14/EN
WP 228

Working Document on surveillance of electronic communications for intelligence and national security purposes

Adopted on 5 December 2014

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Executive Summary

This Working Document contains the legal analysis behind the WP29 *Opinion on surveillance of electronic communications for intelligence and national security purposes* that was adopted on 10 April 2014. The focus of this Opinion lies with the follow up that is needed after the Snowden revelations. To this end, it contains several recommendations on how to restore respect for the fundamental rights of privacy and data protection by the intelligence and security services, and on how to improve supervision of these entities' activities while maintaining national security. The current Working Document contains the result of the discussions and legal analysis on which the Working Party's recommendations are based.

First of all, it is important to note that it is not only European Union law that needs to be taken into account when discussing national security and surveillance issues from a data protection point of view. As important are the principles set out in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, as well as those enshrined in the European Convention on Human Rights and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[1]. Interference with these rights can only be considered if it is in accordance with the law and if it is necessary, proportional and answers a pressing social need. This also entails that other, less intrusive options are unavailable.

In absence of a clear definition of 'national security', the Working Party has examined how this notion should be interpreted, especially since the thin line between law enforcement and national security sometimes seems to fade. In any case, national security needs to be distinguished from the security of the European Union, but also from State security, public security and defence. All of these notions are referred to separately in the EU treaties and underlying legislation, although they are inextricably linked. Whether or not something should be defined as falling under the national security exemption therefore cannot only be explained by strictly legal arguments. What can be said is that, whereas activities by intelligence and security services are generally accepted as falling under the national security exemption, this is not always the case when general law enforcement authorities fulfil similar tasks.

The Working Document also discusses the question if a third country's national security interest can be invoked. The Working Party stresses that the exemption in the treaties offers no possibility to invoke the national security of a third country alone in order to avoid the applicability of EU law. However, it acknowledges that there may be areas where a national security interest of an EU Member State and that of a third country are aligned. If so, this

[1] Their respect is mandatory for all the State parties, including EU Countries

should be properly justified by the EU Member State to the relevant authorities on a case-by-case basis.

A major part of the Working Document discusses the applicability of the transfer regime of Directive 95/46/EC. Even though many details of the surveillance programmes are still unclear, it seems likely that the third country surveillance authorities primarily obtain access to data after they were transferred from a data controller under EU jurisdiction to a location outside EU jurisdiction. Such transfers will in principle take place in accordance with the procedures foreseen in the Directive and its implementing legislation on national level, possibly making use of standard contractual clauses, binding corporate rules or the Safe Harbor agreement. However, none of these instruments contains a provision that would allow for massive, structural or unlimited data transfers. In as far as third country public authorities wish to obtain direct access to personal data under EU jurisdiction, they should make use of the formal means of cooperation, since no explicit possibilities are foreseen in the EU legislation to transfer personal data held by private sector data controllers to third country law enforcement authorities or security services. The Working Document contains examples of scenarios to illustrate its analysis more effectively. The Working Document concludes by commenting on possible options for a way forward.

Table of Contents

1. Introduction

On 10 April 2014, the Article 29 Working Party (hereafter: the Working Party) adopted its Opinion on surveillance of electronic communications for intelligence and national security purposes[2], providing an initial response to the revelations regarding mass surveillance by intelligence services from around the world based on documents primarily provided by Edward Snowden. The Opinion also contains several recommendations to the international community and the legislators in the European Union and its Member States on how to improve personal data protection of individuals when dealing with surveillance.

While the focus of the Opinion lies with the much needed follow up of the data protection consequences of the Snowden revelations, the members of the Working Party have also held extensive discussions on the legal framework of mass surveillance, especially with regard to the applicability of European law to the surveillance activities revealed. The current Working Document contains the result of those discussions. At the same time, the Working Party is convinced that a broader debate, including different stakeholders, needs to take place. The current Working Document is thus primarily intended as a contribution to such a debate. It also provides several scenarios of data transfers with regard to third countries´ intelligence and security services. The Working Party stresses that the analysis in this Working Document does not and cannot give a satisfactory solution for all relevant cross border data processing operations that may occur: a final legal analysis of the legitimacy of a data processing will always depend on the specifics of every case.

2. Surveillance programmes

Since mid-2013, a large number of previously secret surveillance programmes has been disclosed by the media, primarily by The Guardian[3] and The Washington Post[4]. Many of these programmes seem to be directed at the bulk collection of personal data from various online sources and concern both content and traffic data. According to the reports, most of the programmes do not distinguish between suspected and non-suspected individuals. This also revealed that intelligence services involved in surveillance programmes in other countries appear to extensively collaborate with each other.

---

[2] WP215 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

[3] http://www.theguardian.com/world/the-nsa-files.

[4] http://www.washingtonpost.com/nsa-secrets/.

Electronic surveillance by means of signals intelligence[5] has become a common technique for intelligence services over the past decades and should respect the conditions set in the law for lawful interception on communication in order to be used legally. It has however become clear since the Snowden revelations that the borders of legality have been reached, and sometimes also crossed.[6] Surveillance programmes are likely to exist in all parts of the world.

The following overview in sections 2.1 and 2.2 is intended as factual information and is mainly based on information provided in the media reports, the report of the EU-US working expert group[7] as well as information that was declassified by the US authorities following the public disclosures of several surveillance programmes. This brief overview does not represent a position of the Working Party although Working Party views are expressed in later sections. To date, European governments have publicly provided very little information regarding the existence and workings of the alleged surveillance programmes, especially regarding the collaboration of their respective intelligence community with authorities being in charge of those programmes. It has however become clear that mass electronic surveillance is not a strictly American affair, but a phenomenon that takes place in many countries and on a global scale. The example of the US below is meant as an illustration of some of the issues that have arisen as the US example has been arguably the most widely discussed third country example so far but there have also been cases in other countries as set out in section 2.2.

2.1. Surveillance by the US

In the US, most surveillance programmes are run by the NSA. The resulting databases are accessible for searches by the NSA, the CIA and/or the FBI, depending on the programmes. Most of the surveillance programmes are carried out under the USA PATRIOT Act and the Foreign Intelligence Surveillance Act (FISA), but also on the basis of (Presidential) Executive Order 12333.

---

[5] Signals intelligence (or SIGINT) is a term generally used to indicate the collection of information on communication between people as well as the collection of electronic signals from for example radars and weapon systems. The information on communications can contain both content and "about" information, which in the United States is referred to as metadata.

[6] See in particular developments in the USA's Privacy and Civil Liberties Oversight Board (PCLOB) reports – available at: http://www.pclob.gov/

[7] Report on the Findings by the EU Co-chairs of the Ad Hoc EU-US Working Group on Data Protection accompanying the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" (COM(2013) 846 final) - http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf - *This EU-US Working Group addresses the different dimensions of the EU-US relationship in relation to surveillance, encompassing the Patriot Act, the Executive Order 12333, the executive, congressional and judicial oversight functions. The Commission Communication focuses more on the potential changes needed to transfer agreements between EU and US such as the PNR agreement, the TFTP agreement, the Umbrella Agreement on law enforcement matters and Safe Harbour.*

In response to the public debate that erupted following the Snowden revelations, the President of the US created a Review Group on Intelligence and Communications Technologies. This group delivered its report on 12 December 2013, including recommendations on possible changes to the US national security policy.[8] The president has taken these recommendations into account in his preparation of a new policy directive on signals intelligence activities, which was presented at a press conference on 17 January 2014.

The main changes that have been announced are related to the surveillance programmes under Section 215 of the USA PATRIOT Act, especially the so-called business records programme allowing for the collection of traffic data (telephony metadata) by the telecommunication providers. Notwithstanding the conclusion of the Privacy and Civil Liberties Oversight Board (PCLOB) on Section 215 of the USA PATRIOT Act, especially the so-called business records programme allowing for the collection of telephony metadata, that the collection of metadata "lacks a viable legal foundation"[9], mass surveillance programmes will not be ended. However, the President of the US also announced more stringent oversight of the US intelligence activities, including a change in the procedure before the FISA Court, allowing for "the introduction of a panel of advocates from outside government to provide an independent voice in significant cases".[10] And although the President of the US has stressed it is important to rebuild trust with overseas partners, the proposed changes for the collection of foreign intelligence information are rather limited. Collection of signals intelligence for national security purposes will continue in bulk but it is simply the telecommunications providers not the government which will retain the data. He has added that the use of the data will however need to comply with the national security purposes.

The PCLOB released an additional report on Section 702 of the USA PATRIOT Act in July 2014. This report does not go as far in its criticism of existing practices as a previous report on Section 215 (released January 2014). It recognises that "*certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness*", referring to such aspects as the unknown and potentially large scope of the incidental collection of U.S. persons' communications, the use of 'about' collection to acquire internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected. The report makes recommendations to make the PRISM and Upstream programmes (both of

---

[8] Liberty and Security in a Changing World – Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, p. 11, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. (last visited on 20 November 2014)

[9] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, p. 1616, http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf. (last visited on 20 November 2014)

[10] Speech of the President of the United States, available on http://www.whitehouse.gov/blog/2014/01/17/president-obama-discusses-us-intelligence-programs-department-justice. (last visited on 20 November 2014)

which fall within scope of Section 702 of the Patriot Act) more 'reasonable' in relation to the USA's constitutional boundaries.

2.2. Surveillance by European Union Member States and other third countries

The Snowden revelations and those emerging in parallel to the Snowden case are not limited to US surveillance activities but also concern surveillance by intelligence services of EU Member States, be it on European territory or abroad. These are particularly relevant, since several Europe-based intelligence services are now confirmed as having a close working relationship with their US counterparts[11]. The closer the relationship with the United States, the more information is shared on the basis of reciprocity. This goes to show that national security is less 'national' than the word would suggest: data, including personal data, are shared and exchanged by intelligence services on a large scale.

Surveillance programmes run by European intelligence services allegedly vary from the collection of traffic metadata from various sources to the monitoring of web fora and to tapping cable-bound communications. Hardly any of these programmes have however been confirmed by Governments themselves to date[12].

Also outside the European Union, governments are reluctant to confirm the existence of surveillance programmes run by their intelligence services. However, there are clear indications that such programmes are used at least by Australia[13], Russia[14], India[15] and China[16]. The functioning of these revealed activities is however expected to be similar to what has been disclosed thus far: intelligence services collect personal data on a very large scale and cooperate on a global scale, in various alliances, by sharing information. Sometimes, the national security concern of one country seems to have become the concern of many.

---

[11] Statement from Charles Farr to the Investigatory Powers Tribunal, 16 May 2014.

[12] See in particular paragraphs 3, 4 and 5 of the report of the Office of the United Nations High Commissioner for Human Rights on The right to privacy in the digital age published on 30 June 2014 accessible at the following link: https://www.ccdcoe.org/sites/default/files/documents/UN-140730-RightToPrivacyReport.pdf

[13] http://www.theguardian.com/world/2014/oct/13/australias-defence-intelligence-agency-conducted-secret-programs-to-help-nsa

[14]http://www.theguardian.com/world/2014/sep/24/strasbourg-court-human-rights-russia-eavesdropping-texts-emails-fsb-

[15] For example in India: https://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state

[16] For example in China : http://www.theguardian.com/world/2011/jul/26/china-boosts-internet-surveillance (last visited on 20 November 2014)

From a data protection point of view, this leads to various questions. Is the use (processing) of personal data by intelligence services legal? How have the data been acquired and what is the legal basis? Can personal data from private companies in the EU simply be accessed from abroad, without the data subject being aware this happens or even that it may occur? To what extent does the Europe-wide recognised fundamental right to data protection continue to apply (effectively) in this day and age, when personal data apparently are so readily accessible for government services?

These questions have been debated heavily within the Working Party. Thus far, only some conclusions have been drawn, since a full assessment so much depends on the specificities of a case: is there a suspicion, what is the relevant legal framework, is the data collection specific and targeted, etc. At the same time, a debate on the question to what extent the international and European data protection legal framework is and should be applicable needs to take place.

3. General legal framework

When looking at the legal framework applicable to surveillance activities, one cannot avoid considering the national security exemption imposed by article 4(2) of the Treaty of the European Union (TEU). However, a broader spectrum of legislations applies to these activities. Starting from the original international norms that are widely recognised and that have influenced European law, the United Nations legal instruments provide for a universal right for individuals not to be subjected to arbitrary or unlawful interference with their privacy. Council of Europe instruments together with the European Court of Human Rights (ECtHR) case law then ensure a common European understanding of the scope of this right and of the possible interferences with it.

3.1. United Nations legal instruments

The Working Party recalls that international human rights law provides the universal framework against which any interference within individual privacy rights must be assessed.

The international human right to privacy is codified in the United Nations' (UN) Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights[17].

Article 12 of the Declaration and Article 17 of the International Covenant declare that no one shall be subjected to arbitrary or unlawful interference with his privacy.

[17] International Covenant on Civil and Political Rights, General Assembly Resolution, 2200A 16 December 1966.

States subject to the Charter of the United Nations have an obligation to promote universal respect for, and observance of, human rights and freedoms[18]. Moreover, each of the States parties to the Covenant undertake to take the necessary steps, in accordance with their own constitutional processes and with the Covenant to adopt such laws or other measures as may be necessary to give effect to the rights in the Covenant. This includes providing effective remedies, including developing judicial remedies for violations of the Covenant rights and that any of these remedies are effectively enforced.

3.1.1. UN General Assembly resolution 68/167 of January 2014

The UN General Assembly resolution 68/167[19] reaffirmed the Covenant's rights and:

- acknowledged the balancing of the interests involved in privacy and security, noting that public security may justify the gathering and protection of certain sensitive information, but States must ensure full compliance with their obligations under international human rights law;

- affirmed that the same rights that people have offline must also be protected online, in particular the right to privacy and called on States to protect these rights on all digital platforms;

- called upon States Party to take any measures to stop existing violations of these rights and moreover that they create conditions to prevent any violation; and to review their national procedures, practices and legislation (particularly relating to the surveillance of communications, their interception and collection of personal data, including massive surveillance, interception and collection) to ensure that the legislation in force does not currently allow violation of the Covenant's rights; and that the Parties ensure full and effective implementation of their international human rights obligations.

This Resolution also called upon States party to the Covenant to establish independent national oversight mechanisms capable of ensuring transparency and accountability of State surveillance of communications, their interception and collection of personal data. The UN Resolution therefore coincided with the Working Party work on examining existing practices for supervision over the national intelligence services in EU Member States in Working Party Opinion WP215 adopted on 10 April 2014. The Working Party identified the need, following the surveillance revelations in 2013, to conduct an overview of the existing oversight mechanisms in existence for intelligence and national security services' activities at a national level in the EU. The Working Party´s view was that these mechanisms often have an impact on effective EU data protection and privacy enforcement.

[18] Charter of the United Nations, article 55(c)

[19] UN General Assembly resolution 68/167, 21 January 2014 - http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167 (last visited on 20 November 2014)

The Working Party's intention in conducting such a survey was to present a clearer picture of the various arrangements in Europe. This involved identifying where the data protection authority has the power to supervise intelligence services, and where there are limitations. In the Working Party's view, the survey's significant finding is that data protection authorities support closer scrutiny on how EU Member States maintain a coherent legal system for the intelligence services and what the national legal frameworks should contain to ultimately guarantee data protection rights for individuals[20]. The aforementioned Opinion presents the results of this survey in detail[21].

Finally, the UN resolution also requested the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council and to the General Assembly.

While such a Resolution is not legally binding, it sends an important message to the States Party that serious further thought and collective and individual action is needed in line with the purposes of the UN as set out in Article 1 of the UN Charter[22]. The Resolution also aims at expanding the protection guaranteed in the International Covenant on Civil and Political Rights, to electronic communications and privacy.

---

[20] In the Opinion (WP215, p. 13), the Working Party amongst others calls for "*effective, robust and independent external oversight, performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself*".

[21] The survey is not relevant to go into more detail in this Working Document which concentrates on other important legal considerations related to this matter.

[22] The UN Charter, Article 1, paragraphs 3 and 4 state: "3.To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and

4. To be a centre for harmonizing the actions of nations in the attainment of these common ends."

A pertinent question reflecting the call for further thought during the discussion of the UN Report in November 2013 was offered by the German Ambassador, one of the joint sponsors of the Resolution, who asked "But should everything that is technically feasible also be allowed?" Web: http://www.dw.de/germany-brazil-introduce-anti-spying-resolution-at-un-general-assembly/a-17213179 'Germany. Brazil introduce anti-spying resolution'. Deutsche Welle (last visited on 20 November 2014)

3.1.2. UN Report on the Right to Privacy in the Digital Age

This report[23] was adopted in July 2014[24], following the events outlined above. The Report's recommendations and conclusions underlined that "*there is a clear and pressing need for vigilance in ensuring the compliance of any surveillance policy or practice with international human rights law, including the right to privacy, through the development of effective safeguards against abuses*"[25]. The report deplored the circumstances in many countries which have contributed to a lack of accountability for arbitrary or unlawful interference within the right to privacy. This notably includes a lack of transparency around surveillance practices and legal frameworks. The Working Party highlights the UN report's statement that, "*As an immediate measure, States should review their own national laws, policies and practices to ensure full conformity with international human rights law.*"

The UN report also highlights the necessity of ensuring the legal review processes include a dialogue involving all interested stakeholders, including Member States, civil society, scientific and technical communities, the business sector, academics and human rights experts. The Working Party will be particularly interested in this and will endeavour to create more debate in Europe at a special conference in late 2014, as outlined in its Opinion 4/2014.

Separately, the Working Party also notes that the 2013 International Conference of Data Protection and Privacy Commissioners adopted a resolution[26] following up on its previous calls for a more detailed development in international law of the rights to privacy and more specifically, data protection. The Commissioners resolved to "*call upon governments to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in General Comment No. 16 to the Covenant*".

---

[23] Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age. Distributed 30 June 2014. Web: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last visited on 20 November 2014).

[24] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last visited on 20 November 2014).

[25] Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age, distributed 30 June 2014, p.16, paragraph 50,

[26] Resolution on anchoring data protection and the protection of privacy in international law, 35th International Conference of Data Protection and Privacy Commissioners, September 2014. Web: https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf (last visited on 20 November 2014).

In summary, despite some recent initiatives, the right to privacy at the level of the UN has not yet been developed in other[27], more detailed provisions, despite some recent initiatives. In Europe however, the right to respect for private life – as well as the right to data protection – have been qualified in a much more detailed manner, taking the first steps for the collective enforcement of certain rights listed in the Universal Declaration.

3.2. Council of Europe instruments

The two main legally binding instruments regarding fundamental rights and data protection at the level of the Council of Europe are the European Convention on Human Rights[28] (ECHR) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[29] (hereafter: Convention 108).

3.2.1. The ECHR

Article 1 of the ECHR obliges the Parties to secure to everyone within their jurisdiction[30] the rights and freedoms provided in the Convention. This implies that the Parties have not only negative obligations but also positive obligations, which "*require national authorities to take the necessary measures to safeguard a right*[31] *or, more specifically, to adopt reasonable and suitable measures to protect the rights of the individual*"[32,33]. In exceptional circumstances,

---

[27] General Comment 16 of the Human Rights Committee on Article 17 of the ICCPR, adopted on 8 April 1988, sets out a detailed interpretation of the right, including at paragraph 10, certain data protection principles.

[28] Convention for the Protection of Human Rights and Fundamental Freedoms – Rome, 4 November 1950

[29] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data -

Strasbourg, 28 January 1981 – ETS No. 108

[30] The notion of jurisdiction referred to in Article 1 of the ECHR has not been defined in the Convention nor in the preparatory Works. However, ECtHR case law has looked at the concept of effective control by the State when considering jurisdiction in relation to article 1. For example, in its judgment Loizidou v. Turkey of 23 March 1995, the ECtHR recalled that, although Article 1 (obligation to respect human rights) of the ECHR set limits on its scope, the concept of "jurisdiction" under that provision was not restricted to the national territory of the ECHR State parties. In particular, a State's responsibility might also arise when as a consequence of military action – whether lawful or unlawful – it exercised effective control over an area outside its national territory. States' obligation to secure in such areas the ECHR rights and freedoms derived from the fact that they exercised effective control there, whether that was done directly, through the State's armed forces, or through a subordinate local administration. In this respect, see also ECtHR, Al-Skeini and Others v the United Kingdom, 7 July 2011.

Under public international law, jurisdiction stands for the power of a sovereign state to regulate, to adjudicate and to enforce the norms by which its legal subjects are bound.

[31] ECtHR, Hokkanen v. Finland, 24 August 1994.

[32] ECtHR, Lopez-Ostra v. Spain, 9 December 1994.

the ECtHR case law has found that the concept of jurisdiction and the obligations of State Parties may not be restricted to the national territory of the State Party. In its case law on this issue, the ECtHR has considered the concept of the State Party having "effective control" to exercise jurisdiction.

In this regard, the European Parliament's Echelon report states in relation to the instruments of the Council of Europe that *"[Member] states remain responsible for their territory and thus have an obligation to European legal subjects if the exercise of sovereignty is usurped by the activities of the intelligence services of another state"*.[34]

3.2.1.1. Scope of application of the ECHR

In addition to the territorial scope defined in Article 1, the ECHR applies to the territories for whose international relations the Parties are responsible, if they have notified this information in accordance with Article 56(1) of the ECHR.

General limitations of the substantive scope of application of the ECHR are not allowed. However, at the moment of signature and ratification, the Parties had the opportunity to make reservations in respect of a particular provision of the Convention to the extent that the law in force in their territory was not in conformity with the provision in question[35]. As regards EU Member States, none of the reservations concern Article 8 of the ECHR on the right to respect for privacy and family life[36].

3.2.1.2. The right to respect for private life

Pursuant to Article 8(1) of the ECHR, "*everyone has the right to respect for his private and family life, his home and his correspondence*".

---

[33] Jean-François Akandji-Kombe, *Positive obligations under the European Convention on Human Rights*, Human rights handbook No.7, Council of Europe, 2007.

[34] Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) – A5-0264/2001, p. 88.

[35] See Article 57 of the ECHR.

[36] The notifications and declarations are available on http://www.conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=005&CM=8&DF=29/07/2014&CL=ENG&VL=1. (last visited on 20 November 2014).

The concepts of 'private life' and 'correspondence' include telephony and telecommunications data.[37] The case law of the ECHR specifies that the scope of the protection of this fundamental right covers not only the content of the communication, but also, e.g. "*the date and length of telephone conversations*" and "*the numbers dialed*", as such information constitutes an "*integral element of the communications made by telephone*".[38] In other words, the scope of the protection covers the content of the communication and what is also known as 'traffic data' or 'metadata'.

3.2.1.3. Possible interferences with the right to respect for private life

According to Article 8(2) ECHR, an interference by a public authority with the exercise of right to respect for private life may only be admissible if such restriction:

- is in accordance with the law (which must have foreseeable consequences and be generally accessible and)[39] and
- is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

It follows from the first condition that the second one refers to the interests of the Parties to the Convention and not to those of third States, independently of whether those interests coincide.

According to the jurisprudence of the ECHR, "*an exception to a right guaranteed by the Convention, is to be narrowly interpreted*". [40.] In the Klass case, the Court further specified that "*powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions"*[41].

Therefore, it has to be justified that any interference with the right to respect for private life (i.e., in this case, every single access by a governmental authority to personal data relating to communications) is strictly necessary in a democratic society for one of the purposes stated in Article 8(2).

---

[37] See ECtHR, Klass et al, 6 September 1978, para. 41.

[38] See ECtHR, Malone v. the United Kingdom, 2 August 1984, para. 84.

[39] See ECtHR, Malone, 2 August 1984, line 83 et seq.

[40] See ECtHR, Klass and others v. Germany, 6 September 1978, para. 42.. See also Youth Initiative for Human Rights v. Serbia, 25 June 2013 , §§ 24-26, which confirms that also intelligence agencies have to comply with fundamental rights and national laws implementing them.

[41] See Klass, above cited, also in para. 42.

According to the ECtHR, such interference can be considered necessary if it answers a pressing social need, is proportionate to the aim pursued and if the reasons put forward by the public authority to justify it are relevant and sufficient.[42]

In this regard, in S. and Marper v. The United Kingdom[43], the Court specified that the blanket and indiscriminate retention of the fingerprint and DNA data of applicants, as persons who had been suspected, but not convicted, was not justified under Article 8 § 2 of the Convention.

In the EU context, the Court of Justice of the European Union (CJEU) has also stated that, for the interference to be proportionate, it has to be demonstrated that other less intrusive methods were not available.[44]

In the specific case of national security, the ECtHR has noted that the arrangements governing the foreseeability requirement may differ from those in other areas but that the law must at all events state under what circumstances and subject to what conditions the state may carry out secret, and thus potentially dangerous interference within the exercise of the right to respect for private life.[45]

This would be particularly relevant and applicable to any surveillance activity involving a Party to the ECHR, be it or not in collaboration with a third country[46]. Besides, the right to respect for private life is granted to all individuals within the jurisdiction of a Party, regardless of their nationality or place of residence.

[42] See, among others, ECtHR, S. and Marper v. the UK, 4 December 2008, para. 101.

[43] See ECtHR, S. and Marper v. The United Kingdom, 4 December 2008, in particular paragraph 125: "In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data."

[44] See CJEU, Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 9 November 2010, para. 81.

[45] See ECtHR, Rotaru v. Romania, 4 May 2000, para. 50, 52 and 55; and Amann v. Switzerland, 16 February 2000, para. 50 et s.

[46] In such a case the responsibility of the country Party to the ECHR would be engaged, not the one of the third country.

This reasoning is supported by the judgment Loizidou v. Turkey[47] in which the Court stated that "*…the concept of jurisdiction under this provision is not restricted to the national territory of the High Contracting Parties […] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory"*, with reference to the ECtHR's Drozd and Janousek case[48].

3.2.2. Convention 108

The purpose of the Convention is "*to secure in the territory[49] of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')"*.

The Convention is also open for accession to States which are not member of the Council of Europe[50] Ratification of the Convention signals that a country takes a firm commitment to protect personal data and wants to adhere explicitly to common international standards. The Working Party would therefore welcome if non-European countries would indeed join the Convention.

3.2.2.1. Scope of application of Convention 108

In principle, Convention 108 and its additional Protocol apply to "*all automated personal data files and automated processing in the public and private sectors"*[51] unless the Parties have given notice that they will not apply it to certain categories of files in accordance with Article 3(2)(a). This list should be deposited and cannot include categories of files subject to the Party's domestic data protection provisions.[52]

---

[47] See ECtHR, Loizidou v. Turkey, 23 March 1995, para. 62, with reference to the Drozd and Janousek case, see ECtHR, Drozd and Janousek v. France and Spain, 26 June 1992, para. 91.

[48] See ECtHR, Drozd and Janousek v. France and Spain, 26 June 1992, para. 91.

[49] The territory may be further specified by the Parties in accordance with Article 24 of the Convention.

[50] Article 23 of the Convention.

[51] See Article 3(1) of the Convention.

[52] See Article 3(2)(a) of the Convention.

Therefore, the national law implementing the Convention will apply to files relating to the 'national security' of a Party to the Convention unless the Party in question has expressly opted for an exemption and correspondingly reported it in a duly deposited list. Until now, only a minority of the Parties have deposited declarations exempting 'state security' or 'State Secrets'.[53]

Some Parties have also decided to apply the Convention to personal data files which are not processed automatically, in accordance with Article 3(2)(c), or to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality (see Article 3(2)(b).

3.2.2.2. Data protection principles within Convention 108

Chapter II of the Convention contains the 'basic principles for data protection'. The principle of quality of the data (Article 5) includes the obligation that the data shall be obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 states that 'special categories of data' (personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life) and personal data relating to criminal convictions may not be processed automatically unless domestic law provides appropriate safeguards.

Article 7 contains the obligation to take appropriate security measures and Article 8 lays down the data subject's rights of information, access, rectification, erasure, as well as the right to have a remedy if such rights are not complied with.

According to Article 10, the Parties undertakes to establish appropriate sanctions and remedies for violations of these principles, as implemented in the Parties' domestic laws. Article 11 allows the Parties to grant a wider protection than that provided by the Convention.

[53] Ten Parties have made such a declaration, including the EU Member States Ireland, Latvia, Malta and Romania.

3.2.2.3. Exceptions

Article 9 of the Convention provides for exemptions to the obligations to respect the principles of quality (article 5), the special safeguards for sensitive data (article 6) and the rights of data subjects (article 8)[54] if such derogation:

- is provided for by the law of the Party and
- constitutes a necessary measure in a democratic society in the interests of protecting the data subject, the rights and freedoms of others, or state security, public safety, the monetary interest of the state or the suppression of criminal offences.

Once more, it should be recalled that the ECtHR places a great emphasis in its case law on the interpretation of the exemptions in article 8 of the ECHR. This reasoning can, *a fortiori*, be applied to the interpretation of the exemptions contained in the Convention 108[55]. The ECtHR interprets fundamental rights in quite a wide manner, in accordance with the principle of effectiveness, which requires that these rights be interpreted in the sense which best protects the person[56]. This also follows from the additional protocol to the Convention which states that "*the parties have discretion to determine derogations from the principle of an adequate level of protection. The relevant domestic provisions must nevertheless respect the principle inherent in European law that clauses making exceptions are interpreted restrictively so that the exception does not become the rule*".[57]

3.2.2.4. The additional protocol No. 181[58] and the rules on transfers

An additional protocol to Convention 108, not ratified by all EU Member States, lays down the rules on transborder data flows and the obligation to establish independent data protection supervisory authorities.

---

[54] See Article 9 of the Convention.

[55] The Court, it can be argued, allows itself to deal with Convention 108 through the ECHR article 8 provisions.

[56] Jean-François Akandji-Kombe, *Positive obligations under the European Convention on Human Rights*, Human rights handbook No.7, Council of Europe, 2007.

[57] Cf. report on the Additional Protocol to Convention 108 on the control authorities and cross border flows of data, Article 2(2)(a).

[58] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (CETS No.: 181), Strasbourg, 8.11.2001.

Article 2(1) of the additional protocol states that transborder flows of personal data to a State or organisation which is not subject to the jurisdiction of a Party to the Convention may only take place if the recipient State or organisation ensures an adequate level of protection for the intended data transfer.

However, by derogation of this provision, Article 2(2) states that the Parties may allow for the transfer of personal data if (a) their domestic law provides for it because of specific interests of the data subject or of legitimate prevailing interests, especially important public interests; or (b) if the controller responsible for the transfer provides safeguards, which can in particular result from contractual clauses, and these safeguards are found adequate by the competent authorities according to domestic law.

3.2.2.5. Recommendation No. (87)15[59] on processing of personal data in the police sector

In addition to the above mentioned legally binding instruments, the Committee of Ministers has adopted several recommendations addressed to the members of the Council of Europe concerning the processing of personal data. These recommendations have been the basis for enacting domestic legislation in several Member States and some of them are mentioned and implemented in binding EU instruments.

Recommendation No. (87)15 regulates the use of personal data in the police sector. It provides guidance to the Member States on the basis of Article 8 of the ECHR, Convention 108 and the derogations permitted under its Article 9. It covers "*all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order*"[60]. It is therefore only relevant in as far as national security tasks are carried out by regular police authorities instead of by intelligence or security services.

3.2.3. Conclusion

In conclusion, since all EU Member States are also Parties to the ECHR and the Convention, they have a positive obligation, also developed in case-law of the European courts, to secure effective protection of fundamental rights of all individuals within their jurisdiction.

Any limitations to these fundamental rights can only be accepted when they meet the conditions established by the ECtHR and are thus restricted to specific, well described and foreseeable situations. The Working Party therefore points out that if compliance with the Council of Europe instruments is to be considered effective, then no massive, indiscriminate and secret collection of data relating to individuals subject to EU jurisdiction can be tolerated by States party to the ECHR.

[59] Recommendation No. (87)15 regulating the use of personal data in the police sector, 17.09.1987.

[60] See section "Scope and definitions" of Recommendation No. R(87)15.

4. European Union law

Regarding the applicable legislation at European Union level, this section reflects on the scope of the national security exemption and on relevant texts such as Article 16 of the Treaty on the Functioning of the European Union (TFEU), Article 7, 8 and 52(1) of the Charter of Fundamental Rights. At secondary law level, the conditions in which Directive 95/46/EC[61,62] and the e-Privacy directive are assessed and a particular focus is made on the transfers' regime under Directive 95/46/EC.

4.1 National security exemption

Before going into the specifics of European Union legislation, it is necessary to reflect on the meaning of the national security exemption imposed by article 4(2) of the Treaty of the European Union (TEU). This article states that "*the Union shall respect the equality of Member States (...) as well as their national identities (...) It shall respect their essential state functions, including (...) safeguarding national security. In particular, national security remains the sole responsibility of each Member State.*" Therefore, EU law, including the Charter of Fundamental Rights of the European Union (hereafter: the Charter)[63], shall not apply to matters regarding the national security of Member States. This is an important exemption to the applicability of EU law and it is also particularly relevant for many of the questions raised in the present Working Document, since intelligence and security services are generally assumed to carry out their tasks in the light of the Member States' national security.

4.1.1. The absence of a clear definition of what is national security?

In short: the EU is not allowed to legislate on issues related to the national security of the Member States. There is however no clear definition of what is to be understood as 'national security' in EU legislation. On the contrary: the EU Treaties contain and refer to concepts which are very difficult to distinguish from national security, or at least are closely connected to it, and for which the EU is nevertheless competent to legislate.

First of all, Article 75 of the Treaty on the Functioning of the European Union (TFEU) provides in the chapter on the Area of Freedom, Security and Justice (AFSJ) for the competence of the EU to establish a framework for measures to prevent and combat terrorism and related crime. This provision raises the question of how the fight against terrorism can be

[61] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[62] In this chapter, if reference is made to the Directive, this should be read as including the national implementing legislation in the Member States, even if the implementing legislation is not explicitly mentioned.

[63] Offical Journal C 364 of 18 December 2000

distinguished from the protection of national security. Specific measures taken in the fight against terrorism further illustrate this.

The EU and its Member States cooperate closely with the United States when combating terrorism, for example by sharing financial transaction information to be analysed under the Terrorist Finance Tracking Program (TFTP). The scope of application of the underlying TFTP2 Agreement[64] includes the prevention, investigation, detection and prosecution of acts that would seriously destabilise or destroy the fundamental structures of a country. Furthermore, any leads derived from data shared by the EU under this program and relevant for the Member States' counterterrorism effort, are to be shared by the United States. In the view of the Working Party, processing of personal data for such purposes at least comes close to what would generally be understood to be a national security purpose and apparently can be subject to rules agreed upon by the EU.

Additionally, Article 24(1) TEU and article 2(4) TFEU provide that the Union's competence in Common Foreign and Security Policy (CFSP) matters "*shall cover ... all questions relating to the Union's security*". Therefore, "*the Union's security*" is within the scope of EU law and also needs to be distinguished from the national security of the Member States which falls – according to article 4(2) TEU – outside the scope of EU law.

On the level of secondary law, Article 3 of Directive 2000/31/EC[65] states that "*Member States may take measures to derogate ... in respect of a given information society service if the following conditions are fulfilled: (a) the measures shall be ... necessary for one of the following reasons: ... public security, including the safeguarding of national security and defense…".* A similar wording can be found in the data protection Directive 95/46/EC, Article 3(2), and first indent: "*This Directive shall not apply to the processing of personal data - in the course of an activity which falls outside the scope of Community law, ... and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law*". According to these provisions, the concepts of national security, State security, public security and defense all need to be distinguished from one another.

[64] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, 27 July 2010

[65] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

The CJEU case law has not provided a clear definition of 'national security' either. In the Promusicae case[66] the CJEU held that "*[these exceptions] concern, first, national security, defense and public security, which constitute activities of the State or of State authorities unrelated to the fields of activity of individuals…*"

AG Jacobs referred in his opinion in case C-120/94[67] to earlier case law of the European Court of Human Rights (ECtHR). The ECtHR stated that it "*falls in the first place to each Contracting State, with its responsibility for 'the life of [its] nation', to determine whether that life is threatened by a public emergency and, if so, how far it is necessary to go in attempting to overcome the emergency*".

In summary, neither the relevant provisions of EU law nor the CJEUs case law offer a clear definition of what 'national security' is. Moreover, the EU and its Member States use various rather similar notions related to security without defining them: internal security, national security, State security, public security and defense should all be distinguished, but are in the view of the Working Party inextricably linked. Whether or not something should be defined as falling under the national security exemption therefore cannot only be explained by strictly legal arguments. In reality, it appears to be necessary to take account of the political situation at the time the "choice" is made, as well as the relevant actors. What can be said is that, whereas activities by intelligence and security services are generally accepted as falling under the national security exemption, this is not always the case when general law enforcement authorities fulfill similar tasks.

The only institution able to provide more legal certainty on what should and what should not be regarded as falling under the national security exemption is the CJEU. Only the Court can further define the scope of Union law and – subsequently – the applicability of the Charter. Until the moment the Court has given a further clarification of the scope of the national security exemption, the Working Party expects Member States to adhere to the standing case law[68] requiring that recourse to the exemption needs to be justified in each case. For example, in the first Kadi judgement, the CJEU clearly stated that the obligations imposed by an international agreement cannot prejudice the principles of the EU Treaties, including the principle that all EU acts must respect fundamental rights.

---

[66] ECJ, Productores de Música de España (Promusicae) v Telefónica de España SAU (C-275/06, judgment of 29 January 2008), par. 51.

[67] Commission of the European Communities v Hellenic Republic; opinion of 6 April 1995, par. 55.

[68] Including C-387/05, European Commission v Italian Republic, judgment of 15 December 2009, § 45: "*It cannot be inferred that the Treaty contains an inherent general exception excluding all measures taken for reasons of public security from the scope of Community law. The recognition of the existence of such an exception, regardless of the specific requirements laid down by the Treaty, would be liable to impair the binding nature of Community law and its uniform application.*"

In the Rotaru v. Romania case[69], the ECtHR ruled similarly that the data collected has to be relevant to the national security purpose pursued and that, even in a national security context, the law should define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed and lay down limits on the age of information held or the length of time for which it may be kept. It should also contain explicit and detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained.

When assessing the applicability of the national security exemption, it should also be taken into account whether it is a general exemption that applies, as the one laid down in the Treaties and article 3(2) Directive 95/46/EC, or whether it is part of a provision excluding certain safeguards for reasons of national security. The latter is for example the case when allowing Member States to impose limits to the right of access of a data subject for reasons of national security, as provided by article 13(1)a Directive 95/46/EC.

4.1.2. The national security interest of a third country

The analysis presented so far referred to the understanding of the national security exemption in the relationship between the European Union and the Member States. In this context, national security serves as a means to distinguish the Union's competences from the Member States' competences. However, the fact that national security activities of the Member States are excluded from the scope of application of EU law does not mean that EU law ceases to apply where data subject to EU data protection law is accessed by third countries in the name of the national security of such third countries.

The Working Party understands article 4 TEU as an attempt to define the competences of the Union vis-à-vis the Member States. Member States insist upon their sovereignty when it comes to their national security. This, however, is different from the obligation to comply with EU data protection law weighing on controllers even where they are subject to national security legislation of a third country. Therefore, the Working Party points out that the national security exemption has to be interpreted to reflect the competence of the EU vis-à-vis the Member States and not as a general exemption from EU data protection requirements of all activities requested by third countries in the name of national security.

[69] See in particular paragraph 53 to 63 of ECtHR, Rotaru v. Romania judgment , 4 May 2000, accessible at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#{%22itemid%22:[%22001-58586%22]} (last visited 20 November 2014).

Additionally, the Working Party takes the view that it is important to critically assess whether surveillance is actually conducted for the purpose of national security. It should be noted that, while e.g. the disclosed US surveillance activities may first be seen as aimed at protecting national security, it seems, in reality, that the interests covered are much wider. For example, the FISA Act allows for interceptions as soon as the information '*relates to (...) the conduct of the foreign affairs of the United States'.*[70] It is very much questionable that any definition of the national security exception in EU instruments, even stretched beyond its original scope, could cover such a broad purpose. In addition, the Working Party notes the very thin line separating the national security purpose from law enforcement purposes, as the involvement of different agencies (such as the FBI, the CIA and the NSA) in the US surveillance programs also indicates. Respect for the principle of purpose limitation is therefore essential.

The Working Party is concerned that EU (data protection) law may be circumvented in practice with a mere reference to the data processing being needed for national security purposes.[71] This is a dangerous development, certainly if it is not the national security of a Member State which is at stake, but the alleged national security of a third country. The Working Party stresses that the exemption in the treaties offers no possibility to invoke the national security of a third country alone in order to avoid the applicability of EU law.

It should nevertheless be noted that a Member State may claim that a threat to the national security of a (partner or ally) third country also forms a part of this Member State´s own national security, thus making EU law inapplicable. The Working Party acknowledges that there may be areas where a national security interest of an EU Member State and that of a third country co-exist and that, in such cases, the boundaries of an EU Member State's national security may not always be clear. The claim that the national security interest of a third country aligns with an EU Member States' own national security interest should only be accepted if it is properly justified to the relevant authorities on a case-by-case basis. If the Member State fails to do so, it shall comply with EU law. This reasoning is supported by the CJEU judgment in the European Commission v Italian Republic where it said that the mere invocation of the national security exemption is not sufficient to declare that EU law is not applicable.[72] This must be even more the case when a Member State claims a third country's national security interest forms part of its own. Therefore, the legal basis for claiming a third country's national security interest must be clearly set out in national law, including, where

[70] 50 U.S. Code § 1801, paragraph (e)(2)(B)

[71] It should be recalled that following case law from the CJEU, including ZZ v Secretary of State (C-300/11), any limitation to a fundamental right must in particular respect the essence of the fundamental right in question and requires, in addition, that, subject to the principle of proportionality, the limitation must be necessary and genuinely meet objectives of general interest recognised by the European Union (§52) and be subject to judicial review (§58).

[72] C-387/05, § 45 (cited)

relevant, international legally binding political agreements entered into by Member State governments[73].

4.2. Legislating data protection

Article 16(1) of the TFEU lays down the right to the protection of personal data, which applies to "everyone".

In order to implement this right, Article 16(2) provides a new legal basis for the adoption of EU data protection legislation with regards to processing by EU institutions and bodies and by Member States when carrying out activities which fall within the scope of Union law, as well as the rules relating to the free movement of such data. It also requires that independent authorities control compliance with these rules.

Declaration 21 states that in the fields of judicial cooperation in criminal matters and police cooperation, specific rules may be necessary. However, these rules will also be adopted on the basis of Article 16 of the TFEU.

As regards national security, Declaration 20 states that whenever rules on data protection adopted on the basis of Article 16 could have direct implications for national security, the specific characteristics of the matter should be taken into account. It also recalls that the currently applicable legislation, in particular, Directive 95/46/EC, includes specific derogations in this regard.

4.3. The EU Charter of Fundamental Rights

4.3.1. The scope of the EU Charter

As a result of the national security exemption addressed above and contrary to Council of Europe instruments, the scope of application of the Charter is limited. Still, as far as national security of EU Member States is not concerned, the principles enshrined in the Charter, in particular in Articles 7 and 8, apply to EU institutions and bodies and all the activities of Member States when they implement Union law.

[73] The Article 29 Working Party is aware that there are also provisions in some existing international legally binding instruments e.g. MLATs which allow EU Member States to derogate from such instruments but this is only permissible where this would prevent prejudice to that Member State's essential interests (and not the essential interest of another third country that is not party to the instrument). The emphasis is on the EU Member State to clearly justify its own essential interests.

4.3.2 The rights to respect for private life and data protection in the Charter

Article 7 of the Charter, which is similar to Article 8 of the European Convention on Human Rights (ECHR), provides for a general right to respect for private and family life, home and communications, and protects the individual against interference by public authorities. Article 8(1) lays down the right of anyone to the protection of personal data concerning him/her: his or her personal data can only be processed if certain essential requirements are fulfilled. These essential requirements are laid down in article 8(2) and (3) of the Charter which specify that such data must be processed "*fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*". It also provides for the individual's rights of access to and rectification of his/her data and subjects compliance with these rules to the control of an independent authority.

In the judgment which annulled the Data Retention Directive[74], the CJEU maintained that "*the obligation (…) to retain, for a certain period, data relating to a person's private life and to his communications (…) constitutes in itself an interference with the rights guaranteed by article 7 of the Charter. Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right. (…) Likewise, [data retention] constitutes an interference with the fundamental right to the protection of personal data guaranteed by article 8 of the Charter because it provides for the processing of personal data.*"[75] The Court furthermore argues that since, amongst others, no limitations to both storage and access to the telecommunications data are provided for in the legislation and limited rights for individuals have been foreseen, the data retention directive "*entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.*"[76]

Even though the data retention case relates to a matter of law enforcement, the reasoning of the Court is of great importance, especially for those programmes where the purpose of the data processing includes the fight against terrorism and/or serious crime (both of which have been considered as being part of the competence of the European Union[77]). In other words, to be considered compliant with the EU data protection legal framework, these programmes have to be precisely circumscribed by provisions that ensure that they are actually limited to what is strictly necessary. Article 52(1) of the Charter specifies these safeguards.

---

[74] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[75] See CJEU, Digital Rights Ireland and Seitlinger and Others (Joined Cases C-293/12 and C-594/12), 8 April 2014, para. 34-36.

[76] Idem, para. 64

[77] See section 4.1.1.

4.3.3 The scope of restrictions to the fundamental rights to respect for private life and data protection

Article 52(1) of the Charter allows for limitations on the exercise of the rights and freedoms recognised by the Charter, but only if those limitations:

- are necessary and proportional,
- genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others,
- are provided for by law,
- and respect the essence of the rights and freedoms in question.

In the ZZ v. Secretary of State for the Home department case, the CJEU recalled that, "*whilst Article 52(1) of the Charter admittedly allows limitations on the exercise of the rights enshrined by the Charter, it nevertheless lays down that any limitation must in particular respect the essence of the fundamental right in question and requires, in addition, that, subject to the principle of proportionality, the limitation must be necessary and genuinely meet objectives of general interest recognised by the European Union*".[78]

In addition, it confirmed that it has to be demonstrated that the specific limitation in question is actually necessary to safeguard State security: the mere fact that a Member State invokes such exemption is not sufficient: "*The competent national authority has the task of proving, in accordance with the national procedural rules, that State security would in fact be compromised by precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision taken (...). It follows that there is no presumption that the reasons invoked by a national authority exist and are valid.*"[79]

And, even if the need for such limitation is demonstrated, this does not allow for blanket derogation to the obligation to respect fundamental rights: "*If it turns out that State security does stand in the way of disclosure of the grounds to the person concerned, judicial review (...) must (...) be carried out in a procedure which strikes an appropriate balance between the requirements flowing from State security and the requirements of the right to effective judicial*

[78] See ECJ, ZZ v. Secretary of State for the Home department, Case C-300/11, 4 June 2013, para. 51.

Moreover, in the Unitrading case, the CJEU provided that national provisions shall not "render in practice impossible or excessively difficult the exercise of rights conferred by Community law (principle of effectiveness)" CJEU, Unitrading ltd v. Staatssecretaris van Financiën, Case C-437/13, 23 October 2014

[79] Idem, para. 61.

protection whilst limiting any interference with the exercise of that right to that which is strictly necessary."[80]

4.3.4. Interaction between the Charter and the ECHR

The scope of the EU Charter and the ECHR are not identical: as explained above, EU Member States' national security is excluded from the scope of application of EU law, including the Charter, while the ECHR obliges its Parties to secure to everyone within their jurisdiction a series of rights and freedoms, including the right to respect for private life and does not contain a general exemption for national security matters. However, the ECHR still allows Member States to interfere with the exercise of the right to respect for private life in accordance with their national law, as long as this measure is necessary in a democratic society in the interests of national security.

Article 52(3) of the Charter specifies that where rights contained in the Charter correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same as those laid down by the ECHR. The fundamental principles developed under both texts are therefore fully consistent. It also specifies that this provision does not prevent Union law from providing more extensive protection.

4.4. Directive 95/46/EC[81,82]

4.4.1. Scope of application of the Directive

Directive 95/46/EC does not apply to "*processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law*". This limitation of scope is laid down in Article 3(2) of the Directive. It reflects the division of competences between the EU and the Member States, in particular before the entry into force of the Lisbon Treaty. The Directive should however not be considered irrelevant in the context of law enforcement and national security matters. To the contrary: whereas it does not regulate data processing by the law enforcement authorities and the intelligence services, the national laws implementing the Directive do govern the transmission of personal data from data controllers and processors when they are ordered to submit information to

[80] *Idem,* para. 64.

[81] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[82] In this chapter, if reference is made to the Directive, this should be read as including the national implementing legislation in the Member States, even if the implementing legislation is not explicitly mentioned.

intelligence services and law enforcement authorities. Article 13 of the Directive allows – under certain conditions – the national legislator to enact legislative measures restricting certain rights and obligations, thus for example allowing for the change of purpose of the data processing.

As explained in section 4.1, the national security exemption refers to the national security of EU Member States, which "*remains the sole responsibility of each Member State*"[83]. Therefore, if the processing concerns the national security of a third country but not that of the EU or of the EU Member States, the Directive is not precluded. It will apply, provided any of the applicable law criteria described below is fulfilled and, subsequently, data controllers will be expected to comply and may be subject to enforcement actions.

With regard to its personal/territorial scope of application, Article 4(1) provides that national laws implementing the Directive apply to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of an EU Member State;

The Working Party opinion on applicable law gives several criteria to help to identify what a relevant establishment is. It insists on a functional approach, taking into account the context of the activities of the establishment and its degree of involvement in the processing of personal data, rather than the location of the data or of the controller.[84] The CJEU has further specified that Article 4(1)(a) of the Directive does not require that "*the processing of personal data in question be carried out 'by' the establishment concerned itself*"[85]. The Court also considers that this provision cannot be interpreted restrictively, in light of the objective of the Directive of "*ensuring effective and complete protection of the fundamental rights and freedoms (...)*"[86].

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

c) the controller is not established in the EU but, for purposes of processing personal data makes use of equipment[87], automated or otherwise, situated on the territory of an EU Member State (unless such equipment is used only for purposes of transit through the territory of the Community).

[83] Article 4(2) TEU

[84] WP29 Opinion 8/2020 of 16 December 2010 on applicable law.

[85] CJEU, *Google v. Spain,* 13 May 2014, para. 52.

[86] *Idem,* para. 54.

[87] The WP29 opinion on applicable law, cited above, provides further guidance on the notion of equipment.

In that case, Article 4(2) requires the controller to designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

The Working Party welcomes the fact that the territorial scope of application of EU data protection legislations will be more explicitly defined under the proposed General Data Protection Regulation: indeed, Article 3(2) of the European Commission's proposal[88] states that the Regulation will apply to the processing of personal data by a controller which is not established in the Union but where the processing activities are related to (a) the offering of goods or services to such data subjects in the Union or (b) the monitoring of their behaviour.

Although the proposal is currently under discussion by the European Parliament and the Council of the EU, both co-legislators broadly agree on the scope of application proposed by the Commission. The Council of the EU has explicitly supported the territorial scope of the proposed Regulation and has highlighted the need to broadly ensure the application of Union rules to controllers not established in the EU when processing personal data of Union data subjects[89]. The European Parliament has also supported the proposed scope and even broadened it.[90]

In its 2009 data retention ruling, the CJEU ruled that Article 95 of the former EC Treaty (approximation of laws in the internal market) was the valid legal basis to impose a data retention obligation. In its reasoning, the Court considered that Directive 2006/24/EC covered the activities of service providers in the internal market, amended their data protection obligations[91], had significant economic implications for those providers and did not contain rules governing the activities of public authorities for law-enforcement purposes. The argument brought forward by Ireland that the obligation could only be imposed acting under Title VI of the former EU Treaty (justice and home affairs), was rejected.

In the data retention case the compulsory retention of personal data by service providers, even if it had a law enforcement purpose, was a processing subject to national laws implementing

[88] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[89] Council of the European Union, Press release, 3319th Council meeting Justice and Home Affai´rs, 5-6 June 2014 and document 2012/0011 (COD).

[90] European Parliament, legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[91] Laid down by Directive 2002/58 (the e-Privacy Directive).

EU data protection rules (in particular, the e-Privacy Directive[92]). The data retention Directive was therefore a specific derogation of some provisions of the e-Privacy Directive[93].

Similarly, national laws implementing Directive 95/46/EC apply to the processing of data by private parties for commercial purposes, including to the transfer from such private parties. They also apply to the processing by EU Member States' public authorities covered by the Directive, i.e., not excluded by Article 3(2).

The Court also specified that this situation could not be compared to the context of the judgment of the Passenger Name Records (PNR) case[94]. It argued that "*unlike Decision 2004/496 [annulled by the PNR judgment], which concerned a transfer of personal data within a framework instituted by the public authorities in order to ensure public security, Directive 2006/24 covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law enforcement purposes*".

In addition, unlike the recently annulled data retention directive, EU PNR agreements contain data protection safeguards[95] addressed to public authorities processing these data. Such safeguards have been deemed 'adequate' by the Council of the EU[96], although the Article 29 Working Party and the European Data Protection Supervisor did not consider them sufficient[97].

All of this goes to show that if law enforcement requires personal data to be transferred by private companies, the general data protection legal framework will continue to apply until the moment the transfer has taken place. For intelligence services, in many Member States the situation will be different, since they are not subject to the general data protection legislation.[98] Nevertheless, it should be clear that also for transfer of personal data to intelligence services as well as for the collection of personal data by them, an appropriate legal basis needs to be in place.

---

[92] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[93] In particular, of Articles 5, 6 and 9 of Directive 2002/58/EC.

[94] CJEU, Joined Cases C-317/04 and C-318/04, European Parliament v Council of the European Union and Commission of the European Communities, 30 May 2006.

[95] Considered adequate by the Council of the EU but criticised by

[96] See e.g., Article 19 of the current EU-US PNR Agreement (Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, 2011).

[97] See EDPS and Article 29 Working Party Opinions on the PNR agreements, available on www.edps.europa.eu and on http://ec.europa.eu/justice/data-protection/article-29.

[98] WP215 (cited), p. 9

4.4.2. The data protection principles of Directive 95/46/EC

Where a processing activity falls within the scope of the Directive, the data protection principles, rights and obligations that it lays down have to be respected and complied with:

- Principles relating to data quality: according to Article 6 of the Directive, controllers[99] have to ensure that personal data must be (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; and (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed[100].

- Criteria for making data processing legitimate: Article 7 states that personal data may be processed only if (a) the data subject has unambiguously given his consent; or if the processing is necessary for (b) the performance of a contract; (c) compliance with a legal obligation to which the controller is subject; or (d) to protect the vital interests of the data subject; (e) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed (except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject).

- Sensitive data: Article 8 prohibits in principle the processing of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life), unless some exceptions apply[101]. It also subjects the processing of data relating to offences, criminal convictions or security measures to additional safeguards.

- Transparency: Articles 10 and 11 specify the information to be given to the data subject in cases of collection of data from the data subject and where the data have not been obtained from the data subject. According to Article 18, controllers are also obliged to notify any processing activities to data protection authorities[102]. Article 21 provides for the publication of the register of notified processing operations.

---

[99] Article 6(2) of the Directive.

[100] Article 6(1) of the Directive.

[101] Laid down in Article 8(2-3).

[102] See also Article 19.

• Rights of the data subject: Articles 12 and 14 regulate the rights of access to, rectification, erasure and blocking of the data as well as the right to object to the processing.

• Automated individual decisions: Article 15 aims to protect the data subject from certain profiling activities and lays down the right not to be subject to a decision which produces significantly affects him/her or produces legal effects on him/her if such decision is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

• Confidentiality and security of processing: Articles 16 and 17 specify the obligations of controllers and processors to respect the confidentiality of the processing and to implement implement appropriate technical and organisational security measures.

The Directive also provides for supervision by independent data protection authorities of compliance with these rights and obligations and for administrative and judicial redress.

4.4.3. Exceptions to the data protection principles

According to Article 13(1), EU Member States may adopt legislative measures to restrict the scope of the obligations and rights provided by the principles of data quality and transparency and of the rights of access, rectification, erasure and blocking if such a restriction constitutes a necessary measures to safeguard (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); or (g) the protection of the data subject or of the rights and freedoms of others.

Contrary to the general exemptions from the scope of application of the Directive laid down in its Article 3(2), the derogations to specific principles, rights and obligations provided by Article 13(1) or included in other provisions of the Directive[103] assume that the Directive applies in principle to the processing in question. As explicitly required by the Directive[104], such exceptions should then be laid down by Member State's laws, which in many cases also need to provide additional safeguards[105].

[103] *Idem*

[104] See e.g., Article 13(1) and 13(2), which requires a Member State's legislative measure.

[105] See e.g., Article 13(2).

4.5 The e-Privacy Directive

The e-Privacy Directive is closely linked to Directive 95/46/EC as far as the application of the general data protection principles is concerned. This Directive provides for additional safeguards aiming at protecting electronic communications. Its scope is however limited to providers of publicly available electronic communications services.

Article 5(1) of Directive 2002/58 protects the confidentiality of communications as follows: "*Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).*"

A scenario that may trigger the application of Article 5(1) has been described by the press in the context of the Snowden revelations: where intelligence services obtain access to the servers of a communications service provider subject to the ePrivacy Directive through a loophole in the security of this provider's systems (most likely with the provider's cooperation on a confidential basis). The intelligence services could have access to all data arriving and leaving the servers in the extreme case of this scenario.[106]

It could be argued that, by *not outlawing* (or not providing effective oversight to effectively enforce against) such access, (1) Member States are not complying with the obligation to ensure confidentiality imposed on them by the ePrivacy Directive, and (2) providers of publicly available electronic communications services are not complying with national law implementing the requirement of confidentiality of the Directive.

In addition, Articles 6 and 9 of the ePrivacy Directive protect traffic data and location data (other than traffic data), and provide for their immediate deletion or anonymisation, except in specific cases relating especially to billing or marketing purposes, under strict safeguards.

Other forms of processing or transfer of communications and related traffic data to third parties would therefore be illegal under the ePrivacy Directive, except under Article 15(1). According to this provision, strict conditions must be met to any possible limitation to the confidentiality principle ensured by Article 5 and 6: "*any restriction to the confidentiality of communications data must constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC*".

[106] Similar facts in the Belgacom case led the Belgium data protection authority to open an investigation.

These strict conditions have to be interpreted in light of the 2014 CJEU judgment in the data retention case, which stated that such interference needs to be "precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[107] Access and use by national competent authorities should be limited to what is strictly necessary in terms of categories of data and persons concerned, and subject to substantive and procedural conditions. Moreover, national laws should provide for effective protection against the risk of unlawful access and any other abuse, including the requirement that the storage of the data is subject to the control of an independent authority ensuring compliance with EU data protection law.

As already stated, exceptions for national security purposes are valid within the EU framework, for Member States' national security purposes, under strict requirements. They cannot justify interception, access or requests of personal data performed by a third country's public authority, albeit under a national security requirement of that third country.

• 5. Transfer regime following Directive 95/46/EC

The exact functioning of surveillance programmes around the world is not yet fully known. Further facts providing a clearer picture of these programmes may still emerge. However, it is reasonably foreseeable that the third country surveillance authorities only seem to obtain access to data after an international transfer from a company in the EU to another company outside the EU took place.

Such transfers will have to be framed through one of the transfer tools provided for in the Directive 95/46/EC and the foreign entity will thus have to comply with its commitments whenever it receives a request to disclose data or give access to it. This is why it appears necessary to analyse the specific provisions of the transfer tools that might be relevant when a third country surveillance authority is getting access or requesting data that have originally been transferred from the EU.

This part of the Opinion will firstly address the existing legal framework for the international transfers and will then analyze the specific provisions applicable to different scenarios.

Directive 95/46/EC does not provide for any definition of data transfer. However, according to the European Data Protection Supervisor, "it can be assumed as a starting point, that the term is used in its natural meaning, i.e. that data "move" or are allowed to "move" between different users".[108] He further adds in relation to Regulation 45/2001 that "controllers should consider that this term would normally imply the following elements: communication, disclosure or otherwise making available of personal data, conducted with the knowledge or

[107] Cited above, para 65

[108] EDPS Position Paper, The transfer of personal data to third countries and international organisations by EU institutions and bodies, 14 July 2014, p.6

intention of a sender subject to the Regulation that the recipient(s) will have access to it. The term would therefore cover both "deliberate transfers" and "permitted access" to data by recipient(s)".[109]

5.1. Adequate level of protection

As any processing, a transfer should in the first instance comply with the aforementioned principles of the data protection legislation. Subsequently, according to Article 25 of the Directive, the recipient also has to offer an adequate level of protection.

Article 25(2): Third Country Adequacy including Safe Harbor: Article 25 Directive 95/46/EC prohibits all transfers from the European Union, unless a third country provides an adequate level of data protection. If the European Commission takes a decision recognising the third country indeed has such an adequate level of data protection, transfers can take place without further restrictions. In fact this means transfers to the said third country will be treated the same as data exports to another EU Member State.

The Commission has for example already found that in the case of the United States, the Safe Harbor Agreement provides for an adequate level of protection for commercial data transfers from the European Union to US companies having joined this scheme. However, this instrument was not designed to offer an adequate level of protection for the purposes of law enforcement, contrary to other agreements e.g. on the use and transfer of Passenger Name Records (PNR) between the EU and US providing the framework for the exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime[110].

Article 26(2): Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCR): Besides Safe Harbor and pursuant to Article 26(2) of the Directive, transfers from the EU to a third country may also be authorised where the data controller offers "*adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights*". These safeguards may result from "*appropriate contractual clauses*" (e.g. the European Commission's decisions on standard contractual clauses from a data controller to another data controller / from a data controller to a data processor). In addition, since 2003 the Working Party has been developing the Binding Corporate Rules for the authorisation of transfers within a group of companies.

Article 26(1): Derogations to the rules on data transfers: Article 26(1) of the Directive provides that a transfer to a third country which does not ensure an adequate level of protection is possible only if justified by one of the conditions listed in the Article, including

[109] Idem, p. 7

[110] These agreements were negotiated after the annulment of the adequacy decision adopted by the Commission in 2004 in order to allow the transfer of those data.

where "*the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims".*

The Working Party has already developed guidance on the application of Articles 25 and 26 Directive 95/46/EC in its Working Document on transfers of personal data to third countries: applying Articles 25 and 26 of the EU Data Protection Directive.[111] In the Working Party's later paper WP114, the guidance stated that exemptions to the general principle should be interpreted restrictively, including where public interest is concerned[112]. This includes where foreign public authorities are concerned. WP114 states: *"the drafters of the Directive clearly did envisage that only important public interests identified as such by the national legislation applicable to data controllers established in the EU are valid in this connection."*[113]

The use of these derogations implies that the data do not benefit from the protection of the Directive once they are transferred. This is the reason why according to the jurisprudence of the ECtHR they have to be interpreted restrictively (see section 3.2.1.3) and the Working Party recommends that "*transfers of personal data which might be qualified as repeated, mass or structural should, where possible, be carried out within a specific legal framework (i.e. contracts or BCR)".*[114] In any case, the Working Party considers that recourse to the derogation of article 26(1) should, of course, never lead to a situation where fundamental rights might be breached.

5.2. Specific instruments used to demonstrate adequacy or adduce adequate safeguards in accordance with Directive 95/46/EC

5.2.1. The Safe Harbor agreement

Through the Commission decision on Safe Harbor[115], the Safe Harbor principles are considered adequate in the meaning of article 25(2) of Directive 95/46/EC. Therefore,

[111] Article 29 Working Party, WP12, Working document on Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive, 24 July 1998

[112] Article 29 Working Party, WP 114, Working documents on a common interpretation of Article 26(1) of directive 95/46/EC, 24 October 1995, p.7

[113] Article 29 Working Party, WP 114, Working documents on a common interpretation of Article 26(1) of directive 95/46/EC, 24 October 1995, p.15

[114] Article 29 Working Party, WP114, Working documents on a common interpretation of Article 26(1) of directive 95/46/EC, 24 October 1995, p. 9

[115] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441).

compliance with and adherence to the Safe Harbor principles can be used as a basis for transfers and it is respected by a wide range of US organisations[116] which have self-certified their adherence to these as a basis for transfers from the EU.

Concerning Onward Transfers, the Safe Harbor provides that "*to disclose information to a third party, organisations must apply the Notice and Choice Principles*". In other words, when communicating data to a third party acting as a controller[117], the company based in the US and acting as a controller[118]shall inform the data subject about the onward transfer to the third party, offering the opportunity to the data subject to consent (opt-out) to such onward transfer where data is to be used for "a *purpose incompatible with the purpose(s) for which it was originally collected*".

Safe Harbor allows for a limitation of adherence to the Principles "*to the extent necessary to meet national security, public interest, or law enforcement requirements; by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or if the effect of the Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts."*[119]

The level of protection provided by the Safe Harbor has been questioned ever since its creation process. In particular the implementation of the Safe Harbor has been strongly criticized. In its recent Communication on the functioning of the Safe Harbor, the European Commission has addressed the issue of mass surveillance in relation to the Safe Harbor scheme and reported that "*The large scale nature of these programmes [US Surveillance programmes] may result in data transferred under Safe Harbor being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in the Safe Harbor Decision."*[120]

---

[116] The scope of the Safe Harbor is limited, not all organisations can adhere to it.

[117] If the organization wishes to make onward transfers to an entity acting as a processor, it does not need to apply the notice and choice principle. The organization must however ascertain that the third party acting as a processor either is a member of the Safe Harbor or is subject to the Directive or another adequacy finding or enters into a written agreement providing at least the same level of privacy protection as required in the Safe Harbor. However, it should be kept in mind that in the case of surveillance the third country intelligence authority can only be considered as a controller.

[119] This provision is further explained in Annex IV of the Safe Harbor decision : "Explicit Legal Authorizations"

[120] COM(2013) 847 Communication from the Commission to the European Parliament and the Council on the functioning of the safe Harbor from the perspective of EU citizens and companies established in the EU, 27 November 2013, p. 17

Moreover, the Commission added that companies do not systematically indicate in their privacy policies when they apply exceptions to the Principles. The individuals and companies are thus not aware of what is being done with their data.

The European Commission concluded that *"due to deficiencies in transparency and enforcement of the arrangement, specific problems still persist and should be addressed:*

a) transparency of privacy policies of Safe Harbor members,

b) effective application of Privacy Principles by companies in the US, and

c) effectiveness of the enforcement.

Furthermore, the large scale access by intelligence agencies to data transferred to the US

by Safe Harbor certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the US."[121]

The European Commission made 13 recommendations, including the following two which address access by US authorities:

- Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbor. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.

- It is important that the national security exception foreseen by the Safe Harbor Decision is used only to an extent that is strictly necessary or proportionate.

In a letter dated 10 April 2014[122], the Working Party publicly supported the European Commission's recommendations, including those on access by US authorities; and pointed out some additional elements that should be improved in the Safe Harbor Decision. The improvements to the Safe Harbor that will be made by the US in the upcoming months need to be sufficient to restore trust. The Working Party recognises that if the revision process currently undertaken by the European Commission does not lead to a positive outcome, then the Safe Harbor agreement should be suspended. In any case, the Working Party recalls that

[121] idem, pp. 17-18

[122] Letter from the Article 29 Working Party to Vice-President Viviane Reding on the actions set out by the European Commission in order to restore trust in data flows between the EU and the US

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf (last visited 20 November 2014).

data protection authorities may suspend data flows according to their national competence and EU law. The Working Party is also awaiting the outcome of the Max Schrems case which has recently been referred by the Irish High Court to the CJEU on the role of the data protection authorities in relation to Safe Harbour suspensions[123].

5.2.2. Standard Contractual Clauses (SCC)

The 2001 and 2004 SCC contain a list of the data protection principles that should be respected whenever processing data, including when transferring them. These principles are, *inter alia*, the purpose limitation principle, the transparency principle, the security and confidentiality principle, the rules on onward transfers, the right of access, deletion and opposition.

According to the 2010 SCC, the non-EU data importer shall process the personal data only on behalf of the data exporter and in compliance with its instructions. Considering that the EU data exporter is subject to the obligations of the Directive, his instructions will necessarily respect the data protection principles of the Directive. Moreover, the non-EU data importer is not allowed to transfer data unless the EU data exporter requests him to do so.

The SCC also includes rules in case of conflict of laws. For example, in the 2001 and 2004 SCC the Data Importer agrees and warrants "*that he has no reason to believe that the legislation applicable to him prevents him from fulfilling his obligations under the contract and that in the event of a change in that legislation which is likely to have a substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the Data Exporter and to the Supervisory Authority where the Data Exporter is established, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract*".

The 2010 SCC stipulate that the importer agrees "*to process the personal data on behalf of the data exporter and in compliance with its instructions and the clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data/or terminate the contract*." In addition, the clauses specify that the data importer shall promptly notify the data exporter about "*any legally binding request for disclosure of the personal data by a law enforcement authority*". However, that notification does not apply when it is prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

As it has already been established, the massive, indiscriminate and secret access to personal data is considered disproportionate to the aim/purpose pursued. This is the determining factor in the assessment of the lawfulness of the processing. In this context, and considering the recent revelations on the US surveillance programmes, there could be grounds for considering

[123] Schrems v. Data Protection Commissioner, C-362/14 (Irish case reference 2013 No. 765JR: [2014] IEHC 351)

that the US legislation prevents the importer from fulfilling his obligations under the contract and that the exporter could suspend the transfer of data/or terminate the contract. It is up to the data controller to assess the future status of the transfer. The same reasoning would apply to any similar situation in another third country.

Finally, all sets of SCC contain derogations according to which the clauses shall apply subject to the mandatory requirements of the national legislation of the EU Member State applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC[124], that is if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others.[125]

5.2.3 Binding Corporate Rules (BCR)

Similarly to the SCC, BCR for controllers and BCR for processors shall contain all the data protection principles that need to be respected when processing data, including where a transfer takes place to another member of the group.[126]

- **BCR Controller**: According to WP 74 and WP 153, the BCR for controllers shall contain a clear commitment that where a member of the corporate group has reason(s) to believe that the legislation applicable to it prevents the corporate group as a whole from fulfilling its obligations under the BCR and has substantial effect on the guarantees provided by the rules, it will promptly inform the EU headquarters or the EU member of the corporate group with delegated data protection responsibilities or the other relevant privacy function

[124] That is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others.

[125] Commission Decision 2010/87/EU of 5 February 2010, Article 4

[126] See the Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (WP74), adopted by the Article 29 Working Party on 3 June 2003, here after 'WP74'; the Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules (WP108), adopted by the Article 29 Working Party on 3 June 2003, here after 'WP108'; the Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (WP133), adopted by the Article 29 Working Party on 10 January 2007, here after 'WP133'; the Working document setting up a table with the elements and principles to be found in Binding Corporate Rules (WP153), adopted by the Article 29 Working Party on 24 June 2008, here after 'WP153'; the Working document setting up a framework for the structure of Binding Corporate Rules (WP154), adopted by the Article 29 Working Party on 24 June 2008, here after 'WP154'; the Working document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules (WP155), the Article 29 Working Party on 24 June 2008, as last revised and adopted on 8 April 2009, here after 'WP155'; Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities (WP195) – all documents are available on the website of the Working Party

(except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

In addition, the BCR shall also contain a specific commitment that, where there is a mandatory requirement of the national legislation of the data recipient applicable to the members of the corporate group, presenting a difference between a national law and the commitments in the BCR, the EU headquarters, the EU member with delegated data protection responsibilities or the other relevant privacy function will take a responsible decision on what action to take, and will consult the competent data protection authorities. Furthermore, any incidences relating to these requirements have to be detailed and reviewed by regular audits as provided in the BCR.

BCR Processor: opinion WP195 states that any legally binding request for disclosure of the personal data by a law enforcement authority shall be communicated to the data controller unless otherwise prohibited, e.g., a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. In any case, the request should be put on hold and the data protection authority competent for the controller and the lead DPA for the BCR should be clearly informed about it. Each DPA takes action according to its accepted national law and practice.

Moreover, Opinion WP195 provides that the different members of the group adopting the BCR shall make a clear commitment that where a member of the BCR has reasons to believe that the existing or future legislation that it is subject to may prevent it from fulfilling the instructions from the data controller, or its obligations under the BCR or service agreement, then the following will apply: it will promptly notify this to:

- the data controller which is entitled to suspend the transfer of data and/or terminate the contract,
- the EU headquarter processor or EU entity member with delegated data protection responsibilities,
- or the other relevant Privacy Officer/functions, and
- also to the DPA competent for the controller.

5.3. Conclusion on data transfers

Massive, indiscriminate and secret access to personal data originally processed under EU jurisdiction and transferred from the EU to a third country where it is then able to be accessed for that third country's surveillance programmes does not fulfill the requirements of the data transfer provisions of Directive 95/46/EC. Structural (bulk) transfers by data controllers under

EU jurisdiction are subject to EU legislation – and this is including onward transfer to other parties in the recipient country which can only take place by fulfilling the provisions of the Directive and the various available transfer instruments. However, none of these foresee transfers of personal data held by private sector data controllers to public sector authorities of third countries for surveillance purposes. More generally, it was never envisaged to make use of the same instruments in the public sector, and especially for the transfer of information related to law enforcement authorities' activities. [127]

As a result, third countries' public authorities – including law enforcement authorities and intelligence agencies – wishing to access data stored in an EU Member State or otherwise under EU jurisdiction, have to request mutual legal assistance to the national competent authorities through existing official channels such as, where relevant, Mutual Legal Assistance Treaties. These instruments need to take into account data protection principles.

In exceptional cases, individual transfers can be based on the derogations contained in the Data Protection Directive (Articles 13 and 26(1)) or in the third country national law, in the case of countries which have been considered as providing an adequate level of protection in the private sector. The instruments examined above (BCR, Safe Harbor, SCC) also contain exceptions. However, such exceptions are restrictions to a fundamental right and as such should be interpreted restrictively. They could not be a basis for massive, structural or repetitive transfers.

In any case, access by third countries' authorities to transferred personal data for law enforcement purposes – let alone for surveillance purposes – can only be limited in scope. These exceptions could therefore not apply to an unlimited number of cases or persons, as this would be contrary to the principle of proportionality at the heart of EU rules, and contained in article 8 ECHR.

It is also worth recalling that the EU-US Ad Hoc Working Group on Data Protection has confirmed in its report that, while there are many legal bases in US legislation authorising a massive collection of personal data gathered and processed by US companies, these do not respect the criteria of necessity and proportionality laid down by the European Convention on Human Rights. It furthermore confirms that the massive character of these programmes is likely to lead to access and processing that go beyond what is considered as strictly necessary and proportionate.

[127] Since assessments of adequacy require analysis of the application of the rule of law in a third country, this takes at least limited account of public sector characteristics (although it cannot be said that a full adequacy assessment is realistically able to be made for a third country's entire public sector). This is partly why less emphasis was placed on considering the public sector when designing the transfer instruments.

5.4. Examples

The following chapter will illustrate, on the basis of various scenarios, some of the different possible transfers that could take place, in principle irrespective of the question to what third country the data are transferred.

It is obvious that not all possible scenarios can be dealt with in this Working Document. Moreover, the legal framework circumscribing the manifold scenarios is very complex. In order to assess the legality of third country authorities' requests for legal assistance and in terms of the need to ensure that the recipient provides appropriate data protection safeguards it is particularly important whether the data controller is subject to EU data protection law.[128] With regard to the applicability of EU data protection law, however, it is not the location of the data which matters but whether the controller has an establishment in the EU or makes use of equipment in the EU and the data is processed in the context of activities of that establishment. With regard to the applicability of the law of the third countries authorising the collection of data, a number of scenarios are possible which involve conflicting laws (between EU law and the law of that third country), depending on how far that third country extends its jurisdiction.

The answers to these questions are often complex and may yet need further discovery of facts and clarifications of the law, e.g. for the concept of 'transfer'. Thus, the Working Party has reduced the level of complexity for the purpose of this paper.

Example 1: A direct transfer / direct access from an EU private entity to a non-EU public authority

The Working Party firstly recalls that public international law and national law apply fully to these scenarios[129]. Direct transfers of personal data by a private entity from the EU to a public authority of a third country or direct access by a public authority of a third country to these personal data must comply with those legal orders.

In its letter addressed on 5 December 2013 to the Cybercrime Committee of the Council of Europe[130], the Working Party already insisted that the procedure foreseen under Article 32(b)

---

[128] See Directive 95/46/EC, Art.4.

[129] See in particular Article 2(1) and 2(4) of the Charter of the United Nations.

[130] Ref. Ares(2013)3645289 - 05/12/2013, Letter from the Article 29 Working Party to the Data Protection and Cybercrime Division of the Council of Europe.

Subject: Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf

of the Budapest Convention on Cybercrime[131] implies that access or reception of stored computer data located in another Party is subject to the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system, i.e. law enforcement or judicial authorities that need to exchange data in relation to a specific case.

The Working Party also specified in its letter that "*companies acting as data controllers usually do not have the "lawful authority to disclose the data" which they process for e.g. commercial purposes according to the EU data protection acquis*[132]*. They can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required. Data controllers cannot lawfully provide access or disclose the data to foreign law enforcement authorities that operate under a different legal and procedural framework from both a data protection and a criminal procedural point of view."*[133]

The Article 29 Working Party also highlights that these scenarios, if they would take place, would call into question more general fundamental rights issues relating to e.g. due criminal process and criminal procedural guarantees and even qualify as criminal offences in some EU Member States. For example, in France and Germany, such practices would violate telecommunications secrecy as laid down by their national law[134].

---

[131] Article 32 – Trans-border access to stored computer data with consent or where publicly available

"A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

[132] See in particular Article 25 and Article 26 Directive 95/46/EC for transfers to third countries

[133] See aforementioned letter page 3

[134]As an example, § 206 of the German Penal code, relating to the 'Violation of the postal and telecommunications secret', states that:
(1) Whosoever unlawfully discloses to another person facts which are subject to the postal or telecommunications secret and which became known to him as the owner or employee of an enterprise in the business of providing postal or telecommunications services, shall be liable to imprisonment not exceeding five years or a fine.

(2) Whosoever, as an owner or employee of an enterprise indicated in subsection (1) above unlawfully

1. opens a piece of sealed mail which has been entrusted to such an enterprise for delivery or gains knowledge of its content without breaking the seal by using technical means;

Example 2: A transfer from an EU private entity to a non-EU private entity not under EU jurisdiction

In this scenario, the requests from a third country public authority concern data originating from the EU and stored in this third country. A data transfer necessarily occurred in the first place from an EU data exporter to a non-EU data importer for business-related purposes.

a) Transfers to adequate countries or through adequate safeguards

The original transfer for a business-related commercial purpose should take place in compliance with Articles 25 or 26(2) of the Directive 95/46/EC and the data subjects would

---

2. suppresses a piece of mail entrusted to such an enterprise for delivery; or

3. permits or encourages one of the offences indicated in subsection (1) or in Nos 1 or 2 above, shall incur the same penalty.

(3) Subsections (1) and (2) above shall apply to persons who

1. perform tasks of supervision over an enterprise indicated in subsection (1) above;

2. are entrusted by such an enterprise or with its authorisation, to provide postal or telecommunications services; or

3. are entrusted with the establishment of facilities serving the operation of such an enterprise or with performing work thereon.

(4) Whosoever unlawfully discloses to another person facts which became known to him as a public official outside the postal or telecommunications service on the basis of an authorised or unauthorised infringement of the postal or telecommunications secret shall be liable to imprisonment not exceeding two years or a fine.

(5) The immediate circumstances of the postal operations of particular persons as well as the content of pieces of mail are subject to the postal secret. The content of telecommunications and their immediate circumstances, especially the fact whether someone has participated in or is participating in a telecommunications event, are subject to the telecommunications secret. The telecommunications secret also extends to the immediate circumstances of unsuccessful attempts to make a connection.

The French legislation also condemns the violation of correspondences sent, transmitted or received by means of telecommunication under **Article 226-15 of the Criminal Code** and regulates the communication of commercial, industrial, technical and financial data to foreign legal or natural persons under law n° **68-678 of 26 July 1968.**

For more details, see in particular, article 226-15 of the French Criminal code which reads as follows:

Maliciously opening, destroying, delaying or diverting of correspondence sent to a third party, whether or not it arrives at its destination, or fraudulently gaining knowledge of it, is punished by one year's imprisonment and a fine of €45,000. The same penalty applies to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions. - Also see law n° 68-678 of 26 July 1968 " relating to the communication of economical, commercial, industrial, financial or technical documents and information to foreign natural and legal persons, as modified by French act No. 80-538 dated 16 July 1980.

need to be informed about the transfer and its characteristics such as its destination (recipients), purpose as well as the data subject's rights, as required by Article 10 of the Directive. All other data protection principles, data subjects' rights and obligations should also be respected. Compliance with these provisions is required irrelevant of whether the EU data exporter is an entirely distinct entity from the non-EU data importer or if it is one of its subsidiaries.

Furthermore, any access to this personal data by third country authorities as well as communication of personal data to such authorities should be in compliance with EU data protection principles, onward transfer rules set forth in the Directive 95/46/EC and the transfer instruments used as a basis to adduce adequate safeguards (e.g. contractual clauses, Safe Harbor or BCR).

The derogations laid down in the transfer instruments examined above are not sufficiently broad to justify a massive, indiscriminate and secret surveillance that would go beyond the scope of the restrictions of Articles 13 and 26(1) of the Directive. Rather:

a. access should be limited to what is strictly necessary, and

b. purpose should be limited to national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, and

c. according to the European legal framework and to the jurisprudence of the ECtHR and the CJEU, restrictions have to be interpreted narrowly and have to fulfil the criteria of necessity and proportionality.

Last but not least, even though the criteria for derogation on national security grounds would be met, these transfer tools have not proven themselves to be appropriate to guarantee that a third country national security or intelligence agency offers adequate protection to data subjects.

b) Transfers based on the derogations of Article 26(1) of the Directive

In exceptional situations the derogations of Article 26(1) of the Directive could justify the transfer from the EU private entity to the non-EU private entity. However, these exceptions cannot be the basis for massive, structural or repetitive transfers and should not lead to violations of fundamental rights.

Massive, secret and indiscriminate surveillance of personal data fails to fulfill the requirement of an adequate level of protection with regard to respect for both the principles of the Directive 95/46/EC and the conditions for the chosen transfer tool. The assessment of whether the onward transfer is in line with the principles of the Directive and of the transfer tool used

would necessarily fail when it comes to massive, indiscriminate, secret and structural surveillance of personal data. In fact such activities can in no case be considered as compliant with certain data protection principles (incompatible purposes, disproportionate access, lack of transparency, no possible data subject access, no possible data subject objection to processing and offer no adequate means of redress).

Example 3: A transfer from one EU establishment to a non-EU establishment under EU jurisdiction (establishment or means of processing in the EU)

This scenario follows the same transfer structure as the previous one, with the difference that the non-EU private entity falls under EU jurisdiction either because the entity in the EU is an establishment in the sense of Article 4(1)(a) of the Directive or because the non-EU private entity uses means of processing in the EU in accordance with Article 4(1)(c).

As a consequence, the non-EU private entity has to comply with EU law and the conflict of law appears even more clearly than in the previous scenario.

The same legal reasoning can be used in this scenario:

- the derogations allowed by Article 13 of the directive are not sufficiently broad to justify a large scale, systematic and disproportionate surveillance

- to date no transfer tool has proven it can be used to guarantee that a third country national security or intelligence agency offers adequate protection to data subjects.

-

6. Comments on possible options for a way forward

As stated in the introduction, this Working Document is intended as a contribution to a much needed debate on the scope and boundries of the fundamental right to data protection when dealing with surveillance. As is shown in the previous chapters, the Working Party considers several parts of the data protection legislation will continue to apply to data controllers and processors, even when dealing with intelligence services. And rightfully so: the rule of law and the courts require restrictions to fundamental rights to be limited to what is strictly necessary and proportionate, specific and codified in law.

6.1. Data protection reform

There are only two parties who can really provide legal certainty when considering data protection in a surveillance and national security context: the courts and the legislator. Given the ongoing data protection reform in the EU, a unique window of opportunity presents itself to demarcate the situations to which the data protection regime shall apply, including when dealing with data transmissions to law enforcement and intelligence services.

6.1.1. The proposed new Article 43a

The European Parliament's Committee in charge of Civil Liberties, Justice and Home Affairs (LIBE) introduced a new Article 43a in the Commission proposal for a General Data Protection Regulation. Article 43a was based on Article 42 of the original Commission draft proposal[135], which was taken out from the final proposal adopted by the College of Commissioners, where only a relating Recital 90 was included.

This Article relates to transfers or disclosures not authorised by Union law. It recalls that the disclosure of personal data to any authority of a third country (court, tribunal, administrative authority) should only take place after notification of the request and prior authorisation of the supervisory authority, without prejudice to a Mutual Legal Assistance Treaty or an international agreement in force between the requesting third country and the Union or a Member State.

The Article further specifies that the authorisation given by the supervisory authority should be based on an assessment of the compliance of the request with the General Data Protection Regulation and that the competent national law enforcement authority should be informed of the request. Information to data subjects on the disclosure is also required to some extent.

In this regard, the Working Party refers to its statement on the vote of 21 October 2013 by the European Parliament's LIBE Committee. In particular, in its comments relating to access by public authorities and data transfers to third countries it welcomed the mandatory information to individuals when access to data has been given to a public authority. It also insisted on the need for a robust and solid framework of protection and welcomed the use of Mutual Legal Assistance Treaties or international agreements in cases of disclosures not authorised by Union or Members States' law. Finally, it stated that "when confronted with requests from third country public authorities for access, the competent supervisory authority should be the EU national authority dealing with the request rather than the data protection authority".

6.2 Open legal questions

Some elements of the proposed Article 43a may be a step in the right direction, but it will not be the *deus ex machina* solving all other questions. The analysis in this Working Document makes clear that there are fundamental legal questions, including the definition of the key concepts of "national security" and "data transfers", which remain open. A difficult debate is to follow to consider viable solutions to address these fundamental issues, at European and global level, involving all stakeholders. The Working Party considers that in this globalised day and age with unlimited data flows between countries and towards the cloud, new solutions will need to be found. They should ensure that we as a society can continue to protect the fundamental rights of citizens, while at the same time providing a safe and secure place to live.

[135] Leaked by statewatch.org.