Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive

Adopted on 2 February 2021

Table of contents

The European Data Protection Board

Having regard to Article 51 (1) (b) of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[1],

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

HAS ADOPTED THE FOLLOWING RECOMMENDATIONS

1. INTRODUCTION

1. The Working Party Article 29 (WP29) has published a working document[2] on adequacy referential under the General Data Protection Regulation (GDPR)[3]. This working document was endorsed by the European Data Protection Board (EDPB) at its first plenary.

2. As stated in Declaration N°21 annexed to the Lisbon Treaty, specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union (TFEU) may prove necessary because of the specific nature of these fields.

3. On this basis, the EU legislator adopted Directive (EU) 2016/680 (the Law Enforcement Directive, hereinafter the 'LED') laying down the specific rules with regard to the processing of personal data by competent authorities for the purposes of the **prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against the prevention of threats to public security**.

4. The LED determines the grounds allowing the transfer of personal data to a third country or an international organisation in this context. One of the grounds for such transfer is the decision by the European Commission that the third country or international organisation in question ensures an adequate level of protection.

5. Where the working document WP254.rev01 on adequacy referential aims to provide guidance to the European Commission on the level of data protection in third countries and international organisations under the GDPR, the present document aims to provide similar guidance under the LED. It establishes in this context the core data protection principles that have to be present in a

[1] OJ L 119, 4.5.2016, p. 89.
[2] WP254.rev01 adopted by WP 29 on 28 November 2017 as last revised and adopted on 6 February 2018. It updates Chapter I of the Working Document 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', WP12, adopted by WP29 on 24 July 1998.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 26 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 (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

third country or an international organisation legal framework to ensure essential equivalence with the EU framework within the scope of the LED (i.e. for processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties). In addition, it may guide third countries and international organisations interested in obtaining adequacy.

6. The present document focuses solely on adequacy decisions. These are implementing acts of the European Commission according to Article 36(3) of the LED.

2. CONCEPT OF ADEQUACY

7. The LED sets the rules for the transfer of personal data to third countries and international organisations to the extent that such transfers fall within its scope. The rules on international transfers of personal data are laid down in Chapter V of the LED, in particular its Articles 35 to 39.

8. Pursuant to Article 36 of the LED, data transfers to a third country or an international organisation may take place if a third country, a territory or one or more specified sectors within a third country or an international organisation ensure an adequate level of protection. It stems from the Court of Justice of the European Union (CJEU) case law[4] that this provision, must be read in the light of Article 35 of the LED, entitled 'General principle for transfers of personal data', which lays down that 'all provisions [in Chapter V of the LED] shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined'.

9. Where the European Commission has decided that such adequacy level of protection is ensured, transfers of personal data to that third country, territory, sector or international organisation can take place, without the need to obtain any specific authorisation, except where another Member State from which the data were obtained has to give its authorisation to the transfer as provided in Articles 35 and 36 and Recital 66 of the LED. This is without prejudice to the need for the processing of data by the concerned Member States' authorities to comply with the national provisions adopted pursuant to Directive (EU) 2016/680.

10. This concept of 'adequate level of protection' which already existed under Directive 95/46[5] and Council Framework Decision 2008/977/JHA[6] has been further developed by the CJEU in this context and, recently, in the framework of the GDPR.

11. As specified by the CJEU, while the level of protection in the third country must be essentially equivalent to that guaranteed in the EU, 'the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the European Union' but 'those means must nevertheless prove, in practice, effective'[7]. The

[4] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 16 July 2020, ECLI:EU:C:2020:559, §92 (Schrems II).
[5] 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, OJ L 281, 23.11.1995, p. 31.
[6] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.
[7] Case C−362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, ECLI:EU:C:2015:650, §§73 and 74 (Schrems I).

adequacy standard therefore does not require to mirror point by point the EU legislation, but to establish the essential - core requirements of that legislation.

12. In this context, the court also clarified that a Commission adequacy decision should contain any finding regarding the existence, in the third country, of rules adopted by this country intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to this third country, interference which the public entities of that country would be *authorised* to engage in when they pursue legitimate objectives, such as national security[8].

13. The purpose of adequacy decisions by the European Commission is to formally confirm, with binding effects on Member States[9] including their competent data protection authorities[10], that the level of data protection in a third country or an international organisation is essentially equivalent to the level of data protection in the European Union. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors[11].

14. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules[12].

3. PROCEDURAL ASPECTS FOR ADEQUACY FINDINGS UNDER THE LED

15. In order to fulfil its task in advising the European Commission according to Article 51 (1) (g) of the LED, the EDPB should receive all relevant documentation, including relevant correspondence and the findings made by the European Commission. It is absolutely necessary, that all relevant documents are transmitted sufficiently in advance and translated into English to the EDPB to enable informed and useful discussions before the final adoption of adequacy decisions. Where the legal framework is complex, this should include any report prepared on the data protection level of the third country or international organisation. In any case, the information provided by the European Commission should be exhaustive and put the EDPB in a position to assess the analysis carried out by the Commission regarding the level of data protection in the third country or international organisation.

[8] Schrems I, §88.
[9] Article 288 (2) TFEU.
[10] Schrems I, §52.
[11] Recital 67 LED.
[12] Schrems I, §§72-74 and CJEU Opinion 1/15, on the draft agreement between Canada and the European Union, 26 July 2017, ECLI:EU:C:2017:592 (Opinion 1/15), § 134: 'That right to the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law continues where personal data is transferred from the European Union to a non-member country. Even though the means intended to ensure such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from EU law are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union'.

16. The EDPB will provide an opinion on the European Commission's findings in due time, identifying insufficiencies in the adequacy framework, if any, and providing possible recommendations where necessary.

17. According to Article 36 (4) of the LED it is upon the European Commission to monitor - on an ongoing basis - developments that could affect the functioning of an adequacy decision.

18. Article 36 (3) of the LED provides that a periodic review must take place at least every four years. This is, however, a general time frame which must be adjusted to each third country or international organisation with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organisation in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.

19. Given its task to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organisation, no longer ensures an adequate level of protection, the EDPB must, in due time, receive meaningful information regarding the monitoring of the relevant developments in that third country or international organisation by the EU Commission. Hence, the EDPB should be kept informed of any review process and review mission in the third country or to the international organisation. The EDPB recommends being invited to participate in these review processes and missions, as it was foreseen in the Privacy Shield decision and is foreseen in the adequacy decision concerning Japan.

20. It should also be noted that, according to Article 36 (5) of the LED, the European Commission has the power, where the third country or international organisation no longer ensures an adequate level of protection, to repeal, amend or suspend existing adequacy decisions. The procedure to repeal, amend or suspend involves the EDPB by requesting its opinion in accordance with Article 51 (1) (g) of the LED.

21. Furthermore, without prejudice to the powers of prosecutorial authorities, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities or to engage in legal proceedings[13]. It stems in particular from the CJEU Schrems I ruling, that data protection authorities must be able to engage in legal proceedings before the national courts if they find a claim by a person against an adequacy decision well founded[14]. The Schrems II ruling confirmed this assessment[15].

[13] See Article 47 (5) LED and Recital 82 thereof.

[14] See Schrems I, §65: 'It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity'.

[15] See Schrems II, §120: 'Even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of his or her rights and freedoms in regard to the processing of personal data relating to him or her, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity'.

4. EU STANDARDS FOR ADEQUACY IN THE POLICE COOPERATION AND JUDICIAL COOPERATION IN CRIMINAL MATTERS

22. On substance, adequacy decisions should focus on the assessment of the existing legislation of the third country concerned as a whole, in theory and practice, in light of the assessment criteria set out in Article 36 of the LED. A third country or international organisation's system must contain the following basic general, procedural and enforcement data protection principles and mechanisms.

23. Article 36 (2) of the LED establishes the elements that the European Commission shall take into account when assessing the adequacy of the level of protection in a third country or international organisation.

24. In particular, the Commission shall take into consideration the rule of law, respect for human rights and fundamental freedoms[16], relevant legislation, as well as the implementation of such legislation, effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are transferred, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organisation has entered into.

25. It is therefore clear that any meaningful analysis of adequate protection must comprise two basic elements: the content of the rules applicable and the means for ensuring their effective implementation in practice. It is upon the European Commission to verify – on a regular basis - that the rules in place are effective in practice.

26. The core of data protection general principles and procedural and enforcement requirements, which could be seen as a minimum requirement for protection to be adequate, are derived from the Charter of Fundamental Rights of the EU (Charter) and the LED. General provisions regarding data protection and privacy in the third country are not sufficient. On the contrary, specific provisions addressing concretely the right to data protection in the law enforcement area must be included in the third country's or international organisation's legal framework. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union. These provisions have to be enforceable.

27. Furthermore, regarding the principle of proportionality[17], the CJEU 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[18] and by verifying that the **importance of the public**

[16] When assessing the legal framework of the third country, the possibility that death penalty or any form of cruel and inhuman treatment could be imposed on the basis of data transferred from the EU should be taken into account. Indeed, should such penalty or treatment be foreseen in the law of the third country, additional safeguards should be found in the third country legal framework to ensure that data transferred from the EU would not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment (e.g. an international agreement imposing conditions on the transfer, a commitment by the third country not to impose death penalty or any form of cruel and inhuman treatment on the basis of data transferred from the EU or a death penalty moratorium).

[17] Article 52(1) of the Charter.

[18] 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

interest objective pursued by that limitation is proportionate to that seriousness, on the other hand[19].

28. According to the case-law of the CJEU, 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[20]. Derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary[21]. In order to satisfy this requirement, besides laying down clear and precise rules governing the scope and application of the measure in question, the concerned legislation 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'[22].

29. The EDPB has adopted Recommendations identifying essential guarantees reflecting the jurisprudence of the CJEU and the European Court of Human Rights (ECtHR) in the field of surveillance to be found in the law of the third country when assessing the interferences of such third country surveillance measures with the rights of data subjects in case the data are transferred to that third country under the GDPR[23]. To assess whether Article 36(2)a) LED conditions are fulfilled, the EDPB considers that the guarantees set out in these Recommendations have to be taken into account when assessing the adequacy of a third country under the LED in the field of surveillance, bearing in mind further specific conditions in the field of surveillance in this context.

30. In relation to Article 36(2)b) requirement, the third country should not only ensure effective independent data protection supervision but also provide for cooperation mechanisms with the Member States' data protection authorities[24].

31. In relation to Article 36(2) c) requirement, apart from the international commitments the third country or international organisation has entered into, consideration should also be given to obligations arising from the third country's or international organisation's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations, in particular the third country's accession to other international agreements on data protection, e.g. the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account (Convention 108[25] and its modernised version, Convention 108+). The third country's compliance with principles enshrined in international documents such as the Council of Europe Practical Guide on the use of personal

authorities with a means of accurately and permanently tracking the movements of users of mobile telephones (...)' (joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, 6 October 2020, ECLI:EU:C:2020:791, §187, including cited jurisprudence).

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

[20] Schrems II, §180.

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

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

[23] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020.

[24] Recital 67 LED.

[25] Recital 68 LED.

data in the police sector: how to protect personal data while combatting crime may also be taken into account.

32. An adequacy decision should ensure that through the substance of privacy and data protection rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection, including for data in transit to this third country. As underlined by the CJEU in the Schrems II ruling, the high level of protection afforded should also be ensured while data are being transferred to a third country[26].

33. Finally, when adopting an adequacy decision with regard only to a territory or a specified sector in a third country, the European Commission should take into account clear and objective criteria, such as referring to specific processing activities or the scope of applicable legal standards and legislation in force in the third country[27].

A. General principles and safeguards

a) Concepts

34. Basic data protection concepts should exist. These do not have to mirror the LED terminology but should reflect and be consistent with the concepts enshrined in the European data protection law. By way of example, the LED includes the following important concepts: 'personal data', 'processing of personal data', 'competent authorities', 'data controller', 'data processor', 'recipient', 'sensitive data', 'accuracy', 'profiling', 'data protection by design and by default', 'supervisory authority' and 'pseudonymisation'.

b) Lawfulness and fairness of the processing of personal data (Article 4 - Recital 26)

35. 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'[28]. However, in the context of law enforcement, it should be noted that the performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject should not provide a legal ground for processing personal data by competent authorities[29].

36. This legal basis should lay down clear and precise rules governing the scope and application of the relevant data processing activities and imposing minimum safeguards[30]. In addition, the CJEU recalled that 'legislation must be legally binding under domestic law'[31].

[26] See §93.
[27] Recital 67 LED.
[28] See Schrems II, §173.
[29] Recital 35 LED also states that '[w]here the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties'.
[30] See Schrems II, §175 and §180 and Opinion 1/15, § 139 and the case law cited.
[31] See case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, 6 October 2020, ECLI:EU:C:2020:790, §68 – It should also be clear that in the French version of the judgment, the CJEU uses the word '*réglementation*' which is broader than only acts of Parliament.

37. To be lawful, the data processing[32] should be necessary for the performance of a task carried out by a competent authority for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguards against and the prevention of threats to public security[33]. These purposes should be provided in national law.

38. Personal data shall be processed fairly. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[34].

c) The purpose limitation principle (Article 4)

39. The specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data[35].

40. Data should be processed for a specified, explicit and legitimate purpose within the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[36], including the safeguarding against and the prevention of threats to public security within the third country and subsequently used for any of these purposes insofar as this is not incompatible with the original purpose of the processing, (e.g. for parallel enforcement proceedings or archiving in the public interest, scientific, statistical or historical use for such purposes) and subject to appropriate safeguards for the rights and freedoms of data subjects. If personal data are processed by the same or another controller (competent authority[37]) for a purpose of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties other than that for which they have been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose[38]. The existence of a mechanism to inform the relevant Member States' competent authorities of such further processing of data should also be taken into account[39]. In addition, in any case the level of protection of natural persons provided for in the Union by the LED should not be undermined including in those cases where personal data are transmitted from the third country to controllers or processors in the same third country[40].

[32] Processing of personal data wholly or partly by automated means, and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
[33] Competent authorities are any public authority competent for such purposes or any other body or entity entrusted by law to exercise public authority and public powers for such purposes.
[34] Recital 26 LED.
[35] Recital 26 LED.
[36] It includes 'police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence' (Recital 12 LED). It is to be distinguished from a national security purpose or from activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) (Recital 14 LED).
[37] See footnote 33.
[38] Recital 29 LED.
[39] Such mechanism could be for instance mutually agreed handling codes, a notification obligation under an international instrument, including possible automated notifications, or other similar transparency measures.
[40] Recital 64 LED.

d) Specific conditions for further processing for other purposes (Article 9)

41. Concerning further processing or disclosure of data transferred from the EU for other purposes than law enforcement purposes, such as national security purposes, it should also be provided by law, be necessary and proportionate. The existence of a mechanism to inform the relevant Member States' competent authorities of such further processing of data should also be taken into account[41]. Here as well, once further processed or disclosed, the data should benefit from the same level of protection as when they were processed initially by the receiving competent authority.

e) The data minimisation principle

42. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed. In particular, the application of data protection by design and by default requirements, such as limited entry fields (structured communications) or automated and non-automated quality checks, should be taken into account.

f) The principle of data accuracy

43. The data should be accurate and where necessary kept up to date. Nevertheless, the principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made[42].

44. It should be ensured that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available[43] and that procedures are foreseen to correct or delete inaccurate data. In particular, any classification system of the information processed, as to the reliability of the source and as to the facts verification level[44], should be taken into account.

g) The data retention principle

45. Data should be kept for no longer than is necessary for the purposes for which they are processed. Appropriate mechanisms should be established for the erasure of personal data; it may be a fixed period or a periodic review of the need for the storage of personal data (or a combination of both: fixed maximum period and periodic review at certain intervals)[45]. Personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use should be subject to appropriate safeguards (e.g. regarding access)[46].

h) The security and confidentiality principle (Article 29, Recitals 28 and 71)

46. Any entity processing personal data should ensure that the data are processed in a manner that ensures security of the personal data including by preventing unauthorised access to or use of personal data and the equipment used for the processing. This includes protection against, and

[41] See footnote 39.
[42] Recital 30 LED.
[43] Recital 32 LED.
[44] E.g. 4x4 grids for reliability assessments and handling codes.
[45] Article 5 LED.
[46] Recital 26 LED.

appropriate measures to address, unlawful processing as well as accidental loss, destruction or damage, using appropriate technical and organisational measures. When determining the level of the security, the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons should be taken into consideration.

47. Secure channels of communication between Member States' authorities transferring the personal data and third States' receiving authorities should be ensured.

i) The transparency principle (Article 13, Recitals 26, 39, 42, 43, 44, 46)

48. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing[47].

49. Information on all the main elements of the processing of their personal data should be made available to the individuals. This information should be easily accessible and easy to understand, using clear and plain language. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to them[48] and other information insofar as this is necessary to ensure fairness.

50. Some exceptions to this right of information may exist. Such limitation should however be allowed by a legislative measure and be necessary and proportionate to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others, as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned. Such restrictions should also be considered and assessed taking into account the possibility of lodging a complaint with a supervisory authority or seeking a legal remedy. In any case, any possible restriction should be temporary and not blanket and should be framed by similar conditions, safeguards and limitations to those required under the Charter and the ECHR, as interpreted in the case-law of the CJEU and by the ECtHR respectively, and in particular respect the essence of those rights and freedoms.

j) The right of access, to rectification and erasure (Articles 14 and 16)

51. The data subject should have the right to obtain confirmation about whether or not data processing concerning him/her is taking place and where that is the case, have access to his/her data. This right should at least comprise certain information about the processing such as the purposes of and legal basis for the processing, the right to lodge a complaint with the supervisory authority or the categories of personal data concerned[49]. This is particularly important in case transparency is achieved through general notice (e.g. information on the authority's website).

52. The data subject should have the right to obtain rectification of his/her data for specified reasons, for example, where they are shown to be inaccurate or incomplete. The data subject should also have the right to have his/her data erased when for example their processing is no longer necessary or is unlawful.

[47] Recital 26 LED.
[48] Both the substantive rights (right of access, to rectification etc...) and the right to redress.
[49] Article 14 LED.

53. The exercise of those rights should not be excessively cumbersome for the data subject.

k) Restrictions on data subject rights

54. Possible restrictions to these rights could exist in order to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others, as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned. Such restrictions should also be considered and assessed taking into account the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

l) Restriction on onward transfers (Article 35, Recitals 64-65)

55. The onward transfers of personal data by the initial recipient to another third country or international organisation must not undermine the level of protection, provided for in the Union, of natural persons whose data is transferred. Therefore, such onward data transfers should be permitted only where the continuity of the level of protection afforded under EU law is ensured[50]. In particular, the further recipient (i.e. the recipient of the onward transfer) should be a competent authority for law enforcement purposes[51] and such onward transfers of data may only take place for limited and specified purposes and as long as there is a legal ground for that processing.

56. The existence of a mechanism for the relevant Member State's competent authorities to be informed and authorise such onward transfer of data has to also be taken into account. The initial recipient of the data transferred from the EU should be liable and be able to prove that the relevant competent authority of the Member State has authorised the onward transfer[52] and that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision concerning the third country to which the data would be onward transferred[53].

m) Accountability principle (Article 4(4))

57. The controller should be responsible for and be able to demonstrate compliance with the data protection principles found in Article 4 of the LED.

[50] See also Opinion 1/15.
[51] See footnote 33.
[52] In this context, the existence of an obligation or a commitment to implement relevant handling codes defined by the transferring Member States' authorities should be taken into account.
[53] The above requirements are without prejudice to the specific conditions for onward transfers to an adequate country set out under the LED ((Article 35 (1) c) and e)).

B. Examples of additional principles to be applied to specific types of processing

a) Special categories of data (Article 10 and Recital 37)

58. Specific safeguards should exist where 'special categories of data' are involved[54], addressing the specific risks involved[55]. These categories should reflect those enshrined in Article 10 of the LED. Processing of special categories of data should therefore be subject to specific safeguards and only be allowed where strictly necessary under certain conditions for instance to protect the vital interest of an individual.

b) Automated decision making and profiling (Article 11 and Recital 38)

59. Decisions based solely on automated processing (automated individual decision-making), including profiling, which produce adverse legal effects or significantly affect the data subject, should only take place under certain conditions established in the third country legal framework[56].

60. In the European Union framework, such conditions include, for example, the provision of specific information to the data subject and the right to obtain human intervention on the part of the controller, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision.

61. The third country law should, in any case, provide for necessary safeguards for the data subject's rights and freedoms. In this regard, the existence of a mechanism to inform the relevant Member State's competent authorities of any further processing such as the use of the transferred data for large scale profiling, should also be taken into account.

c) Data protection by design and by default (Article 20)

62. When assessing adequacy, attention should be paid to the existence of an obligation for controllers to adopt internal policies and implement measures which adhere to the principles of data protection by design and data protection by default taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to adopt appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.

[54] Such special categories are also known as 'sensitive data' in Recital 37 LED.
[55] Such additional safeguards could be e.g. specific security measures, limited access rights for staff, restrictions as to further processing, automated decision-making, onward sharing or onward transfers.
[56] Opinion 1/15, § 173.

C. Procedural and enforcement mechanisms

63. Although the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union[57], a system consistent with the European one must be characterized by the existence of the following elements:

a) Competent independent supervisory authority (Articles 36(2)b and 36(3) and Recital 67)

64. One or more independent supervisory authorities, tasked with ensuring and enforcing compliance with data protection and privacy provisions in the third country should exist. The supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In that context, the supervisory authority should have all adequate enforcement powers to effectively ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able, on its own initiative, to conduct investigations. It should also be tasked with assisting and advising data subjects in exercising their rights (see also point c below). The adequacy decisions should identify, where applicable, that supervisory authority or authorities and the cooperation mechanisms with the supervisory authorities of the Member States to enforce data protection rules.

b) Effective implementation of data protection rules

65. A third country system should ensure a high degree of awareness among data controllers and those processing personal data on their behalf of their obligations, tasks and responsibilities, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as can systems of direct verification by authorities, auditors, or independent data protection officials.

66. A third country data protection framework should oblige data controllers or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority. Such measures should include keeping records or log files of data processing activities for an appropriate period of time. They may also include for example data protection impact assessments, the designation of a data protection officer or data protection by design and by default.

c) The data protection system shall facilitate the exercise of data subject rights (Articles 12, 17 and 46 LED)

67. A third country data protection framework should oblige data controllers to facilitate the exercise of data subject rights referred to under section A j) above and provide that its supervisory authority, upon request, inform any data subject concerning the exercise of their rights[58].

d) The data protection system shall provide appropriate redress mechanisms

68. Although there is currently no case law in relation to the adequacy of a third country legal system under the LED, the CJEU has interpreted the fundamental right to effective judicial protection as

[57] Schrems I, §74.
[58] The exercise of data subjects' rights could be either direct or indirect.

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[59] in compliance with the conditions laid down in that article.

69. According to settled case law of the CJEU, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, 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 her, 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[60].

70. The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to ensure compliance.

71. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling any infringements of the right to data protection and respect for private life to be identified and punished in practice.

72. Where rules are not complied with, the data subject whose personal data are transferred to the third country should be provided as well with effective administrative and judicial redress in the third country, including for compensation for damages as a result of the unlawful processing of his/her personal data. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

[59] The CJEU considers that an effective judicial protection can be ensured not only by a court, but also by a body which offers guarantees essentially equivalent to those required by Article 47 of the Charter (see Schrems II, §197). This might be relevant in particular for international organisations.
[60] Schrems II, §§187 and 194, including cited jurisprudence.