essentials essential objectives of general public interest, and (b) the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression. See Convention 108+, Art 11(3).

40 Convention 108+, Art 11(1)(a) gives the possibility to exclude Art 5(4) but not Art 5(3). Compare also the UK Data Protection Act.

41 Alessandra Pierucci & Jean-Philippe Walter, *Joint statement 'Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services* (Strasbourg, 7 September 2020) 5. See also the issue paper of the Council of Europe's Commissioner for Human Rights 'Democratic and effective oversight of national security services (2015).

42 Convention 108+, Art 15(2)(a-d).

43 Convention 108+, Art 15(9).

44 Convention 108+, Art 15(2)(e).

45 Convention 108+, Art 15(3-4).

46 Convention 108+, Art 15(7-8).

thorities may neither seek nor accept instructions,[47] and State Parties have to ensure that they have sufficient resources.[48]

In a national security context, certain exceptions and restrictions on these oversight mechanisms are permitted. Under the regime of Convention 108+, State Parties are neither obliged to give those authorities the powers to issue decisions and to impose administrative powers in this context, nor to give them the power to engage in legal proceedings or to bring violations of the Convention to the attention of the competent judicial authorities.[49] However, when a State Party decides to give a national security supervisor limited powers, it should be aware that the necessity and proportionality assessments apply in a strict sense to those provisions. In addition, Convention 108+ underlines that exceptions and limitations are possible but only when the oversight stays independent and effective.[50]

This latter requirement of effectiveness is particularly important. It is hard to imagine any *ex post facto* oversight that would qualify as 'effective', when a supervisory authorities has no investigative powers whatsoever. On the other hand, it seems imaginable to have an 'effective' supervisory authority, even though the authority has no power to intervene. A supervisory authority can, for example, effectively enforce compliance by pressuring a supervised government body behind the scenes or by producing public reports and enforcing change through social and political channels. This would also fit the holistic approach of the ECtHR, which assesses a system of safeguards as a whole when judging on its legality.[51]

However, the ECtHR recently raised the bar, at least for *ex post facto* oversight on bulk interception regimes. [52] In *Centrum för Rättvisa* the Swedish supervisory authority for the intelligence agencies had the power to issue legally binding decisions. It could decide for processing that led to breaches to stop, to issue remedies and to hold those responsible for breaches liable. The ECtHR stated that the powers and procedural guarantees an authority possesses are relevant in determining whether or not a remedy meets the effectiveness-requirement. The Court characterised these kind of binding powers of the Swedish authority as 'satisfactory' and therefore effective. The Court considered that this regarded the processing of data where the impact on the fundamental rights is the greatest – especially in the accessing, analysis and storage phases of processing personal data.[53]

V. Consequences for the EU and EU Member States

Looking at the different legislative frameworks it becomes clear that the national security domain within the EU can become quite fragmented. Different legal regimes with different applications across the EU Member States exist.[54] The GDPR has a broader catalogue of material exceptions than Convention 108+.[55] There is an important difference between the GDPR of the EU and Convention 108+ by the CoE as the latter applies at least partly in the domain of national security, whereas the influence of the GDPR in that domain is very limited but not non-existent, given the overlap between national security and EU-security. CoE-members need to stay within the remit of article 8 of the ECHR even for activities related to national security, such as national intelligence activities and data processing by secret services, so if an activity of an EU Member State falls outside the scope of EU law, the ECHR still offers a fundamental rights protection that has to be respected.[56] The ECtHR has in a number of cases affirmed that surveillance activities constitute an interference with the respect for private life.[57]

47 Convention 108+, Art 15(5).

48 Convention 108+, Art 15(6).

49 Convention 108+, Art 11(3) and 15(2)(a-d).

50 Convention 108+, Art 14.

51 See also Venice Commission, *Report on the democratic oversight of signals intelligences agencies*, CDL-AD(2015)011, 27-28.

52 See in more detail Bart van der Sloot, 'Big Brother Watch and others v. the United Kingdom & Centrum för Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?' (2021) EDPL 2, 319-326.

53 *Centrum för Rättvisa* App no 35252/08 (GC, ECtHR 25 May 2021) , para 350.

54 Jan-Jaap Oerlemans & Mireille Hagens, 'National security and the processing of personal data' (*Montaigne Centrum Blog*, 23 September 2020) <blog.montaignecentre.com/nl/blog_author/mireille-hagens/> accessed 26 January 2022.

55 See for a detailed overview of all differences between GDPR and Convention 108+ Jörg Ukrow, 'Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108' (2018) 4 EDPL 2, 239-247.

56 All EU Member States are party to the ECHR. Cf. on the national security relevance European Union Agency for Fundamental Rights & Council of Europe, *Handbook on European data protection law* (Publications Office of the European Union, 2018 edition), 273.

57 *Klass and Others/ Germany* App no 5029/71 (ECtHR, 6 september 1978); *Rotary/ Romania* [GC] App no 28341/95 (ECtHR, 4 May 2000); *Szabó and Vissy/ Hungary* App no 37138/14 (ECtHR, 12 January 2016).

1. Consequences for the EU Member States

For EU Member States, it is difficult to generally assess the exact difference Convention 108+ will make, as this highly depends on the current state of their national laws. It is likely that certain Member States will have to make adjustments to their national legislation in order to bring it in line with Convention 108+. It is interesting to point out that due to the similarities in terminology, content, and rules of the GDPR and Convention 108+, a regulatory framework very similar to the GDPR will then become applicable to the national security domain after this not being the case "only" under GDPR.

As the rules for data processing in a national security context vary widely across the EU, Convention 108+ might bring more harmonisation in the area of national security, even if EU Member States decide to make use of the exceptions offered for the national security domain.

As an example, we point out an existing discussion in the Netherlands to show the potential implications of Convention 108+. This regards to oversight of national intelligence services. The two oversight bodies for the national security services, TIB and CTIVD, observed 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'[58]. Currently, only the TIB may make binding *ex ante* decisions about the use of certain powers in the national security field. The CTIVD – the oversight body for the *ex post facto* oversight – has extensive investigative powers and also periodically publishes public reports, but has no power to intervene. At least, not yet. Soon the Dutch legal basis for the gathering of bulk data will be changed, partly because of Convention 108+. This will create the possibility for the CTIVD to take binding measures so it could stop any data processing that leads to breaches.[59] Because those oversight decisions will have far-reaching effects, a special appeal procedure to the Dutch superior administrative court – the Council of State – will be established. These amendments seek to bring national law into line with the recent case law of the European courts and with Convention 108+.[60]

2. Consequences for the EU

We have already mentioned that the European Union wants to become a party to Convention 108+. While attempts in the 1990s to join the DPC failed, the EU now aims for accession to the Convention in line with its ambition to set the tone globally for privacy and data protection regulation.[61] Although it is currently impossible to say with certainty whether or not it will succeed this time, we will briefly discuss some possible consequences of such an accession of the Convention.

Convention 108+, although significantly more detailed and modern than the original DPC, has little concrete legislative improvements or changes to offer to the EU, especially if all Member States already are party to the Convention. After all, the topics governed by Convention 108+ are now already largely covered by the EU's current data protection framework.[62] We therefore assume that a signatory status of the EU will mainly be a symbolic act.

However, we also see some issues regarding a possible accession of the EU to Convention 108+, especially concerning the application to the area of national security. If the EU would become a party to Convention 108+, the legislative landscape with the differences would be complicated. In that case, the EU would become member to a convention that obliges it to implement rules and ensure certain principles and rules regarding *national* security. This seems strange: the EU then binds itself to legislation of the Council of Europe that also includes an area where it actually has little or no legislative authority within the EU legal order. This could lead to interesting legal questions about the EU regulatory competences – especially when the ECtHR and the CJEU start to

58 TIB and CTIVD memo on Convention 108+ and oversight on national security, https://english.ctivd.nl/documents/publications/2021/02/17/memo-en.

59 See the legislative proposal 'Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma' (2022).

60 See for a comparative approach the analysis, with reference to the TIB and CTIVD memo, of German intelligence law K. Vieth-Dtlmann & T. Wetzling, *Caught in the Act? An analysis of Germany's new SIGINT reform* (The Human Rights, Big Data and Technology Project, Stiftung Neue Verantwortung) (2021) 55-56.

61 See in more detail Anu Bradford, *The Brussels Effect: How the European Union rules the world* (Oxford 2020) 132-136. See also Alessandro Mantelero, 'The future of data protection: Gold standard vs. global standard' 2021 (40) CLSR 105500.

62 See also COM(2018) 449 final (Brussels, 5.6.2018).

further harmonise their interpretations. Although one could argue that these parts of Convention 108+ cannot apply to the EU in case of an accession, the question can be put forwarded whether becoming a signatory is at all possible.

VI. Conclusion

This report gave an overview of the implications of the European legislative framework for privacy and data protection on the national security domain. The focus was mainly on Convention 108+, which amends the currently existing Data Protection Convention of the Council of Europe. Unlike the Data Protection Convention and the GDPR, Convention 108+ will be applicable to data processing within the domain of national security. The report demonstrated the several implications this has, especially with regard to oversight mechanisms. However, in the context of national security, certain exceptions and restrictions to Convention 108+ will still be possible which is why ratifying states will have to meticulously examine their national security legislation in the light of (the provisions of) then applicable Convention 108+. It is not unlikely that they will have to strengthen the legal safeguards for the privacy protection of citizens also in this context.