Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

Adopted on 10 November 2020

Table of contents

The European Data Protection Board

Having regard to Article 70 (1) (e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),[1]

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[2],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Having regard to the Article 29 Working Party working document on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees hereinafter "EEG"), WP237,

HAS ADOPTED THE FOLLOWING RECOMMENDATIONS

1. INTRODUCTION

1. Following the Schrems I judgment, EU Data Protection Authorities assembled in the Working Party 29 drew upon the jurisprudence to identify the European Essential Guarantees, which need to be respected to make sure interferences with the rights to privacy and the protection of personal data, through surveillance measures, when transferring personal data, do not go beyond what is necessary and proportionate in a democratic society.

2. The EDPB would like to stress that the European Essential Guarantees are based on the jurisprudence of the Court of Justice of the European Union (hereinafter: CJEU) related to Articles 7, 8, 47 and 52 of the Charter of Fundamental Rights of the EU (hereinafter: the Charter) and, as the case may be, on 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.[3]

[1] This paper does not address situations of transfers or onward sharing falling under the scope of the Law Enforcement Directive (Directive (EU) 2016/680).

[2] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

[3] In these Recommendations, the term "fundamental rights" is derived from the EU Charter of Fundamental Rights of the EU. However, it is used to also cover the "human rights" as included in the European Convention on Human Rights.

3. The update of this paper is meant to further develop the European Essential Guarantees, originally drafted in response to the Schrems I judgment[4] by reflecting the clarifications provided by the CJEU (and by the ECtHR) since it was first published, in particular in its landmark Schrems II judgment.[5.]

4. In its Schrems II judgment, the CJEU stated that the examination of the Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries, in the light of Articles 7, 8 and 47 of the Charter, has disclosed nothing to affect the validity of that decision, but invalidated the Privacy Shield Decision. The CJEU held that the Privacy Shield Decision was incompatible with Article 45 (1) GDPR, in the light of Articles 7, 8, and 47 of the Charter. The judgment can thus serve as an example where surveillance measures in a third country (in this case the U.S. with Section 702 FISA and Executive Order 12 333) are neither sufficiently limited nor object of an effective redress available to data subjects to enforce their rights, as required under EU law in order to consider the level of protection in a third country to be "essentially equivalent" to that guaranteed within the European Union within the meaning of Article 45 (1) of the GDPR.

5. The reasons for the invalidation of the Privacy Shield also have consequences on other transfer tools.[6] Even though the Court interpreted Article 46(1) GDPR in the context of the validity of the Standard Contractual Clauses (hereinafter: SCCs), its interpretation applies to any transfer to third countries relying on any of the tools referred to in Article 46 GDPR[7.]

6. It is ultimately for the CJEU to judge whether 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 required to assess individual cases, either ex officio or following a complaint, and to either refer the case to a national Court if they suspect that the transfer does not comply with Article 45 where there is an adequacy decision, or to suspend or prohibit the transfer if they find Article 46 GDPR cannot be complied with and the protection of the data transferred required by EU law cannot be ensured by other means.

7. The aim of the updated European Essential Guarantees is to provide elements to examine, whether surveillance measures allowing access to personal data by public authorities in a third country, being national security agencies or law enforcement authorities, can be regarded as a justifiable interference or not.

8. Indeed, the European Essential Guarantees form part of the assessment to conduct in order to determine whether a third country provides a level of protection essentially equivalent to that guaranteed within the EU but do not aim on their own at defining all the elements which are necessary to consider that a third country provides such a level of protection in accordance with Article 45 of the GDPR. Likewise, they do not aim on their own at defining all the elements that might be necessary to consider when assessing whether the legal regime of a third country prevents the data exporter and data importer from ensuring appropriate safeguards in accordance with Article 46 of the GDPR.

---

[4] CJEU judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, EU:C:2015:650 (hereinafter: Schrems I).

[5] CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, case C-311/18, ECLI:EU:C:2020:559 (hereinafter: Schrems II).

[6] See §105 of Schrems II.

[7] See §92 of Schrems II.

9. Therefore, the elements provided in this paper should be seen as the essential guarantees to be found in the third country when assessing the interference, entailed by a third country surveillance measures, with the rights to privacy and to data protection, rather than a list of elements to demonstrate that the legal regime of a third country as a whole is providing an essentially equivalent level of protection.

10. Article 6(3) of the Treaty on European Union establishes that the fundamental rights enshrined in the ECHR constitute general principles of EU law. However, as the CJEU recalls in its jurisprudence, the latter does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law.[8]Thus, the level of protection of fundamental rights required by Article 46(1) of the GDPR must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter. This being said, according to Article 52(3) of the Charter the rights contained therein which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that Convention, and consequently, as recalled by the CJEU, the jurisprudence of the ECtHR concerning rights which are also foreseen in the Charter of Fundamental Rights of the EU must be taken into account, as a minimum threshold of protection to interpret corresponding rights in the Charter.[9] According to the last sentence of Article 52(3) of the Charter, however, "[t]his provision shall not prevent Union law providing more extensive protection."

11. Therefore, the substance of the Essential Guarantees will continue to be partly based on the jurisprudence of the ECtHR, to the extent that the Charter as interpreted by the CJEU does not provide for a higher level of protection which prescribes other requirements than the ECtHR case law.

12. This paper explains the background and further details the four European Essential Guarantees.

2. INTERFERENCES WITH FUNDAMENTAL RIGHTS

13. The fundamental rights to respect for private and family life, including communications, and to the protection of personal data are laid down in Articles 7 and 8 of the Charter and apply to everyone. Article 8 furthermore sets conditions for the processing of personal data to be lawful and recognizes the right of access and rectification, as well as imposes that these rules are subject to the control of an independent authority.

14. "(T)he operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data".[10] Thus, Articles 7 and 8 of the Charter apply to this specific operation and their protection extend to the data transferred, which is why data subjects

[8] See § 98 of Schrems II.

[9] See § 124 of joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others (hereinafter: La Quadrature du Net and others).

[10] CJEU, Schrems II, § 83.

whose personal data are transferred to a third country must be afforded a level of protection essentially equivalent to that which is guaranteed within the European Union.[11]

15. According to the CJEU, when the fundamental right to respect for private life enshrined in Article 7 of the Charter is affected, by means of processing an individual's personal data, the right to data protection is also affected, as such processing falls within the scope of Article 8 of the Charter, and, accordingly, must necessarily satisfy the data protection requirement laid down in that article.[12]

16. Therefore, as regards possible interference with fundamental rights under the EU law, the obligation imposed on providers of electronic communications services (…) to retain traffic data for the purpose of making it available, if necessary, to the competent national authorities, raises issues relating to compatibility with Articles 7 and 8 of the Charter.[13] The same applies to other types of data processing, such as the transmission of data to persons other than users or access to that data with a view to its use[14,] which, thus, entails an interference with those fundamental rights. Moreover, access to the data by a public authority constitutes a further interference, according to settled case-law.[15]

17. In order to find an interference, it does not matter "whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference."[16] The CJEU also stressed that whether or not the retained data has been subsequently used is irrelevant.[17]

18. However, Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society.[18]

19. The Charter includes a necessity and proportionality test to frame limitations to the rights it protects. Article 52(1) of the Charter specifies the scope of possible limitations 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".

20. The CJEU reiterated that EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter "must lay down clear and precise rules governing the scope and application of the measure and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse", in particular where personal data is subjected to automatic processing and "where there is a significant risk of unlawful access to that data".[19]

[11] CJEU, Schrems II, § 96.
[12] CJEU, Schrems II, §§ 170-171.
[13] CJEU, case C-623/17, Privacy International (hereinafter: Privacy International), § 60.
[14] CJEU, Privacy International, § 61.
[15] ECtHR, Leander, §48; ECtHR, Rotaru §46; CJEU, Digital Rights Ireland, §35.
[16] CJEU, Schrems II, § 171, including cited jurisprudence.
[17] CJEU, Schrems II, §171, including cited jurisprudence.
[18] CJEU, Privacy International, §63.
[19] CJEU, Privacy International, §68 and jurisprudence referred therein.

21. According to the CJEU, the protection of the right to privacy requires that derogations from and restrictions to the right to data protection "must apply in so far as is strictly necessary". Furthermore, an objective of general interest must be reconciled with the fundamental rights affected by the measure, "by properly balancing" such objective against the rights at issue.[20]

22. Consequently, access, retention and further use of personal data by public authorities within the remit of surveillance measures must not exceed the limits of what is strictly necessary, assessed in the light of the Charter, otherwise it "cannot be considered to be justified, within a democratic society".[21]

23. The four European Essential Guarantees, as they are developed in the next chapter, intend to further specify how to assess the level of interference with the fundamental rights to privacy and to data protection in the context of surveillance measures by public authorities in a third country, when transferring personal data, and what legal requirements must consequently apply in order to evaluate whether such interferences would be acceptable under the Charter.

3. THE EUROPEAN ESSENTIAL GUARANTEES

24. Following the analysis of the jurisprudence, the EDPB considers that the applicable legal requirements to make the limitations to the data protection and privacy rights recognised by the Charter justifiable 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

25. The Guarantees are based on the fundamental rights to privacy and data protection that apply to everyone, irrespective of their nationality.

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

26. Under Article 8(2) of the Charter, personal data should, inter alia, be processed "for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law",[22] as the CJEU recalled in the Schrems II ruling. Furthermore, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter within the EU must be provided for by law. Thus, a justifiable interference needs to be in accordance with the law.

[20] CJEU, Privacy International, §68 and jurisprudence referred therein.
[21] CJEU, Privacy International, §81.
[22] See §173 Schrems II.

27. This legal basis should lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.[23] In addition, the Court recalled that "legislation must be legally binding under domestic law".[24] In this regard, the CJEU clarified that the assessment of the applicable third country law should focus on whether it can be invoked and relied on by individuals before a court.[25] The Court therefore indicates that the rights granted to data subjects shall be actionable; where individuals are not provided with enforceable rights against public authorities, the level of protection granted cannot be considered as essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR.[26]

28. Furthermore, the Court stressed that the applicable law must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted[27] (see infra under Guarantee B the relation between these requirements and the principles of necessity and proportionality).

29. Moreover, the CJEU has also indicated that "the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned".[28]

30. Finally, the European Court of Human Rights "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".[29] The ECtHR as well has clarified that the legal basis should at least include 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.[30]

31. Lastly, the interference must be foreseeable as to its effect for the individual in order to give him/her adequate and effective protection against arbitrary interference and the risk of abuse. As a result, the processing must be based on a precise, clear but also accessible (i.e. public) legal basis.[31] The ECtHR, concerning this question, 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

[23] See §175 and §180 Schrems II and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, § 139 and the case-law cited.

[24] See § 68 Privacy International – It should also be clear that in the French version of the judgment the Court uses the word "réglementation" which is broader than only acts of Parliament.

[25] See § 181 Schrems II, in this paragraph the CJEU refers to the US Presidential Policy Directive 28.

[26] See § 181 Schrems II.

[27] See § 68 of Privacy International, in relation to Member State law.

[28] See Schrems II, § 175 and the case-law cited, as well as Privacy International, § 65.

[29] ECtHR, Liberty, §63.

[30] ECtHR, Weber and Saravia, §95.

[31] ECtHR, Malone, §§65, 66.

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".[32]

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

32. In accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms 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.[33]

33. Regarding the **principle of proportionality**, the Court held, in relation to Member State laws, that the question as to whether a limitation on the rights to privacy and to data protection may be justified must be assessed, on the one hand, by measuring the **seriousness of the interference** entailed by such a limitation[34] and by verifying that the **importance of the public interest objective** pursued by that limitation is proportionate to that seriousness, on the other hand.[35]

34. In La Quadrature du net and others, it can be noted that the CJEU ruled, in relation to the law of a Member State and not to a third country law, that the objective of safeguarding national security is, due to its importance, capable of justifying measures entailing more serious interferences with fundamental rights, than those which might be justified by other objectives such as of combating crime. It found however that this is the case as long as there are sufficiently solid grounds for considering that the State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable and subject to meeting the other requirements laid down in Article 52(1) of the Charter.[36]

---

[32] ECtHR, Zakharov, §229.

[33] Schrems II, § 174.

[34] In this context, the court noted for instance that "the interference constituted by the real-time collection of data that allows terminal equipment to be located appears particularly serious, since that data provides the competent national authorities with a means of accurately and permanently tracking the movements of users of mobile telephones (...)" (La Quadrature du Net and others, § 187, including cited jurisprudence).

[35] La Quadrature du Net and others, § 131.

[36] §§136 and 137. See also Privacy International, as the Court specified, such threats can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. § 75. For instance, in La Quadrature du Net and others, the Court noted that the automated analysis of traffic and location data covering generally and indiscriminately the data of persons using electronic communications systems constitutes an interference particularly serious so that, such measure

35. In this regard, according to the settled case-law of the Court, derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary.[37] In order to satisfy this requirement, besides laying down clear and precise rules governing the scope and application of the measure in question, the legislation in question must impose minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. "It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing".[38]

36. In Schrems II, the CJEU has stressed that legislation of a third country which does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter. Indeed, according to the case law, a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned.[39]

37. Regarding the **principle of necessity**, the CJEU has made clear that legislations "authorising, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union (...) without any 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 the data and its use entail", do not comply with that principle.[40] In particular, laws permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[41]

38. Likewise, however this time when assessing a Member State law and not a third country law, the CJEU held in La Quadrature du Net and others, that "legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data retained and the objective pursued".[42] In the same context, in Privacy International, it also held that the legislator "must

---

can meet the requirement of proportionality only in situations in which the Member State concerned is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and, among other conditions, provided that the duration of the retention is limited to what is strictly necessary (§§174-177).

[37] Schrems II, §176, including cited jurisprudence.

[38] Schrems II, § 175.

[39] Schrems II, § 180.

[40] Schrems I, § 93 with further references. See, however this time in relation to a Member State law and not a third country law, Privacy International, § 71, including cited jurisprudence. In this case, the Court stated that a Member State legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by the Directive on privacy and electronic communication, read in light of the Charter (§81).

[41] Schrems I, §94.

[42] La Quadrature du Net and others, § 133. In this context, the Court confirmed that legislative measures which provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data, are

rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue".[43]

Guarantee C - Independent oversight mechanism

39. The EDPB 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 public authority for further processing. The ECtHR has specified multiple times 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[44] (e.g. an administrative authority or a parliamentary body). The independent oversight over the implementation of surveillance measures was also taken into account by the CJEU in the Schrems II judgment.[45]

40. The ECtHR specifies that while prior (judicial) authorization of surveillance measures is an important safeguard against arbitrariness, regard must also be given to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of actual abuse.[46] In the Schrems II case, the CJEU also took into account the scope of the supervisory role of the oversight mechanism, which did not cover the individual surveillance measures.[47.]

41. With regard to Member States law, the CJEU identified a number of measures which are in compliance with EU law only if they are subject to effective review carried out by a court or an independent administrative authority whose decision is binding. The aim of that review is to verify that a situation justifying the measure exists and the conditions and safeguards that must be laid down are observed.[48] For real-time collection of traffic and location data, the review should allow to check ex ante, inter alia, whether it is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the measures may take place without such prior review; however, the Court still requires that the subsequent review takes place within a short time.[49]

42. As to the independence of oversight mechanisms in relation to surveillance, the findings of the CJEU concerning the independence of a body in the context of redress could be taken into account (see

precluded by the Directive on privacy and electronic communication, read in light of the Charter. By contrast, the Court ruled that, in situations of a serious threat to national security that is shown to be genuine and present or foreseeable, the legislator may allow, for safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data. Such measure must however meet specific conditions. In particular, the instruction may be given only for a period that is limited in time to what is strictly necessary, which may be extended if that threat persists (§168).

[43] Privacy International, § 78, including cited jurisprudence. In Privacy International, as regards an authority's access to personal data provided under a Member State law, the Court ruled that "general access to all retained data**,** regardless of whether there is any link, at least indirect, with the aim pursued, cannot be regarded as being limited to what is strictly necessary" (§77 -78).

[44] ECtHR, Klass, §§17, 51.

[45] Schrems II, §§ 179, 183.

[46] ECtHR, Big Brother Watch under appeal §§319-320.

[47] Schrems II, § 179.

[48] CJEU, La Quadrature du Net and others, §§ 168, 189.

[49] CJEU, La Quadrature du Net and others, § 189.

infra under guarantee D). Furthermore, the case law of the ECtHR may offer additional elements. This Court has expressed its preference for a judge to be responsible to maintain oversight. However, it is not excluded that another body may be responsible, "as long as it is sufficiently independent from the executive"[50] and "of the authorities carrying out the surveillance, and [is] vested with sufficient powers and competence to exercise an effective and continuous control".[51]The ECtHR added that "the manner of appointment and the legal status of the members of the supervisory body"[52] 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."[53] The ECtHR also "notes that it is essential that the supervisory body has access to all relevant documents, including closed materials".[54] Finally, the ECtHR takes into account "whether the supervisory body's activities are open to public scrutiny".[55]

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

43. 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 considers that they are not or have not been respected. The CJEU explained in Schrems I 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."[56]

44. When assessing a Member State law allowing real time collection of traffic and location data, the Court considered that notification is necessary "to enable the persons affected to exercise their rights under Articles 7 and 8 of the Charter to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased, as well as to avail themselves, in accordance with the first paragraph of Article 47 of the Charter, of an effective remedy before a tribunal".[57] Nevertheless, it also recognized that the notification of persons whose data has been collected or analysed must occur only to the extent that and as soon as the notification no longer jeopardizes the tasks for which those authorities are responsible.[58]

---

[50] ECtHR, Zakharov, §258, Iordachi and Others v. Moldova, §§ 40 and §§ 51 and Dumitru Popescu v. Romania, §§ 70¬73.

[51] ECtHR, Klass §56 and Big Brother Watch under appeal §318

[52] ECtHR, Zakharov, §278.

[53] ECtHR, Zakharov, §278.

[54] ECtHR, Zakharov, §281.

[55] ECtHR, Zakharov, §283.

[56] CJEU, Schrems I, §95.

[57] See § 190 of La Quadrature du Net and others and CJEU, Opinion 1/15, §220.

[58] See § 191 of La Quadrature du Net and others.

45. For the ECtHR, as well, the question of an effective remedy is inextricably linked to the notification of a surveillance measure to the individual once the surveillance is over. In particular, the Court found that "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".[59] The ECtHR thus acknowledged that in some cases there might be no notification, however an effective remedy must be provided. In this case, this Court has made clear, for instance in the Kennedy case, that a court offers sufficient redress possibilities, if it meets a series of criteria, i.e. 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 and that there is no evidential burden to be overcome in order to lodge an application with it.[60] In undertaking its examination of complaints by individuals, the court should have access to all relevant information,[61] including closed materials. Finally, it should have the powers to remedy non-compliance.[62]

46. Article 47 of the Charter refers to a tribunal, even though in language versions other than English the preference is given to the word "court",[63] while the ECHR only obliges Members States to ensure that "everyone whose rights and freedoms are violated shall have an effective remedy before a national authority",[64] which does not necessarily need to be a judicial authority.[65]

47. The CJEU, in the context of the Schrems II judgment when assessing the adequacy of the level of protection of a third country, has reiterated that "data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data".[66] In the same context, the CJEU considers that an effective judicial protection against such interferences can be ensured not only by a court, but also by a body[67] which offers guarantees essentially equivalent to those required by Article 47 of the Charter. In its Schrems II ruling, the CJEU both underlined that the independence of the court or body has to be ensured, especially from the executive, with all necessary guarantees, including with regards to its conditions of dismissal or revocation of the appointment,[68] and that the powers which should be granted to a court have to be compliant with the requirements of Article 47 of the Charter. In this

[59] ECtHR, Zakharov, §234.
[60] ECtHR, Kennedy, § 190.
[61] The EDPB 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).
[62] ECtHR, Kennedy §167.
[63] The word tribunal is for example translated as "Gericht" in German and "gerecht" in Dutch.
[64] Article 13 ECHR.
[65] ECtHR, Klass §67.
[66] See § 194 Schrems II.
[67] See §197 Schrems II in which the Court expressly uses this word.
[68] See § 195 Schrems II.

regard, the body[69] shall be granted the power to adopt decisions that are binding on the intelligence services, in accordance with legal safeguards on which data subjects could rely.[70]

4. FINAL REMARKS

48. The four European Essential Guarantees are to be seen as core elements to be found when assessing the level of interference with the fundamental rights to privacy and data protection. They should not be assessed independently, as they are closely interlinked, but on an overall basis, reviewing the relevant legislation in relation to surveillance measures, 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.

49. These guarantees require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework.

50. 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".[71]

51. Consequently, the assessment of the third country surveillance measures against the EEG may lead to two conclusions:

- The third country legislation at issue does not ensure the EEG requirements: in this case, the third country legislation would not offer a level of protection essentially equivalent to that guaranteed within the EU.

- The third country legislation at issue satisfies the EEG.

52. When assessing the adequacy of the level of protection, pursuant to Article 45 GDPR, the Commission will have to evaluate whether the EEG are satisfied as part of the elements to be considered to guarantee that the third country legislation as a whole offers a level of protection essentially equivalent to that guaranteed within the EU.

53. When data exporters rely, along with the data importers, on appropriate safeguards under Article 46 of the GDPR, given the requirements of the third country legislation specifically applicable to the data transferred, they would need to ensure that an essentially equivalent level of protection is effectively achieved. In particular, where the law of the third country does not comply with the EEG requirements, this would imply to ensure that the law at stake will not impinge on the guarantees and safeguards surrounding the transfer, in order for a level of protection essentially equivalent to that guaranteed within the EU to be still provided.

[69] See §197 Schrems II in which the Court expressly uses this word.

[70] See § 196 Schrems II.

[71] ECtHR, Kennedy §153.

54. The EDPB has issued further guidelines and recommendations to be taken into account to proceed with the assessment, depending on the transfer tool to be used and on the necessity to provide appropriate safeguards, including as the case may be, supplementary measures.[72]

55. Furthermore, it should be noted that the European Essential Guarantees are based on what is required by the law. The EDPB underlines that the European Essential Guarantees are based on the fundamental rights that apply to everyone, irrespective of their nationality.

56. The EDPB reiterates that the European Essential Guarantees are a referential standard when assessing the interference, entailed by third country surveillance measures, in the context of international data transfers. These standards stem from EU law and the jurisprudence of the CJEU and the ECtHR, which is binding on Member States.

[72] Adequacy Referential WP 254 rev.01, Revised and Adopted 6 February 2018; EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 November 2020.