ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 237

Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)

Adopted on 13 April 2016

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 and Consumers, B-1049 Brussels, Belgium, Office No MO-59 02/013.

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

Table of content

1. INTRODUCTION 3

2. INTERFERENCES TO FUNDAMENTAL RIGHTS 4

3. THE EUROPEAN ESSENTIAL GUARANTEES 6

4. GUARANTEE A - PROCESSING SHOULD BE BASED ON CLEAR, PRECISE AND ACCESSIBLE RULES 7

5. GUARANTEE B - NECESSITY AND PROPORTIONALITY WITH REGARD TO THE LEGITIMATE OBJECTIVES PURSUED NEED TO BE DEMONSTRATED 7

6. GUARANTEE C - AN INDEPENDENT OVERSIGHT MECHANISM SHOULD EXIST 9

7. GUARANTEE D - EFFECTIVE REMEDIES NEED TO BE AVAILABLE TO THE INDIVIDUAL 11

8. CONCLUDING REMARKS 12

ANNEX 1 – JURISPRUDENCE 13

1. Introduction

On 6 October 2015, the Court of Justice of the European Union (hereinafter: CJEU) published its landmark ruling in the case *Maximillian Schrems v. Data Protection Commissioner*[1]. Following a request for a preliminary ruling from the Irish High Court, the CJEU decided to annul the so-called Safe Harbour decision based on the fact that it did not make sufficiently clear the United States (hereinafter also: the U.S.) legislation offered adequate safeguards to protect personal data originating in the European Union (hereinafter: the EU).

With the invalidation of the Safe Harbour decision, many data transfers to the United States immediately became unlawful, since so many companies relied on the provisions of a no longer existing decision to send data to the U.S. The CJEU raised questions on the extent of possible national security and law enforcement related interferences with the fundamental rights[2] of the persons whose data is transferred from the European Union to the United States. Since these possible interferences are not limited to data transferred under the Safe Harbour decision, doubts were also raised about whether other transfer tools (ad hoc contractual clauses, Standard Contractual Clauses (hereinafter: SCCs), Binding Corporate Rules (hereinafter: BCRs) and derogations pursuant Article 26(1) of Directive 95/46/EC (hereinafter: the Directive)) offer an adequate safeguard when data is sent to the U.S.

The WP29 has therefore decided in its meeting of 16 October 2015 to assess the consequences of the Schrems judgment to all data transfers to the United States. To this end, the WP29 inventoried and analysed CJEU jurisprudence related to Articles 7, 8 and 47 of the Charter of Fundamental Rights (hereinafter: the Charter) and the jurisprudence of the European Court of Human Rights (hereinafter: ECtHR) related to Article 8 of the European Convention on Human Rights (hereinafter: ECHR) dealing with surveillance issues in States party to the ECHR. Together, this jurisprudence provides guidance on what can and what cannot be regarded as a justifiable interference to fundamental rights in a democratic society. The result of this analysis is what the WP29 calls the four European Essential Guarantees (hereinafter also: the Guarantees).

These Guarantees are to be distinguished from what the CJEU calls "a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of [the EU data protection Directive] read in the light of the Charter". Essentially equivalent is the bar set by the CJEU to obtain an adequacy decision as foreseen in article 25(6) of the European data protection Directive, whereas the European Essential Guarantees provide guidance when assessing if an interference with a fundamental right can be justified and apply to all data processing operations, including transfers on the basis of Articles 25 and 26 of the Directive.

[1] The references to all jurisprudence cited in this analysis can be found in Annex 1

[2] In this Working Document, the term "fundamental rights" is derived from the EU Charter on Fundamental Rights. However, it is used to also cover the "human rights" as included in the European Convention on Human Rights. In the view of the WP29, both should be respected in a similar way.

This Working Document explains the background of the four European Essential Guarantees. The WP29 would like to stress that these Guarantees are primarily based on the jurisprudence of the CJEU and the ECtHR. They should however be read in conjunction with the interpretation the WP29 has given in earlier opinions to various elements of the EU data protection legal framework. As far as data transfers to the United States are concerned, the WP29 refers to its Opinion 01/2016 on the level of protection provided by the EU – U.S. Privacy Shield, which includes an assessment of the European Essential Guarantees for data transfers to the U.S.

2. Interferences to fundamental rights

The fundamental rights to private and family life and to data protection are laid down in Articles 7 and 8 of the Charter and apply to everyone. Article 8 furthermore provides basic guidance on data processing, including the need for purpose limitation, independent control by a supervisory authority and the availability of a legal basis laid down by law as well as rights of access and rectification. In Schrems, the CJEU reiterates that "EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled jurisprudence, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data"[3]. This level of fundamental rights protection against arbitrary interference should be ensured when data are transferred to a country considered as adequate on the basis of Article 25 of the Directive. A similar regime should apply to data transfers based on Article 26 of the Directive, if only because fundamental rights apply across to board and not only depending on the legal basis for a data transfer. Additionally, it should be noted that Article 4 of the SCCs, in application of Article 26(4) of the Directive, obliges DPAs to make an assessment whether the law of a third country imposes upon the importer of data "requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society."[4] However, the assessment if fundamental rights are respected may turn out differently in an individual case than it would be for a general approval of data transfers to a third country.

The fundamental rights protection offered to personal data in Europe not only relies on EU law, but also on the protection offered by the ECHR.[5] Recently, the ECtHR in the Zakharov case has reiterated its position regarding interferences to the fundamental right to a private

[3] Schrems, §91

[4] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 96/46/EC of the European Parliament and of the Council (2010/87/EU)

[5] The WP29 recalls Article 6(3) TEU, where it is stated that the "Fundamental rights, as guaranteed by the European convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law".

life. These can only be justified if they are in accordance with the law, in pursuit of a legitimate aim and necessary in a democratic society to achieve any such aim.[6]

Both the Charter and the ECHR include a necessity and proportionality test to frame limitations to the rights they protect[7]. Article 52(1) of the European Charter specifies the scope of possible limitation to Articles 7 and 8 by stating that "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

At the same time, the limitation clause in Article 8(2) of the ECHR also specifies that "there shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing 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".

According to both Courts, any limitation to or interference with the fundamental rights to privacy and data protection (i.e. the collection, storage, access or use and dissemination of personal data from an individual for purposes for which it was not originally transferred, but for national security or intelligence purposes) can only be justified if it is "strictly necessary in a democratic society".[8] In their judgments, the Courts have described in some detail what they understand to be necessary in a democratic society, including the requirement that any measure must be taken in accordance with the law and should offer "minimum safeguards against abuse"[9].

The ECtHR furthermore consistently recognizes that States Parties have "a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security" [10] when assessing the necessity of a measure. This right of countries to introduce legislation intended to maintain national security or to collect data for intelligence purposes is naturally also recognised by the WP29. Moreover, intelligence gathering can be a perfectly legitimate aim to process personal data, as has also been underlined by the ECtHR, most recently in the Szabó case.[11] This can even include the use of secret surveillance measures, as long as adequate and effective guarantees against abuse are in place preventing that surveillance "undermine[s] or even destroy[s] democracy under the cloak of defending it"[12].

[6] ECtHR, Zakharov, §227
[7] For more details, see http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15%281997%29.pdf
[8] ECtHR, Klass, §§42, 48; ECtHR, Malone, §81 and others
[9] CJEU, Schrems, §91 including cited jurisprudence
[10] ECtHR, Weber and Saravia, §106
[11] ECtHR, Szabó, §57
[12] ECtHR, Szabó, §57

In principle, all data processing operations, including surveillance measures[13], constitute an interference, especially where data relating to the private life of an individual is stored by a public authority[14] and/or where providers of publicly available electronic communication services or of public communications networks are obliged to retain data relating to a person's life and to his communications[15]. Access of a competent (law enforcement) authority to the data constitutes a further interference[16]. In order to determine an interference, "it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered"[17].

Both the CJEU and the ECtHR have made clear in their judgments that it is ultimately their decision if interferences with a fundamental right can be justified. However, in absence of such a judgment and in application of the standing jurisprudence, data protection authorities are empowered to assess individual cases, either ex officio or following a complaint, in order to decide whether a data transfer can (continue to) take place if they find an interference with the fundamental rights to privacy and data protection.

3. The European Essential Guarantees

The WP29 has drawn upon the jurisprudence to identify what it calls the *European Essential Guarantees* that should be in place to make sure interferences do not go beyond what is necessary in a democratic society. The European Essential Guarantees are primarily based on the jurisprudence of the CJEU and the ECtHR in cases related to the application of the rights to privacy and data protection in Europe. This means the Guarantees in the first place apply in and to the Member States of the European Union and the Council of Europe when applying European or national legislation interfering with these rights. Since data transferred outside the EU should be offered continued protection against arbitrary interference, the European Essential Guarantees will also have to be seriously taken into account for all transfers to third countries.

The WP29 underlines that the Guarantees are based on the fundamental rights that apply to everyone, notwithstanding their nationality.

Following the assessment of the jurisprudence, the WP29 comes to the conclusion that the requirements can be summarised in four European Essential Guarantees:

A. Processing should be based on clear, precise and accessible rules
B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
C. An independent oversight mechanism should exist
D. Effective remedies need to be available to the individual

[13] ECtHR, Malone, §64
[14] ECtHR, Amman, §70
[15] CJEU, Digital Rights Ireland, §34
[16] ECtHR, Leander, §48; ECtHR, Rotaru §46; CJEU, Digital Rights Ireland, §35
[17] CJEU, Schrems, §87 including cited jurisprudence

4. Guarantee A - Processing should be based on clear, precise and accessible rules

A justifiable interference first needs to be in accordance with the law. The interference must be foreseeable as to its effect for the individual in order to give him/her adequate protection against arbitrary interference. As a result, the processing must be based on a precise, clear and accessible (i.e. public) legal basis.[18] This legal basis should in any case be set out in statute law including the nature of the offences which may give rise to an interception or surveillance order, a definition of the categories of people that might be subject to surveillance, a limit on the duration of the measure, the procedure to be followed for examining, using and storing the data obtained, and the precautions to be taken when communicating the data to other parties.[19] It must also include the circumstances and substantive and procedural conditions relating to the access of the competent authorities.[20] Finally, the Court "does not consider that there is any ground to apply different principles covering the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance".[21]

The ECtHR recalled in the Zakharov case that "the reference to 'foreseeability' in the context of interception of communications cannot be the same as in many other fields". It specified that in the context of secret measures of surveillance, such as the interception of communications, "foreseeability cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly". However, considering that in this kind of situation the risks of arbitrariness are evident "it is essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures".[22]

5. Guarantee B - Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

Any data processing by government authorities is, by definition, an interference with the right to privacy and data protection.[23] This is also the case for data processing by government authorities for intelligence purposes, which can still be justifiable, but only when necessary and proportionate in relation to a legitimate objective.

In Schrems, the CJEU has stated that "legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any

[18] ECtHR, Malone, §§65, 66, 70
[19] ECtHR, Weber and Saravia, §95
[20] CJEU, Digital Rights Ireland, §61
[21] ECtHR, Liberty, §63
[22] ECtHR, Zakharov, §229
[23] See for example CJEU, Digital Rights Ireland, §36

differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail".[24]

In Szabó, a Chamber of the ECtHR states that "in the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. (…) Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. (…) This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. (…) However, it is not warranted to embark on this matter in the present case".[25]

In Digital Rights Ireland, the CJEU suggests that legislation "covering all persons and all means of electronic communication" should include "any differentiation, limitation or exception being made".[26] Additionally, the CJEU considers the legislator needs to provide for an "objective criterion by which to determine the limits of the access (…) and their subsequent use". [27]

At the same time, in Zakharov, the Grand Chamber of the ECtHR states that "the existence of a reasonable suspicion against the person concerned"[28], who must be clearly identified by name, address, telephone number or other relevant information"[29], needs to be verifiable, which would indicate only targeted data collection should be allowed.

The Courts do not seem to have taken a final position on the legality of the massive and indiscriminate collection of personal data (i.e. non-targeted bulk collection) and their subsequent use, including the question under what circumstances such collection and use of personal data could take place. The CJEU is expected to address this question at least to some extent in the course of 2016, both in the joined cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Davis and others[30] and in the advice to be given on the validity of the PNR Canada agreement.[31]

[24] CJEU, Schrems §93
[25] ECtHR, Szabó, §§68-70
[26] CJEU, Digital Rights Ireland, §57
[27] CJEU, Digital Rights Ireland, §60
[28] ECtHR, Zakharov, §260
[29] ECtHR, Zakharov, §264
[30] CJEU, Joined Cases C-203/15 and C-698/15
[31] CJEU, Case A-1/15

As regards the content of communications data, the CJEU is clearer. It has stated in the Schrems judgment that public authorities should not be allowed to have access to the content of electronic communications on a generalised basis.[32] Legislation permitting public authorities to have such access must indeed be regarded as compromising not only the right, but "the essence of the fundamental right to respect for private life".[33] However, the court does not define what it understands 'on a generalised basis' to mean.

6. Guarantee C - An independent oversight mechanism should exist

Since the 1970s, the ECtHR has held that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body[34] (e.g. an administrative authority or a parliamentary body). No matter the form of independent supervision, the existence of oversight authorities forms "an essential component of the protection of individuals with regard to the processing of personal data".[35] The WP29 recalls that an interference takes place at the time of collection of the data, but also at the time the data is accessed by a government authority for further processing for intelligence purposes.

The ECtHR considers independent oversight can take place at various stages during the life-cycle of a data processing operation: when the surveillance is first ordered, while it is being carried out and/or after it has been terminated.[36] Given the special nature of data processing for intelligence purposes, it is accepted that the processing takes place without the data subject being informed, in any case at the start and during the surveillance operation. The ECtHR specified that "as regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be affected without the individual's knowledge. (…) In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[37]

The CJEU specifies that "the access (…) to the data retained [should also be] made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions."[38]

---

[32] CJEU, Schrems, §94
[33] CJEU, Schrems §94
[34] ECtHR, Klass, §§17, 51
[35] CJEU, Commission v. Germany, §23
[36] ECtHR, Klass §§55-56; ECtHR, Zakharov, §233
[37] ECtHR, Zakharov, §233
[38] CJEU, Digital Rights Ireland, §62. The Court made these matters clear by holding that the Data Retention Directive was invalid because it did not meet these requirements.

It should be noted that the ECtHR appears to have drawn its conclusions in cases about telephone tapping, where prior authorisation to collect the data and the subsequent access to the data would be difficult to distinguish. However, the CJEU quotation stems from the data retention case Digital Rights Ireland, dealing with metadata, which by virtue of the concerning legislation implies the collection of a large amount of non-targeted data.

As regards oversight ex post, this is mainly related to the remedies available to the individual. This is addressed as part of Guarantee D. It is noted that in some situations, also ex officio controls ex post could take place to verify the compliance of surveillance measures with the applicable legislation. As far as the WP29 is aware, the Courts have not set specific criteria for such ex officio and ex post oversight.

As to the independence of oversight mechanisms in relation to surveillance, the Strasbourg Court has expressed its preference for a judge to be responsible to maintain oversight. However, it is not excluded that another body can be responsible, "as long as it is sufficiently independent from the executive"[39] and "of the authorities carrying out the surveillance, and [is] vested with sufficient powers and competence to exercise an effective and continuous control"[40]. The ECtHR adds that "the manner of appointment and the legal status of the members of the supervisory body"[41] need to be taken into account when assessing independence. This includes "persons qualified to hold judicial office, appointed either by parliament or by the Prime Minister. In contrast, a Minister of Internal Affairs – who not only was a political appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance – was found to be insufficiently independent."[42] The ECtHR also "notes that it is essential that the supervisory body has access to all relevant documents, including closed materials"[43]. Finally, the ECtHR takes into account "whether the supervisory body's activities are open to public scrutiny"[44].

Specifically for data protection authorities, the CJEU in three cases has given its view on what independence in the light of the Directive entails. Since some data protection authorities are also competent to supervise data processing operations for intelligence purposes, this standard set by the CJEU may be relevant in such particular situations. First of all, this means that the authority should perform its duties free from external influence. "[I]ndependence precludes inter alia any directions or any other external influence in whatever form, whether direct or indirect, which may have an effect on their decisions".[45] The Court also recalls that "functional independence is not by itself sufficient to protect that supervisory authority from all external influence".[46]

[39] ECtHR, Zakharov, §258
[40] ECtHR, Klass §56
[41] ECtHR, Zakharov, §278
[42] ECtHR, Zakharov, §278
[43] ECtHR, Zakharov, §281
[44] ECtHR, Zakharov, §283
[45] CJEU, Commission v. Hungary, §51 including cited jurisprudence
[46] CJEU, Commission v. Austria, §42

7. Guarantee D - Effective remedies need to be available to the individual

The final European Essential Guarantee is related to the redress rights of the individual. (S)he must have an effective remedy to satisfy his/her rights when (s)he has the idea they are not respected. The CJEU explained in Schrems that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article."[47]

For the ECtHR, the question of an effective remedy is inextricably linked to the notification of a surveillance measure to the individual once the surveillance is over. "There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications".[48]

In case there is no notification, the ECtHR has made clear in the Kennedy case that it is satisfied a court offers sufficient redress possibilities, if it meets a series of criteria: an independent and impartial body, which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the court should have access to all relevant information[49], including closed materials. Finally, it should have the powers to remedy non-compliance.[50]

The question is whether an effective remedy can only be provided by an ordinary court, or also by a different body that is sufficiently independent and has sufficient powers to remedy non-compliance. Article 47 Charter refers to a tribunal, even though in language versions other than English the preference is given to the word "court".[51] At the same time, the ECHR only obliges Member States to ensure that "everyone whose rights and freedoms (…) are violated shall have an effective remedy before a national authority"[52]. This does not necessarily need to be a judicial authority, as the ECtHR has clarified in Klass.[53]

[47] CJEU, Schrems §95
[48] ECtHR, Zakharov, §234
[49] The WP29 notes that the Council of Europe Commissioner for Human Rights considers that the so-called "third parties" rule – under which intelligence agencies in one country that provide data to intelligence agencies in another country can impose a duty on the receiving agencies to not disclose the transferred data to any third party – should not apply to oversight bodies in order not to undermine the possibility of an effective remedy (Issue Paper on Democratic and effective oversight of national security services)
[50] ECtHR, Kennedy §167
[51] The word tribunal is for example translated as "Gericht" in German and "gerecht" in Dutch.
[52] Article 13 ECHR
[53] ECtHR, Klass §67

Nevertheless, the Strasbourg Court has strong expectations of the body providing the effective remedy, as it has made clear in Kennedy.

8. Concluding remarks

The four European Essential Guarantees that are described in this opinion are no unconditional Guarantees. Also when looking at their formulation, it should be clear that all four require a certain degree of interpretation.

Should a third country allow for interferences that go beyond what should be regarded as strictly necessary in a democratic society, an individual could call upon its DPA for help in investigating and protecting his/her fundamental rights. The WP29 underlines that DPAs will make an assessment on an individual basis or in order to approve (or evaluate) massive, structural or repetitive data transfers based on one of the transfer tools. The outcome of such an assessment may vary and enforcement action could include prohibiting or suspending data transfers on a case-by-case basis.

The WP29 notes that the interpretation of European Essential Guarantee B (the need to demonstrate necessity and proportionality) may be subject to an update in the course of 2016, when the CJEU will issue its decisions in the cases PNR Canada, Tele2 Sverige and Davis. In the mean time the WP29 recalls that it has consistently considered that massive and indiscriminate collection of data (non-targeted bulk collection) in any case cannot be considered as proportionate.[54]

The European Essential Guarantees should not be assessed independently, but on an overall basis, reviewing the relevant legislation in relation to data collection for surveillance purposes, the minimum level of safeguards for the protection of the rights of the data subjects and the remedies provided under the national law of the third country. As the ECtHR stated in Kennedy, an "assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by national law"[55].

The WP29 underlines that the Guarantees are based on the fundamental rights that apply to everyone, notwithstanding their nationality. Furthermore, it should be noted that the Guarantees are based on what is required by the law and not necessarily on what is the current practice in the EU Member States. The WP29 does not maintain a double standard and has therefore already called several times upon the Member States to ensure their surveillance legislation is in line with the jurisprudence of the CJEU and the ECtHR.

[54] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf
[55] ECtHR, Kennedy, §153

Annex 1 – Jurisprudence

Throughout this opinion reference is made to case law from both the Court of Justice of the European Union and the European Court of Human Rights. The references of the various cases, including relevant cases that are not explicitly referenced, but have been used in the preparation of this Opinion, are as follows:

- Amman v. Switzerland
  European Court of Human Rights, 16 February 2000
  Application no. 27798/95

- Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria
  European Court of Human Rights, 28 June 2007
  Application no. 62540/00

- Bucur and Toma v. Romania
  European Court of Human Rights, 8 January 2013
  Application no. 40238/02

- Chahal v. United Kingdom
  European Court of Human Rights, 15 November 1996
  Application no. 22414/93

- Commission v. Austria
  Court of Justice of the European Union, 16 October 2012
  Case C-614/10

- Commission v. Germany
  Court of Justice of the European Union, 9 March 2010
  Case C-518/07

- Commission v. Hungary
  Court of Justice of the European Union, 8 April 2014
  Case C-288/12

- Copland v. United Kingdom
  European Court of Human Rights, 3 April 2007
  Application no. 62617/00

- Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others
  Court of Justice of the European Union,8 April 2014
  Joined Cases C-293/12 and C-594/12

- Gillan and Quinton v. United Kingdom
  European Court of Human Rights, 12 January 2010
  Application no. 4158/05

- Hokkanen v. Finland
  European Court of Human Rights, 23 September 1994
  Application no. 19823/92

- Huvig v. France
  European Court of Human Rights, 24 April 1990
  Application no. 11105/84

- Klass and others v. Germany
  European Court of Human Rights, 6 September 1978
  Application no. 5029/71

- Leander v. Sweden
  European Court of Human Rights, 26 March 1987
  Application no. 9248/81

- Liberty and others v. United Kingdom
  European Court of Human Rights, 1 July 2008
  Application no. 58243/00

- López Ostra v. Spain
  European Court of Human Rights, 9 December 1994
  Application no. 16798/90

- Malone v. United Kingdom
  European Court of Human Rights, 2 August 1984
  Application no. 8691/79

- Rotaru v. Romania
  European Court of Human Rights, 4 May 2000
  Application no. 28341/95

- S. and Marper v. United Kingdom
  European Court of Human Rights, 4 December 2008
  Applications nos. 30562/04 and 30566/04

- Schrems v. Data Protection Commissioner of Ireland
  Court of Justice of the European Union, 6 October 2015
  Case C-362/14

- Szábo and Vissy v. Hungary
  European Court of Human Rights, 12 January 2016
  Application no. 37138/14

- Weber and Saravia v. Germany
  European Court of Human Rights, 29 June 2006
  Application no. 54934/00

- Zakharov v. Russia
  European Court of Human Rights, 4 December 2015
  Application no. 47143/06

- ZZ v. Secretary of State for the Home Department
  Court of Justice of the European Union, 4 June 2013
  Case C-300/11