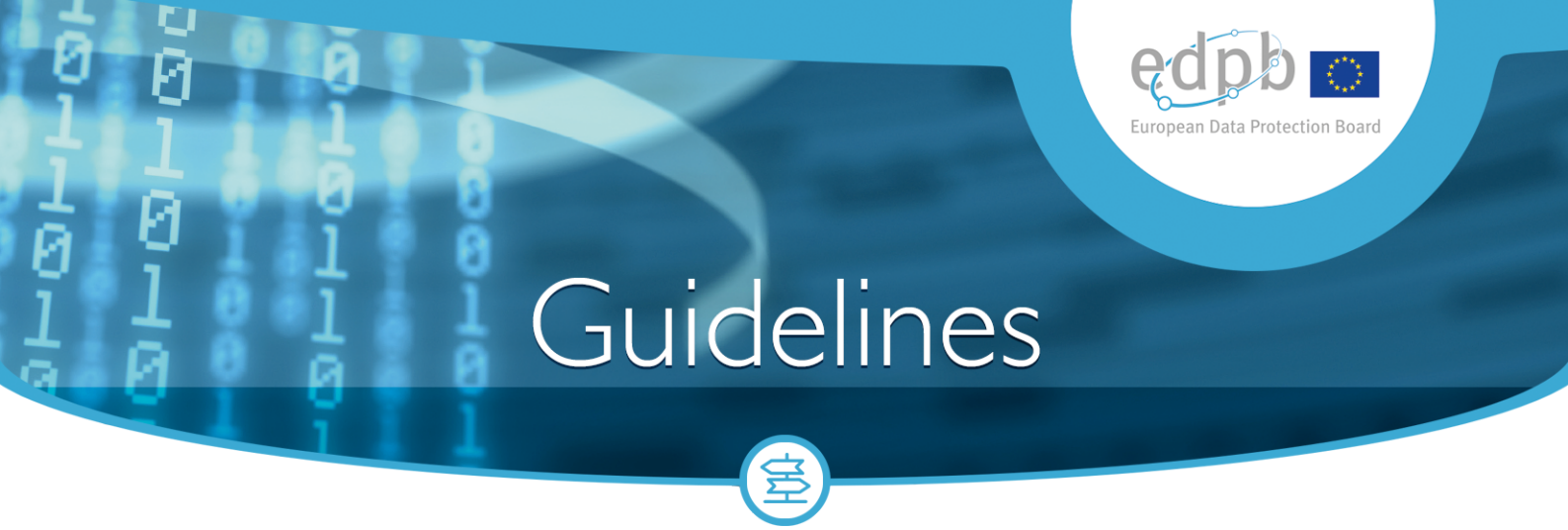

Guidelines 01/2023 on Article 37 Law Enforcement Directive

Version 2.0

Adopted on 19 June 2024

Version history

Version 1.0	27 September 2023	Adoption of the Guidelines for public consultation
Version 2.0	19 June 2024	Adoption of the Guidelines after public consultation

Executive summary

These guidelines provide guidance on the application of Article 37 LED, in particular on the legal standard for appropriate safeguards to be applied by competent authorities pursuant to Article 37(1)(a) and (b) LED and, accordingly, on the relevant factors for the assessment of whether such safeguards exist. These guidelines therefore include an indication as to the EDPB's expectations of Member States, as negotiating parties, when envisaging concluding or amending a legally binding instrument between the concerned Member State(s) and a third country or international organisation pursuant to Article 37(1)(a) LED.

The EDPB notes that Article 35(3) LED applies to transfers carried out under Article 37 LED. Article 37 LED should therefore be applied in light of the principle that the level of data protection applicable in the European Union must not be undermined by the transfer of personal data to another jurisdiction. The EDPB concludes that Article 37 LED requires an essentially equivalent level of data protection in the recipient third country or international organisation. However, this requirement relates to the specific data transfer or category of transfers at hand. Pursuant to Article 37 LED, essential equivalence to the protection guaranteed under the LED should be ensured for that particular case and not necessarily with regard to the entire existing legislation in the third country or international organisation.

The EDPB has already adopted Recommendations on the adequacy referential under the LED, addressing which data protection principles have to be present to ensure essential equivalence with the EU framework within the scope of the LED. The EDPB considers that the principles and safeguards outlined in these Recommendations apply in substance in the context of Article 37 LED, i.e. with regard to the specific transfer or category of transfers.

A legally binding instrument in the meaning of Article 37(1)(a) LED has to be concluded by the entity empowered to enter into obligations with respect to the safeguards provided in the instrument. The international agreement should thus have the force of law. Such legally binding instrument can be enforced by the Parties and by data subjects whose personal data processing is governed by the agreement. The legally binding instrument should contain all relevant rules to allow overcoming any shortcomings or limitations of the legislation of the third country or international organisation in terms of data protection by setting a framework of appropriate safeguards that afford an essentially equivalent level of data protection.

The EDPB considers that the use of a legally binding instrument regulating personal data transfers between the Parties should, in the absence of an adequacy decision, in principle, take precedence, over an assessment by the controller according to Article 37(1)(b) LED as it provides more legal certainty, transparency, foreseeability, stability, consistency and guarantees on the effective application of data protection safeguards.

In this context, the EDPB recalls its Statement on international agreements including transfers, adopted on 13 April 2021, inviting Member States to assess and, where necessary, review their international agreements that involve international transfers of personal data. The EDPB emphasizes that consideration should be given to the aim of bringing those agreements in line with the LED requirements for data transfers, where this is not yet the case, to ensure that the level of protection of natural persons guaranteed by the LED is not undermined when personal data is transferred outside the Union.

With respect to Article 37(1)(b) LED and in light of the above-mentioned greater guarantees offered by legally binding instruments, competent authorities may rely on such an assessment only when this

is based on a careful analysis of the relevant legal framework and practices showing that the transfers in question are subject to appropriate safeguards. In assessing the risks surrounding the transfers for the purpose of Article 37(1)(b) LED, competent authorities should examine the protection of the personal data to be transferred in view of the risks their sharing with third countries raises for the fundamental rights and freedoms of the data subjects, their legitimate interests and those of other persons concerned. Knowing in detail the circumstances surrounding the data transfers conducted or to be conducted is necessary to be able to identify these risks to the rights and freedoms of natural persons, and in particular to the right to data protection, and any safeguards that are appropriate to mitigate them.

As for any other processing operation, a competent authority must be aware of and consider in a granular manner the nature, scope, context and purposes of the transfer. More specifically, competent authorities may analyse and categorise their transfers considering characteristics relevant to assess the risks posed to fundamental rights of the data subjects such as the specific purposes of the transfer, the quantity of data transferred or the seriousness of a criminal offence.

There may be cases where appropriate safeguards already follow from the third country's international commitments, its legislation and practices. In other cases, competent authorities may need to provide, to the extent they are legally competent, for additional safeguards in light of the features of the specific transfer mentioned above, to ensure an essentially equivalent level of protection to that guaranteed under the LED and national law. The commitment of the receiving authority in the third country to respect and comply with such additional safeguards is necessary so that they are effective.

The fact that the transfer mechanisms provided in Articles 36 to 38 LED operate in cascade in general also affects the accountability obligations of the controller. The accountability obligations on the controller when relying on Article 37(1)(b) LED are enhanced pursuant to Article 37(2) and 37(3) LED because it is the controller alone who determines, based on its own assessment, whether appropriate safeguards exist. This involves higher risks of inconsistencies, less transparency, and less legal certainty for data subjects in comparison with transfers legally framed by adequacy decisions or legally binding instruments.

With regard to the obligation imposed by Article 37(2) LED and taking into account the justifying reason for adopting this provision, competent authorities should inform their data protection authorities in regular intervals about the categories of transfers that were carried out under 37(1)(b) LED. The information submitted should include the receiving competent authorities as well as the number of transfers. This would allow supervisory authorities to have a general overview and to focus their action with regard to possible 'ex post' lawfulness control on specific categories of transfers.

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] (hereinafter "LED")

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

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. This document seeks to provide guidance as to the application of Article 37 of the LED on transfers of personal data by competent authorities of EU Member States (hereinafter "Member States") to third country authorities or international organisations competent in the field of law enforcement. In particular, these guidelines aim to provide clarity on the legal standard for appropriate safeguards to be applied by competent authorities pursuant to Article 37(1)(a) and (b) LED and, accordingly, on the relevant factors for the assessment of whether such safeguards exist.

2. These guidelines also intend to give an indication as to the expectations of the European Data Protection Board (hereinafter "EDPB") on the safeguards for the protection of personal data required to be put in place by a legally binding instrument pursuant to Article 37(1)(a) LED. The EDPB recommends Member States, as negotiating parties, to use these guidelines as a reference when envisaging concluding or amending such instruments.[2]

3. In this respect, these guidelines furthermore provide guidance to national supervisory authorities (SAs) where they are consulted or otherwise involved by Member States in the negotiation of instruments pursuant to Article 37(1)(a) LED or where they subsequently review the implementation of such instruments. These guidelines also address the role of SAs in the context of the controller's accountability obligations according to Article 37(2) and (3) LED.

4. The EDPB notes that there is an increasing call for guidance at EU level as to the practical application of Article 37 LED across Member States. In its recent position and findings on the application of the LED, the Council has considered that guidelines for Article 37 LED would be of particular importance for Member States.[3] To this end, the Council expresses that such guidance should be based on a pragmatic approach taking into account the practical needs of competent authorities.[4] The EDPB

[1] OJ L 119, 4.5.2016, p.89.
[2] See also Section 3.
[3] Council position and findings on the application of the 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, paragraph 19, 20 (https://data.consilium.europa.eu/doc/document/ST-13943-2021-INIT/en/pdf).
[4] *Ibid*, paragraph 20.

included the development of guidance for Article 37 LED in its work programme[5] and recognizes that the ability to exchange information, including personal data, is a key element for effective international cooperation in criminal matters. The EDPB wishes to emphasize that the transfer of personal data to third countries can only be permissible within and on the basis of the applicable legal framework and while ensuring a high level of protection of personal data.[6] In line with the tasks assigned to it in Article 51 LED, these Guidelines provide an interpretation by the EDPB of this legal framework and its binding requirements set out in the law.

2 ESSENTIAL ELEMENTS OF APPROPRIATE SAFEGUARDS

2.1 The notion of transfer

5. The transfer of personal data is a processing operation under Article 3(2) LED and, as such, is subject to any general condition the LED lays down for processing operations, in addition to those it imposes specifically on transfers.

6. Within the scope of Article 37 LED, the notion of "transfer" captures different scenarios. First, the term "transfer" under Article 37 covers direct transfers by a competent authority in the EU to authorities in a third country or to multiple third countries or to an international organisation, whether made on its own initiative or at the request of the recipient. Second, the term "transfer" also includes transfers to third countries via an intermediary, such as international organisations (e.g. Interpol). This includes, for example, making data available to third countries via international databases.

7. In addition, making available personal data to third countries by granting them direct access to national databases also qualifies as a transfer.[7] The remote access from a third country by an official of a competent authority of a Member State, such as a liaison officer, to national databases of this Member State does however not qualify as a transfer. In such cases, a transfer occurs the moment this official discloses to or shares the data with competent authorities from third countries in the exercise of his/her official functions. Queries by a competent authority in the EU in the database of a third country or of an international organisation also constitute a transfer when personal data is provided to perform the query or when (further) processed by the third country competent authority or the international organisation, including in logs.

8. For all these different scenarios, a "transfer" always includes the process of the transmission as such. Therefore, Article 37 LED and the appropriate safeguards are also applicable to data in transit between a Member State and the third country of destination.

9. Within the framework of Article 37 LED, the notion of "transfer" is not limited to individual transfer operations, but can also refer to specific categories or sets of transfers, i.e. transfers which are defined by common characteristics such as the purpose of processing or the categories of data transferred justifying a collective assessment applicable to all such transfers. Article 37, like Articles 35 and 36 in Chapter V of the LED, use the term "transfer" in the singular form, when referring in practice to

[5] EDPB Work Programme 2021/2022, p. 5 (https://www.edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf).
[6] Recitals 4 and 25 LED.
[7] See the notion of transfer in the EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 18 November 2021, para 7.

multiple operations involving transfers from one Member State to third countries.[8] Also, Article 38 (1) LED begins by referring to *"a transfer"* or *"a category of transfers"* and ends using *"the transfer"* in its singular form to cover both situations. Furthermore, Article 38 LED allows transfers to proceed on the basis of categories, even in the absence of appropriate safeguards pursuant to Article 37 LED, where the transfer is necessary for certain purposes. *A fortiori,* transfers based on categories would also be possible where they are covered by appropriate safeguards in the meaning of Article 37 LED.[9] In practice, it would also be excessively burdensome to require competent authorities to conduct such comprehensive assessments on every individual transferring operation. Such a requirement would run counter to one of the LED's objectives: to facilitate the transfer of personal data to third countries and organisations, while ensuring a high level of protection of personal data.[10]

2.2 The notion of appropriate safeguards in the law enforcement context

10. International cooperation in criminal matters is nowadays a key element in the fight against crime and thus for the safeguarding of the EU area of freedom, security and justice. This involves the exchange of necessary information, including the transfer of personal data – not only between Member States, but also with third countries. As noted above, the LED aims to facilitate the free flow of personal data for law enforcement purposes by competent authorities within the Union, as well as the transfer of such data to third countries and international organisations, while ensuring a high level of protection of personal data.[11]

11. A transfer, as any other processing operation covered by the LED, must first be lawful[12] and comply with the general principles relating to the processing of personal data.[13] In addition, transfers must comply with the specific legal framework established in Chapter V of the LED. This set of legal rules establishes a structured legal framework enabling data transfers to third countries. According to Article 35(1)(d) LED, transfers are permitted if the Commission has adopted an adequacy decision pursuant to Article 36, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37, derogations for specific situations apply pursuant to Article 38. Thus, these provisions operate in cascade[14], meaning that Articles 37 and 38 LED presuppose that the previously established transfer mechanism is not available in the case at hand.

[8] See for instance Article 36(1) LED which refers to a "transfer" of personal data from EU Member State to a third country in the framework of adequacy decisions. Article 38(1) LED refers indistinctively to "a transfer" or a category of transfers.

[9] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA also uses the term « category of transfers of personal data » (Art. 2 (u)).

[10] See recitals 4 and 25 LED, and paragraph 113 of CJEU Decision C-505/19 WS v Bundesrepublik Deutschland of 12 May 2021.

[11] Recitals 4 and 25 LED.

[12] Article 8 LED.

[13] Article 4 LED.

[14] By way of derogation from point (b) of Article 35(1) LED, Article 39 LED does not concern transfers of personal data between competent authorities, but establishes the rules governing data transfers directly to recipients established in third countries.

12. Taking into account that the Commission, so far, has adopted only one LED adequacy decision[15] and that Article 38 LED constitutes a derogation for specific cases, competent authorities for the time being are mainly dependent on appropriate safeguards as regulated in Article 37 LED in order to transfer personal data to third countries.[16]

13. There are two ways to establish appropriate safeguards pursuant to Article 37(1) LED. First, appropriate safeguards may be provided in a legally binding instrument; second, the controller may carry out a self-assessment of whether appropriate safeguards for personal data exist at their destination, considering all circumstances surrounding the envisaged data transfer.

14. However, the LED offers only limited guidance to competent authorities on the application of Article 37 in practice. In particular, the LED does not set out specific formal or substantive requirements for appropriate safeguards, nor does it provide a set of mechanisms or tools for establishing appropriate safeguards or any requirement to authorise the provision of appropriate safeguards, as in Article 46 General Data Protection Regulation (hereinafter "GDPR"). Only Recital 71 indicates to some extent how Article 37 LED is to be applied.

15. This may also result from the fact that the legislator has chosen to adopt a directive in order to regulate data processing in the field of law enforcement, including international cooperation in criminal matters. As such, the LED determines binding results to be achieved, while leaving to the Member States the choice of form and methods (Article 288(3) Treaty on the Functioning of the European Union (hereinafter "TFEU")). The LED in principle aims at a minimum harmonisation across Member States, which may provide for higher safeguards for the protection of personal data in their national laws than those foreseen in the LED.[17]

16. The purposes of data processing under the LED, namely the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, serve the public interest. Pursuant to Article 8 LED, data processing under the LED must always be necessary for the performance of a task carried out by a competent authority for one of those purposes and based on Union or Member State law.[18] The consequences of personal data processing in the police and criminal justice context, however, can be particularly serious, for example, if the data are used as incriminating evidence or otherwise may have a discriminatory effect. When applying the LED and its transposing national legislation, competent authorities should ensure that the interference with the rights of the data subjects derived from the envisaged processing is necessary and proportionate to the objective of public interest they pursue (i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security).[19]

17. The EDPB notes that the LED explicitly links its transfer provisions to the continued safeguarding of the right to data protection[20]. According to Article 35(3) LED, titled "General principles for transfers of

[15] Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4801 final.

[16] As far as bilateral or multilateral agreements referred to in Article 61 LED are not available (see also Section 3.4).

[17] Article 1(3) LED.

[18] Recital 35 LED.

[19] Article 1(1) LED.

[20] Article 35(3) LED.

personal data", it shall be ensured that the level of personal data protection provided by the LED is not undermined when they are transferred outside the EU jurisdiction. For adequacy decisions it is well established that Article 36 LED, read in the light of Article 35(3) LED, requires that the level of data protection in a third country or an international organisation is essentially equivalent to the level of data protection within the European Union.[21] The EDPB notes that Article 35(3) LED also applies to transfers carried out pursuant to Article 37 LED. In particular, Article 37 LED is not framed as an exception to the general rule laid down in Article 35(3) LED. This provision should therefore also be understood and applied in light of the principle that the level of data protection applicable in the European Union must not be undermined by the transfer of personal data to another jurisdiction. Therefore, the EDPB concludes that Article 37 LED requires an essentially equivalent level of data protection in the third country or international organisation regarding the specific transfer or category of transfers.[22]

18. In this regard, it is important to recall the standard set by the Court of Justice of the European Union (hereinafter "CJEU") for essential equivalence. As specified by the CJEU, while the level of protection in the third country or international organisation 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"[23]. Therefore, essential equivalence does not require to mirror point by point the European legislation, but to in fact ensure the core elements of that legislation, in this case the LED, read in the light of the Charter of Fundamental Rights of the European Union (hereinafter "the Charter"). This is without prejudice to higher safeguards for the protection of personal data which Member States may provide in their national legislation in accordance with Article 1(3) LED.

2.3 Requirements for appropriate safeguards ensuring an essentially equivalent level of data protection within the framework of Article 37 LED

19. The EDPB recalls that adequacy decisions adopted by the Commission formally confirm, with binding effect on Member States[24] including their competent data protection authorities[25], that the level of data protection in a third country or international organisation is essentially equivalent to the level of data protection in the European Union. Therefore, adequacy decisions should focus on the assessment of the existing legal framework of the third country or international organisation concerned as a whole, based on the assessment criteria set out in Article 36 of the LED.[26] The EDPB notes that Article 37 LED has a different scope. Article 37 LED regulates specific transfers or categories of transfers to authorities in a third country or to an international organisation and, accordingly, the requirement of appropriate

[21] Recital 67 LED, EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021, paragraph 8 et seq.

[22] For data transfers under the GDPR, the CJEU applied the standard of essential equivalence to both adequacy decisions under Article 45 GDPR and appropriate safeguards under Article 46 GDPR (Schrems II, C-311/18). For deducing the standard of essential equivalence for adequacy decisions as well as appropriate safeguards, the CJEU referred in particular to the provision of Article 44 GDPR, according to which "all provisions in [Chapter V] must be applied to ensure that the level of protection for natural persons guaranteed by [the GDPR] is not undermined." This general rule, as well as the notion of "appropriate safeguards", is also found in the LED. There is no indication that - contrary to the wording - the legislator intended to impose different concepts herewith under GDPR and LED.

[23] Schrems I C-362/14, paragraph 74.

[24] Article 288 TFEU.

[25] Schrems I C-362/14, paragraph 52.

[26] EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021, paragraph 22.

safeguards relates to a specific data transfer or category of transfers. Pursuant to Article 37 LED, essential equivalence should be ensured for that particular transfer or category of transfers and not necessarily with regard to the entire existing legislation in the third country or international organisation. Therefore, the scope of the assessment of essential equivalence under Article 37 LED does not correspond to the general and wide encompassing assessments the Commission carries out in accordance with Article 36 LED based on the criteria set out therein.[27]

20. Recital 71 LED provides some guidance on the elements that may be taken into account when assessing whether appropriate safeguards are in place. When a competent authority considers transferring personal data under Article 37(1)(a) LED, legally binding instruments could for example be legally binding bilateral agreements concluded by Member States implemented in their legal order which could be enforced by data subjects, ensuring compliance with data protection requirements and data subject rights, including the right to obtain effective administrative or judicial redress. A competent authority wishing to make use of the possibility to transfer personal data under Article 37(1)(b) LED should be able to take into account, when assessing all the circumstances surrounding the transfer, cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data as well as confidentiality obligations and the principle of specificity[28]. Under their respective legal framework, Europol and Eurojust are able to transfer personal data to an authority of a third country or an international organisation on the basis of such cooperation agreements. However, the agreements under which Europol or Eurojust transfer personal data can inform but cannot replace the assessment to be carried out by the controller in the Member State pursuant to Article 37(1)(b) LED. When considering such agreements in the context of Article 37(1)(b) LED, the controller in the Member State should consider if the safeguards agreed therein apply not only to the exchange with Europol/Eurojust based on the specific agreement, but also to the transfer in question. The competent authority should also take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment.

21. While those conditions could, according to Recital 71 LED, be considered to be appropriate safeguards, Recital 71 LED further specifies that these conditions and safeguards are not exhaustive. That said, the EDPB considers that when a competent authority is carrying out the assessment under Article 37 LED, it should analyse not only the list of elements provided for in Recital 71 but the extent to which core data protection principles and safeguards, derived from the Charter and the LED, are provided for as enforceable in the applicable legal framework of the third country, be it in a specific data protection law or in any other source of applicable law such as criminal law or criminal procedure law, to the case at hand, offering an essentially equivalent level of protection to that guaranteed in the Member State of the transferring authority.

22. The EDPB has already adopted Recommendations on the adequacy referential under the LED, addressing which data protection principles have to be present to ensure essential equivalence with the EU framework within the scope of the LED.[29] The EDPB considers that the principles and safeguards outlined in these Recommendations also apply in substance in the context of Article 37 LED. However, since these Recommendations pertain to adequacy decisions pursuant to Article 36 LED and therefore, in line with the rationale of Article 36 LED, take into account all possible aspects of data protection,

[27] See also EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021.
[28] See Recital 71 LED.
[29] EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021 (https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en).

they are not fully operational in each and every case under Article 37 LED. In fact, and as already stated, the appropriate safeguards according to Article 37 LED need to be afforded with regard to the specific transfer or category of transfers at hand. Likewise, the standard of essential equivalence under Article 37 LED can and need to be applied solely to the processing of the data that are subject to the relevant transfer. The appropriate safeguards thus depend on the data in question and the circumstances of the processing. It is therefore neither possible nor necessary to make an abstract assessment in this regard.

23. Additionally, the EDPB recalls that Article 35(1)(a), (b), (c), (e) LED lay down requirements that apply to all provisions of Chapter V and thus also to transfers carried out under Article 37 LED. In particular, personal data may only be transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1) of the LED and insofar as the transfer is necessary for such purposes.[30]

3 ARTICLE 37(1)(A) LED

3.1 The choice of this legal mechanism for transfers

24. In the absence of an adequacy decision issued by the Commission to enable personal data to be transferred to a third country or to an international organisation, data transfers can still take place if appropriate data protection safeguards are provided in a legally binding instrument between the concerned Member State(s) and the third country or international organisation.

25. The legal requirement of Article 37(1)(a) LED means that such safeguards have to be included in the text of the legally binding instrument, in order to afford to the personal data an essentially equivalent protection when being transferred to a third country or an international organisation.

26. Therefore, the legally binding instrument has to ensure that the general principles for transfers provided by Article 35 of the LED are complied with. This includes the interplay with other provisions of the Directive (e.g. the principles applicable to data processing, lawfulness of processing and data subjects' rights), in order to ensure the level of protection of natural persons provided by the LED is not undermined.

27. Furthermore, the legally binding instrument may contain higher safeguards than contained in the LED if the national law transposing the Directive so provides pursuant Article 1(3) of the LED.

3.1.1 What constitutes a legally binding instrument under Article 37(1)(a)

28. It is important to clarify from the outset what might constitute a legally binding instrument within the context of the application of Article 37(1)(a) LED. First, it should be distinguished between the mere existence of an agreement on cooperation between Parties that entails the exchange of personal data, on the one hand and, on the other hand, the existence of an agreement that regulates the processing

[30] It is clear from the wording of Article 35(1)(b) LED that a competent authority under the LED, as data controller, cannot engage a third country processor in case this entails transfers to such countries, whenever the data processing is carried out for a purpose set out in Article 1(1) LED. While Recital 64 refers to processors in third countries, this reference can, in light of the explicit and unambiguous wording of Article 35(1)(b) LED, only relate to a processor acting on behalf and under the instructions of the third country competent authority receiving the data and providing for appropriate safeguards. A derogation from Article 35(1)(b) LED requires an express provision as the one foreseen in Article 39(1) LED for other recipients.

of personal data and adduces the necessary safeguards. It is not sufficient to have an agreement in place (such as a MLAT), which provides for a legal basis for the judicial cooperation on criminal matters between the Parties and the inherent data exchanges. Such an agreement does not qualify as a lawful mechanism for the international transfer of personal data under this provision of the LED[31], unless it contains appropriate data protection safeguards.

29. The rules on personal data processing may be set up on an autonomous and specific instrument, the scope of which is to regulate transfers under the LED, or alternatively they may be inserted and become part of a more general agreement on cooperation under the scope of the LED. Either way is admissible, as long as the instrument contains the necessary safeguards to extend the protection of the data to the third country or international organisation.

30. The same rationale was already applied by the EDPB in its Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies. Though such guidelines do not cover transfers by competent authorities for criminal law enforcement purposes[32], it is relevant to underline that they as well recognize that *any legally binding and enforceable instrument should encompass the core set of data protection principles and data subject rights.*[33]

31. Secondly, the legally binding instrument may assume a bilateral or multilateral form, i.e. an agreement or a convention, between a Member State and a third country or third countries or an international organisation. This instrument may also take the shape of an EU agreement, as per Article 3(2) and 218 TFEU.

32. A mere agreement between competent authorities of the Member States and the third country [34] may not be enough to provide for all the appropriate safeguards required by the LED, in particular redress mechanisms and enforceable rights to data subjects as interpreted in the case-law of the CJEU. Its coverage would be limited by the legal tasks of those authorities, which by themselves are not in a position to engage in commitments beyond their responsibility.

33. It might nevertheless be allowable to conclude a legally binding agreement between competent authorities insofar as the third country applicable legislation, at least to a certain extent, already ensures an essentially equivalent level of data protection, as guaranteed in the EU, implemented in its legal order and the competent authorities have the power to commit in such an agreement to put in place the necessary additional safeguards that are not provided in the existing legal framework. In such case, the agreement may limit itself to regulate concrete aspects of the data transfers, while relying on and expressly referring to the specific provisions of the Parties' legislation to provide for the appropriate safeguards with regard to the protection of personal data, including effective and independent redress for data subjects.

34. Since, according to Article 37(1)(a) of the LED, the appropriate safeguards are to be provided in the legally binding instrument, the agreement has to contain at the very least the specific referral to the applicable legal provisions of the Parties affording for those safeguards. Furthermore, this type of

---

[31] This is without prejudice that such agreements may provide a general legal basis for the transfer of the data if the conditions laid down in Article 61 of the LED are met.

[32] See paragraph 4 of Guidelines 2/2020, in its version 2.0, adopted in 15 December 2020 (https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en).

[33] *Ibid*, paragraphs 65-68.

[34] For instance, a Joint Investigation Team (JIT) agreement only binds the Parties on what is covered by the legal tasks of the competent authorities, i.e. related to the operational aspects of the data processing.

choice is not without risk, should the assessment of the other Party's legal framework that it relies upon falls short of guaranteeing an essentially equivalent level of protection.

35. Therefore, what matters is that the entity or body which is a Party to the legally binding instrument in the meaning of Article 37(1)(a) LED is the entity empowered to enter into obligations with respect to the safeguards provided in the instrument.

36. The international agreement should thus have the force of law. As a result, it requires foreseeability for the addressees, it applies in all its elements to the transfers in question and it establishes obligations and enforceable rights to the Parties. Such a legally binding instrument can then be enforced by the Parties and by data subjects whose personal data processing is governed by the agreement.

3.1.2 The advantages of having such an instrument

37. A legally binding instrument regulating the processing of personal data allows overcoming any shortcomings from a data protection perspective, by providing in itself the appropriate safeguards that might be lacking in the legal framework of the third country or the international organisation.

38. One of the main advantages is that such an instrument establishes a clear and structured basis for the exchange of personal data within the context of police and judicial cooperation in criminal matters with enhanced legal certainty for the national competent authorities. This will certainly increase the level of compliance by controllers while reducing their accountability obligations and potential liabilities. In addition, they would be exempted from conducting assessments on the existence of appropriate safeguards in the third countries or international organisations. On the contrary, as per Article 37(1)(b) LED, the higher the discretion granted to national competent authorities to conclude on the appropriate safeguards, the more they will be held accountable for the compliance of their transfers, in order to meet the requirements of the LED.

39. The high-level involvement of Member States in a legally binding instrument (e.g. preparation, drafting, negotiation, approval) entails a commitment, which is beneficial to promote and accelerate cooperation. A stable legal framework for exchange of information will improve the progress of investigations and proceedings in the Member States.

40. A binding agreement allows tailor-made rules not only for data protection, but also to regulate other areas of cooperation between the Parties.

41. Transparency towards individuals and closer monitoring by Governments and Parliaments is another relevant advantage of having a binding legal instrument framing the data transfers and providing the respective appropriate safeguards.

In conclusion, in the absence of an adequacy decision, though the LED presents in Article 37(1) two possible scenarios for transfers subject to appropriate safeguards, the EDPB considers that the use of a legally binding instrument regulating the personal data transfers between the Parties presents significant advantages and should, in principle, take precedence. It sets a firmer and transparent legal framework with higher legal certainty, enforceable by the Parties and the data subjects. Possible shortcomings of the legislation of the recipient third country would be compensated by adducing the necessary safeguards to ensure an equivalent level of protection.

3.2 The preparatory work and negotiation

42. The negotiation of a legally binding instrument in this context requires, as part of the preparatory work, a good overview of the relevant legal framework of the third country or international organisation. While this does not require the same in-depth evaluation of the third country as the Commission would undertake for an adequacy decision, under Article 36(2) of the LED (see Section 2.3), it should consider the relevant elements required by that provision, applied to the concrete agreement.

43. Indeed, it is necessary to have an accurate understanding of the rule of law, respect for fundamental rights, the relevant legislation and its implementation in the concerned areas (e.g. police cooperation or judicial cooperation in criminal matters), as well as relevant case law that may clarify its interpretation, redress mechanisms for data subjects whose data are transferred, including international commitments the third country or international organisation has entered into. This assessment is crucial to identify shortcomings in the legal framework of the third country or international organisation and to find a way to counterweight them by adducing the necessary safeguards in the legally binding instrument[35].

44. For this purpose, Member States could request the other Party, also during the negotiation, to provide the needed elements to carry out or complete this assessment. Governmental bodies experienced in international affairs (e.g. Ministries of Foreign Affairs, Justice and Interior) are usually competent to negotiate these types of agreements. They often have more resources and expertise to assess the human rights and rule of law situation in third countries than the national competent authorities that transfer personal data at the operational level.

45. If the third country already has data protection legislation, that is key-indicator for the evaluation. When considering the data protection rules possibly in force in the third country or international organisation, Member States should carefully check the scope of application of that legislation, as well as whether any relevant international legal instrument adhered to was actually effectively implemented, and how, in the third country legal order. Special attention should be paid to derogations in the law enforcement field that might render the data protection safeguards ineffective, in particular regarding data subjects' rights.

46. While preparing and negotiating the terms of the agreement, it should be ensured that the concepts are understood the same way, since likely the terminology used by the Parties in their respective legal frameworks might be different (see below 3.3.1). That is a very significant issue and requires a careful approach. The objective is not to mirror the EU legal regime, but instead to ensure that there is correspondence to the EU principles and guarantees, and ultimately the legally binding instrument contains the data protection appropriate safeguards required by the LED. This is also important in view of future interpretation and enforcement, including by supervisory authorities and courts, once the agreement will be in force.

47. The Member States negotiators should also take into account that the agreement cannot contain provisions not admissible under EU or national law, which would put at risk the lawfulness of the data processing[36].

48. Lastly, it should be noted that a legally binding instrument may be subject to the prior consultation of the supervisory authority.[37] In any case, Member States are in all circumstances encouraged to engage

[35] This precludes Member States from accepting, without prior analysis, standard agreements proposed by third countries, which are not open to negotiation.

[36] See, for instance, section 2.3.4 of these guidelines about the respect for fundamental rights, in particular in the situations described in Recital 71 LED.

[37] The interpretation of Article 28 LED in this context has to be further clarified.

with the national SA before the conclusion of the legally binding agreement to allow for a timely, constructive and meaningful exchange in order to verify that the appropriate safeguards are in place, in line with the requirements of Article 37(1)(a) LED. In that context, the SA should be provided with all relevant information regarding the third country or international organisations, including the respective assessments made, when available.

3.3 Contents of the legally binding instrument

3.3.1 General aspects

49. Wherever the legally binding instrument does not cover exclusively data protection issues, but governs police and/or judicial cooperation in criminal matters, the data protection clauses should be clearly identified and distinguished from other clauses dealing with other kind of information, which is not personal data.

50. The essential data protection rules should be included in the clauses of the main text while detailed provisions could be described in annexes, which are still an integral part of the agreement, to avoid overburdening the text (e.g. specific security measures, categories of data subjects or data categories, specific rules on handling the information, channels of communication, procedures in case of emergency).

51. The subject matter of the agreement should not be confused with the purpose of the data processing it entails. The objective of an agreement is usually broad, though it has to fit the scope of the LED, while the purpose of the data processing should be explicit and specific. This is of key relevance as it affects the application of rules for the further processing of data by other competent authorities in the third country, as well as it influences the outcome of the application of other data protection principles, such as data minimisation and data retention (Article 4 (1) (b), (c) and (e) of the LED).

52. Moreover, having in mind the scope of the LED, provided by its Article 2, the agreement should expressly provide that the authorities of the Parties involved in the processing of personal data within the context of that legally binding instrument are competent for the purposes set out in Article 1(1) of the LED.

53. As stressed above (paragraph 46), the agreement should contain a list of relevant definitions to ensure that the Parties have a common ground of understanding and apply data protection rules in a consistent manner. Terminology may vary from the one in the EU legal framework, as long as the concepts are recognized. In this regard, the definition of 'personal data' is of course essential and needs to entail the exact same meaning and broad scope as under EU law; otherwise, some data processing could be excluded from the agreement. The same applies to the concept of data processing, which needs to encompass an equivalent range of processing operations. Other definitions, such as data subject, data controller, processor, third party, data recipient, competent authority, special categories of personal data, data security/data breach, onward transfer are also relevant as a basis to build on the rules.

54. In addition, including other concepts outside the data protection field (like, 'suspect' or 'criminal offence') is very useful to shape the applicable scope of data processing. More specifically, agreeing on such notions may serve, for example, to exclude political offences qualified as 'terrorist acts' and to facilitate the application of the principle of dual criminality. Those concepts could be retrieved from other international instruments signed by both Parties, or taken directly from an EU legal text.

55. The text of the agreement should contain, in the text itself, all relevant data protection rules governing the data processing to be carried out in the context of such instrument. Consequently, general references to the national or international legal frameworks should not be inserted in the agreement; otherwise, that would exclude such matters from being regulated in the text of the agreement itself, where the appropriate safeguards should be provided. Such referral[38] should only be done, instead, to specific provisions of the legislation providing concrete safeguards, and only after a thorough assessment of the third country's legislation indicating that the level of protection ensured by the LED is not weakened. All safeguards need to be provided in the agreement in a legally binding form.

56. It should be underlined that specific conditions or restrictions on the use of data could be imposed by Member States[39] in the text of the agreement, following national legal requirements or specific operational needs. Indeed, Article 1(3) of the LED provides for the possibility of Member States having higher safeguards than those established in the Directive for the protection of the rights and freedoms of the data subjects.

57. In conclusion, the legally binding instrument should contain all relevant rules to allow overcoming any shortcomings or limitations of national legislation of the third country in terms of data protection by setting a framework of appropriate safeguards that afford an essentially equivalent level of data protection to the one guaranteed in the EU.

3.3.2 Essential elements

58. In order to provide the appropriate safeguards, and in view of the data protection principles referred to in Chapter 2 of these Guidelines, the legally binding instrument should contain a set of essential elements in the main text. Eventually, more detailed requirements may be introduced in an annex, which will be full part of the agreement, while avoiding overburdening the main text.

59. Against this background, in light of and without affecting the standard of essential equivalence, the following elements should in particular be addressed in the legally binding instrument[40]:

    i. Determine scope as much as possible by specifying the purpose(s) of the processing and areas covered. A catalogue of offences or identification criteria based on penalties thresholds should be envisaged;

    ii. Describe the categories of data subjects affected by the processing and the respective categories of personal data to be transferred (see paragraph 54). In case special categories of data, referred to in Article 10 of the LED, are to be processed, clearly identify which personal data will be at stake and provide that the processing may only take place where strictly necessary and subject to additional safeguards for the rights and freedoms of the data subject. The additional protective measures should be expressly described in the agreement. Exclude, however, any profiling of the data subject that would result in discrimination on the basis of the processing of special categories of data;

[38] The references to legislation should be specific and not general. See also paragraph 34.

[39] Recital 65LED states that *Member States should provide that any specific conditions concerning the transfer should be communicated to third countries or international organisations.*

[40] When a multilateral agreement is at stake involving several third countries and different levels of protection, all appropriate safeguards should be included in the text of the agreement in a comprehensive manner to ensure the highest possible minimum common denominator.

iii. Provide that competent authorities who will be exchanging data are competent for any or all general purposes set out in Article 1(1) of the LED. The identification of the competent authorities for the Parties may be inserted in the annex or referred to further declarations by the Parties;

iv. Provide that data should not be further processed by the identified competent authorities of the receiving Party for another purpose, without previously informing the transferring Party, duly justified, and in any case only for compatible use. The Parties should ensure that the specific purposes for which data is to be further processed are still within the scope of the LED;

v. Exclude the disclosure to other authorities of the receiving Party, unless it has been provided in advance [set period] written information to the transferring Party, which may object to such data sharing or impose certain conditions for the processing. The information provided to the transferring Party shall identify the data recipient authority or body, which has to be an authority competent for the purposes referred to in Article 1(1) of the LED, and state the reasons for disclosing the data and the categories of data shared. Further processing of the data shall be limited to the general purposes set out in Article 1(1) of the LED. The Parties shall ensure that where data is shared to other authorities of the receiving Party the data will be processed under the same conditions as set out in the agreement and be afforded the same protection;

vi. Provide that data processed should be relevant, adequate and limited to what is necessary for the purpose for which it was transferred and further processed;

vii. Provide that data should be accurate and up-to-date. If any Party becomes aware that the data transferred or being processed is inaccurate or out-of-date, it shall notify the other Party without delay. Where it is confirmed that the data is inaccurate or out-of-date, each Party shall take every reasonable step to rectify or erase the data concerned;

viii. Determine that the data transferred and further processed shall not be kept indefinitely but it shall only be retained for the period necessary to achieve the purpose for which it was transferred and further processed. Specific restrictions could be imposed on data storage periods;

ix. Exclude automated individual decision-making, including profiling, based on the data transferred, which would produce adverse legal consequences or otherwise significantly affect the data subject, unless appropriate safeguards for the rights and freedoms of the data subject are established in the third country legal framework or in the text of the agreement. Such safeguards could 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, to obtain an explanation of the decision reached after such assessment or to challenge the decision;

x. Provide for the obligation of the Parties to adopt adequate and necessary security measures, of technical and organisational nature, to ensure that personal data is kept confidential and is protected against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. More detailed security measures could be developed in an annex (e.g. encryption of data, access controls for users based on the principle of 'need-to-know', existence of audit logs

for monitoring users' activity and so forth). It is essential that security measures should cover data processed in the place of destination, as well as in transit;

xi. Provide that any personnel who processes personal data is bound by professional secrecy or any other statutory obligation of confidentiality, and, if applicable, that the level of confidentiality assigned to the information by the requested authority should be ensured by the requesting authority. Detailed rules may be established in the annex, for example if the Parties agree to apply the security levels used by Interpol;

xii. Provide that, in case of a personal data breach affecting the data transferred, the concerned Party shall notify immediately the other Party and provide a description of the incident, including its immediate impact, and the relevant measures taken or proposed to be taken to address the breach and mitigate any adverse effects;

xiii. Exclude the onward transfers to third countries or international organisations, unless prior written authorisation is obtained from the transferring Party, taking into account the requirements of Article 35(1)(e) LED. For that purpose, it should be established that the information provided to the transferring Party shall, at least, identify the country of destination or the international organisations and the data recipient, it shall state the reasons for the onward transfer, including the criminal offence involved, and the categories of data transferred. Data transferred onward should be protected by the same conditions and safeguards as in the transferring Party;

xiv. Ensure that each Party keeps a record of all written exchanges of information required by the agreement, in particular the requests for authorisation, the authorisations given, notifications and so forth. This record is a tool for accountability and enables self-auditing and monitoring of the implementation of the agreement by SAs;

xv. Ensure, at least, that data subjects have the right of access, rectification and erasure of the personal data concerning them. Identify to which authorities data subjects should address their requests or, at least, provide for the obligation to have that information publicly available and easily accessible at all times;

xvi. Derogations to these rights have to be expressly established in the agreement and applied only if necessary and proportionate in a democratic society with due regard for the fundamental rights of the natural person concerned. It should be provided that the limitations to the rights are only possible, partially or fully, to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, and to protect the rights and freedoms of others;

xvii. Ensure independent oversight, monitoring and enforcing compliance with data protection requirements;

xviii. Ensure administrative and judicial redress, identifying the existing mechanisms, towards which data subjects may enforce their data protection rights;

xix. Include in the agreement a consultation and suspension clause, in case of breach of its data protection rules until the situation is resolved. Such clause should also cover situations when legislative developments undermine somehow the safeguards afforded by the legally binding instrument;

xx. Provide that, in case of suspension or termination of the agreement, the personal data already transferred shall keep being processed under the conditions set out by the agreement.

3.3.3 Additional tailor-made clauses

60. Supplementary clauses, tailor-made for specific contexts, and providing additional safeguards, can be inserted at the discretion of the Parties and in principle regarded as best practice.

Some examples of such rules are:

i. Provide that the Parties exchange on a regular basis information on the exercise of rights by data subjects, including statistics on the number of requests and their outcome, notably the number of cases where the right was restricted. In addition, the Parties can agree to keep a record of all requests submitted for a certain period yet to be defined;

ii. Provide for the possibility of indirect exercise of data subject rights via an independent body, e.g. the national data protection supervisory authorities.

iii. Provide that the Parties exchange relevant information about the use of redress mechanisms related to the application of the agreement, including the decisions taken on that account;

iv. Include in the data subjects' rights catalogue the right to have the data processing restricted, pursuant Article 16 of the LED, while the accuracy of the personal data is still being established. During that period, the Parties should limit the use of such data, in particular the data should not be further transmitted to any third party;

v. Provide that, in case of justified urgent need, essential for the prevention of an immediate and serious threat to public security of the Parties of this agreement or of the third State concerned, the data may be onward transferred to that third State without prior authorisation. In such a case, information shall be provided to the other Party immediately afterwards;

vi. Set a minimum period of time for keeping the record of notifications and authorisations given within the context of the agreement, referred to in paragraph 60 (xiv) of these guidelines.

vii. Obligation to report to the other Party if there are changes in the legal framework that might significantly affect the agreement;

viii. Furthermore, in a situation of suspension or termination of the agreement shorter retention periods could be envisaged and a prohibition for the receiving Party to continue with any onward transfer of data;

ix. The data of the personnel of the competent authorities exchanging the data should also be protected. As a result, such data could also be included in the list of categories of data with reference to that specific category of data subjects;

x. Provide that a contracting Party may not invoke the fact that another Party has transferred incorrect or out-of-date data to relieve itself of its responsibility under its national law towards the data subject.

3.4 Interplay with concluded international agreements in this field

61. Article 61 LED is a transitional "grandfathering" clause, which, in the same vein as Article 60 LED[41], provides that those international agreements involving the transfer of personal data to third countries or international organisations, which were concluded by Member States prior to the entry into force of the law enforcement directive, and which complied with pre-existing EU law, shall remain in force until amended, replaced or revoked.

62. The LED did not provide for a fixed deadline for their amendment to bring them into conformity with the appropriate safeguards required by the LED, and more specifically by Article 37(1)(a)LED, if these agreements do not contain already all of these safeguards. Consequently, pursuant to Article 61 LED, competent authorities from Member States may continue using these agreements to transfer data to third parties until these agreements are amended, replaced or revoked. That said, under EU law, Member States have a general obligation to bring all their international commitments in compliance with EU law. Therefore, if any existing agreement would not comply with the requirements of Article 37(1)(a) LED, it should be reviewed.

63. Furthermore, Member States must process the data received in the framework of these agreements in accordance with the LED and national law. In addition, new amendments or replacements of existing agreements, or new agreements Member States may conclude will need to contain all the necessary appropriate safeguards to comply with the LED and qualify as a "legally binding instrument" under Article 37(1)(a) LED.

64. It should be recalled that the EDPB, in its Statement 04/2021 on international agreements including transfers[42], adopted on 13 April 2021, invites *Member States to assess and, where necessary, review their international agreements that involve international transfers of personal data*. For agreements concluded prior to 6 May 2016, this review should be done in order to determine whether, while pursuing the important public interests covered by the agreements, further alignment with current Union legislation and case law is needed.

65. The EDPB emphasizes that consideration should be given to the aim of bringing those agreements in line with the LED requirements for data transfers, where this is not yet the case, to ensure that the level of protection of natural persons guaranteed by the LED is not undermined when personal data is transferred outside the Union.

---

[41] Nevertheless, Article 62(6) of the LED provides that the Commission shall review Union legal acts, including those referred to in Article 60, in order to align them with the LED. For that purpose, see COM(2020) 262 final, where the Commission identifies that the Prüm Decisions need to be revised in order to align, inter alia, rules on transfer of personal data to a third country or international organisation with the LED (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0262).

[42] See EDPB Statement 04/2021 on international agreements including transfers, adopted on 13 April 2021, p. 1 (https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf).

4 ARTICLE 37(1)(B)LED

4.1 When may Article 37(1)(b) LED be used to transfer data

66. The mechanisms of the legal framework for transfers listed under Chapter V of the LED operate in cascade.[43] Consequently, competent authorities may resort to Article 37(1)(b) LED to transfer data to a third country or to an international organisation only where there is no adequacy decision issued under Article 36 LED. In the absence of an adequacy decision the use of a legally binding instrument should in principle take precedence over an assessment according to Article 37 (1)(b) LED, covering the transfer. The controller should verify this in a first step[44]. While the standard of essential equivalence applies to both alternatives of Article 37(1) LED, legally binding instruments provide transfers of personal data with more legal certainty, transparency, foreseeability, stability, consistency and guarantees on the effective application of data protection safeguards, especially if the transfers are frequent, massive, structural or occur on a large-scale. The conclusion of a legally binding instrument under Article 37(1)(a) on a specific category/ies of transfers would make self-assessments under Article 37(1)(b) no longer necessary for those transfers.

67. The term "transfer" may be understood in the context of Article 37(1)(b) as encompassing specific categories or sets of transfers which are defined by some common characteristics[45] and one-time transfers to third countries or international organisations. The transfers conducted under Article 37(1)(b) LED may thus also be frequent, structural or large scale if they comply with all the requirements of the LED and the transposing national law, including those of Article 35 LED. The transfers must be covered by safeguards that are appropriate to ensure for that specific transfer or category of transfers an essentially equivalent level of protection to that guaranteed under the LED[46] and national law.[47]

4.2 How to assess all the circumstances of the transfer

4.2.1 Factoring the risk to data subjects into the assessment of the transfer

68. The general objective of the LED and national transposing law is to protect the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data, while ensuring that competent authorities are able to exchange personal data where EU or national law allows it for the performance of their tasks in the public interest.[48] This objective of facilitating and strengthening data sharing, while ensuring a high level of protection of personal data, also comprises international cooperation in criminal matters.[49]

---

[43] Art.35(1)(d) LED.

[44] In this regard, the controller should pay particular attention to the applicability and validity of the adequacy decision and the legally binding instrument. In addition, the EDPB encourages controllers to carefully consider planned or ongoing negotiations for a legally binding instrument under Article 37(1)(a) LED before proceeding to transfers under Article 37(1)(b) LED, in order not to undermine such negotiations.

[45] These include the purposes for which the information is processed, the categories of data subjects part of the transferred data, the criminal offence and/or its seriousness, the types and number of authorities to which data is transferred, the authority at the origin of the transfer (e.g. police, judicial), the country or countries to which data is transferred, and the nature and conditions of the execution of the criminal penalty (see Section 4.2.2 below).

[46] Art. 35(1) LED.

[47] Art. 1(3) LED.

[48] Art. 1(2) LED and Recital 35 LED.

[49] Recitals 4 and 25 LED.

69. The protection of the personal data exchanged in international cooperation is therefore an essential factor that competent authorities from the EU must take into account in their assessment of when and how to transfer data to authorities in third countries. Competent authorities should also examine the protection of these data in view of the risks its sharing with third countries raises for the fundamental rights and freedoms of the data subject on whom data is transferred, their legitimate interests and those of other persons concerned.[50] This is especially important when using Article 37(1)(b) LED to transfer data to third countries, in the absence of adequacy decisions or legally binding instrument covering a transfer.[51] Competent authorities should notably assess before processing personal data, including transferring it to third countries, whether such processing is necessary and proportionate for the purpose they pursue under the LED[52] in the light of all the circumstances of the transfer.

70. There are other factors, independent from the protection of the personal data of the data subject, which competent authorities should duly take into account before proceeding with a transfer. Some of these additional factors are the legal framework permitting the exchange of data (e.g. bilateral or multilateral agreement or instrument, reciprocity or comity), the importance of the sharing for the criminal investigation or procedure, the confidentiality level of the data, requirements from criminal procedural law, the dual criminality principle, the impact on other fundamental rights of the data subject, and possible political or diplomatic considerations.[53]

4.2.2 Categorising and assessing the transfers based on their risks to the fundamental rights and freedoms of data subjects

71. Knowing in detail all the circumstances surrounding the specific data transfers conducted or to be conducted is necessary to be able to identify the risks to the rights and freedoms of natural persons, and in particular to the right to data protection, and any safeguards that are appropriate to mitigate them.[54]

72. As for any other processing operation, a competent authority must be aware of and consider in a granular manner the nature, scope, context and purposes of the transfer.[55] More specifically, competent authorities should analyze and categorise their transfers considering the characteristics mentioned below. These characteristics are relevant to assess the risks posed to fundamental rights of the data subjects by each transfer in their relevant context.

73. **Categories of data subjects:** the LED[56] and other EU[57] and international legal frameworks[58] require distinguishing between different categories of data subjects (e.g. suspects, convicted criminals, victims, witnesses, persons of interest, associates, missing persons). The risks to the rights of data subjects will vary depending on the category of the subject and the context in which the transfer is

[50] Recitals 28, 37, 50, 51, 52, 58, 60, Articles 19, 27 LED.
[51] See for example the additional risks to data subjects where data is transferred abroad on their ability to exercise these rights which recital 74 LED notes. The absence of adequacy decisions or legally binding instrument increases these risks.
[52] See references to the application at the operational level of the necessity and proportionality principle in Recitals 26, 29, Art.4(2)(b) LED.
[53] Another exception for the transfer may concern the national security of the Member State or the third countries. Competent authorities should assess in accordance with their national law, whether the assistance provided could threaten the sovereignty, security, public order or other essential interests of the State.
[54] Article 37(1)(b), Recital 71 LED.
[55] See the responsibilities of the controller for any processing of data in Recitals 50, 51, 58, and Article 19 LED.
[56] Recital 31 and Art. 6 LED.
[57] Recital 43, Art.18 (3)(a)(5), Art.30, 34(2)(a), Annex II Europol Regulation.
[58] Article 44 INTERPOL's Rules on the Processing of Data.

made. This will be especially the case where the competent authority transfers special categories of personal data, as defined in Article 10 LED.

Example: The transmission of an image of a victim of child sexual exploitation to competent authorities in third countries to identify the victim will require enhanced data security confidentiality safeguards, and data minimisation to avoid the re-victimisation of the victim of sexual exploitation. Some of these safeguards could be restricting the access to these data to analysts and investigators from services specialised and trained in the area of online child sexual exploitation; foreseeing technical measures to ensure the separation of these data from other police data and databases; and minimising the amount of information transferred (e.g. full image, sanitised image, or hash code of the image) depending on its categorisation and the specific purposes sought through the cooperation. These safeguards could thus be different from those applicable to an international request for location and arrest of a convicted criminal, which may be widely shared among law enforcement authorities (and even the public in some cases), and include as much information as possible to identify and find the individual.

74. **Specific purposes of the transfer**: a transfer must serve one of the purposes described under Article 1(1) LED, namely, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Within these general purposes, transfers serve specific purposes such as to locate and obtain information on a person in the framework of a criminal investigation, to identify a person or to carry out crime analysis to identify threats, trends and criminal networks. To ascertain the safeguards that are appropriate for this transfer, the competent authority should determine as much as possible which of these specific purposes the transfer is pursuing. The choice of adequate measures to protect the rights of data subjects may also depend on whether a Member State competent authority is transferring data to obtain more data for its own purposes, such as for a criminal investigation it is conducting; or whether this competent authority is responding to a request made by a foreign authority for its own criminal investigation and prosecution.

Example: Finding a missing person in the framework of a criminal investigation may in practice require the transfer of more personal information and the disclosure of these data to multiple authorities in third countries (and possibly also to the public) than locating a witness of a serious crime. In the latter case, the protection of the witness and his/her rights may warrant more stringent (confidentiality) measures, as the personal information may be considered particularly sensitive in this context. The purpose of finding a missing person, on the one hand, and a witness to a serious crime, on the other, may thus necessitate different data protection safeguards.

Example: Transferring data on known movements across borders of foreign terrorist fighters to conduct strategic crime analysis together with a third country authority[59] to help prevent crime may require different safeguards than providing data to a third country's authorities to help it detect and prosecute a suspect for a serious crime.[60] In the first case, the purpose pursued to produce strategic crime analysis reports to inform law enforcement strategies to tackle international terrorism may justify setting longer retention periods and more flexible standards of accuracy and reliability for the data processed, as well as limiting the access to data to a specialised body (e.g. police intelligence information units) in the receiving country. In the second case, the retention periods will usually need to be shorter and the data of high quality and accuracy to prevent prejudicing persons other than the

[59] See for example Art18 (2)(b) of the Europol Regulation and Article 10(2)(h) of INTERPOL's Rules on the Processing of Data.

[60] See for example Article 10(2)(a) of INTERPOL's Rules on the Processing of Data.

suspect due to misidentifications or applying coercive measures on the suspect that may no longer be necessary and are based on outdated information, while the data may need to be widely shared among law enforcement authorities (and in some cases the public) to find the suspect.

75. **Quantity and nature of data transferred***:* The risks to the rights of data subjects will vary depending on the quantity of data transferred, as well as on its nature (e.g. sensitive data). The different stages and purposes of an investigation, in compliance with the data minimisation principle, may lead to transfers which may vary in the amount and categories of data.

Example: If a police service is seeking to identify a person whom it has very little information about in the beginning of an investigation, the transfer request would initially likely be limited to the question of whether the data subject is known to the police services of one or more third countries. The answer provided by the third country would allow the police and justice either to direct the investigation to another country or to start a more extensive data exchange. In the same vein, the type of investigation may also require the exchange of a single piece of data.

76. **Types and number of authorities to which data is transferred:** Article 35(1)(b) LED provides as a condition for transfers that the authority in the third country or international organisation is competent for the purposes referred to in Article 1(1) LED. The specific purpose for which a transfer or category of transfers is conducted should determine to which specific authorities in the third country data may be transferred to guarantee that data is processed in the third country only for the purposes for which it has been transferred (principle of specificity).[61] The legal framework of the third country or the additional safeguards provided in the data exchange should establish the principle of purpose limitation and prevent it from being processed for incompatible purposes. Entities in the third country may have a mandate to serve different purposes (e.g. crime prevention, national security, etc.), which may require to define more granularly the service within that entity accessing the data. The wider the dissemination of data in the third country among its authorities, the higher the data protection risks to the fundamental rights, such as its use for purposes incompatible[62] with those for which it was provided and data breaches. These risks thus need to be factored into the assessment of whether to transfer data to certain third countries and with which safeguards.

Example: A competent authority in a Member State may transfer data only to units in the third country's police forces dedicated to information on organised crime for the purpose of conducting joint crime analysis. The competent authority may request that such information is not shared with other authorities within those countries that are not directly competent in this area, in order to limit data protection risks and undermining its criminal investigation. The competent authority may also ensure that the receiving authorities in the third country commit themselves to informing the competent authority before any further processing of these data by different units or police services for different purposes, so that the competent authority may signal its objection to this processing if it so wishes.

77. **Seriousness of the criminal offence:** the seriousness of the criminal offence[63] is also relevant to evaluate the risks that the transfer may pose to the rights of a data subject, and which safeguards would be appropriate to mitigate such risks.

[61] Recital 71 LED.
[62] Article 4(1)(b) and Recital 29 LED.
[63] Recital 65, Art. 35(1)(e) LED.

Criminal offences with low penalties foreseen may not justify neither sending the data as part of requests to third countries, nor to respond to requests on such types of offences received from authorities in third countries.

The dual criminality principle often present in MLATs would also be relevant in this regard to determine if data may be shared with third countries.

Advancing criminal investigations in cases of serious crimes such as terrorism and organised crime may justify sending out personal data as part of a request. At the same time, in order to avoid the risk of contributing to political prosecutions or the application of death penalty or any form of cruel and unusual punishment,[64] the seriousness of the criminal offence would also warrant a reconsideration of the transfer or adopting additional safeguards when responding to a request in this area from certain countries.

Example: In light of the risks to the rights and freedoms of the data subject once the data will be transferred in a third country, the competent authority of an EU country may consider it disproportionate to send a request for international police cooperation on a criminal offence with a penalty of less than a year of prison, or to respond to a request for information on a person wanted for the offence of bounced cheques. Conversely, it may deem necessary and proportionate to send personal data to an authority of a third country as part of request in a case of terrorism. In this case, the competent authority would still have to subject the transfer of personal data to appropriate safeguards to mitigate any potential and unwarranted risks to the rights of the data subject.

78. **Authority at the origin of the transfer**: the authority at the origin of the transfer may be judicial, police, other law-enforcement authorities or other bodies or entities entrusted by Member State law to exercise public authority and public powers for the purpose of the LED.[65] The nature of this authority, its institutional mandate and independence, and the rules to which it is consequently subject, may also be relevant in the assessment of the risks of the transfer and the safeguards it may need in accordance with those provided for example in national rules on judicial proceedings.[66]

Example: Personal data that is sent to third countries on the request or with the authorisation of a judicial or other independent authority of a Member State provides additional guarantees and safeguards to the rights and freedoms of a data subject than when a competent authority such as a police body shares personal data informally with its counterpart in a third country.

79. **Country or countries to which data is transferred:** the overall level of protection of personal data[67] and other fundamental rights and freedoms in the third country is another important feature of the transfer. The level of protection of natural persons provided for in the EU by the LED cannot be undermined by the transfer to third countries or international organisations.[68] The competent authority should take into account elements in the third country such as those listed under Article 36(2) LED together with the others mentioned above before deciding on transferring the data and on the safeguards that would be appropriate to ensure an essentially equivalent level of protection of the data in the light of the risks involved, including rules for onward transfers.

[64] Recital 71 LED.
[65] Recital 11 and Art. 7 LED.
[66] Recital 49 LED.
[67] Recital 65 LED.
[68] Recital 64, Art. 35(3) LED.

Example: Sharing data with a third country on which there are doubts over its general respect for the rule of law, human rights, and fundamental freedoms entails higher risks to the rights and freedoms of a data subject, including the right to data protection.

80. **Nature and conditions of the execution of the criminal penalty in the third country:** The risks to the rights and freedoms of the data subject will be higher where there is a possibility that, based on the personal data transferred, the data subject faces death penalty or any form of cruel and inhuman treatment in the third country (see also paragraph 78 above).[69] The competent authority should then assess whether to proceed with the transfer and any safeguards to be added to prevent this risk.

Example: A competent authority receives a request from a third country for information that could serve to sentence the data subject for a drug trafficking offence, which some third countries punish with the death penalty. The competent authority makes such data transfers contingent on obtaining a commitment of the third country not to impose death penalty or any form of cruel and inhuman treatment.

4.2.3 Determining if the existing safeguards are appropriate

81. Article 37(1)(b) would operate in cases where there would be no adequacy decision (Article 36 LED) or legally binding instrument (Article 37(1)(a) LED) between the EU Member State and the third country providing appropriate safeguards for categories of transfer. There may be cases where appropriate safeguards already follow from the third country's international commitments, its legislation and practices. In other cases, competent authorities may need to provide, to the extent they are legally competent, for additional safeguards in light of the features of the specific transfer mentioned above, to ensure an essentially equivalent level of protection to that guaranteed under the LED and national law, for example, depending on the individual case, via MoUs, exchange of letters or other kind of arrangements (see also paragraph 86).

International instruments and frameworks to which the third country is bound

82. The third country and its authorities may already have committed themselves to privacy and data protection obligations and standards via multilateral or bilateral international instruments and frameworks binding also Member States and their authorities. Without prejudice to the possible application of the transitional provision of Article 61 LED to them[70], the ratification of such instruments may not by itself provide for an essentially equivalent level of protection, as this will depend, in particular, on their specific implementation in each country (e.g. ratification of Convention 108 and additional protocols).[71] Yet, the ratification of such international instruments may still be relevant as a factor in the assessment of existing safeguards[72] and the level of protection under Article 37(1)(b) LED.

83. The competent authority may share or send the data to one or several third countries via an intermediary such as an international organisation (e.g. Interpol). These international bodies may already have legal frameworks for transfers that may protect the data transferred with some appropriate safeguards.[73] The competent authority will be able to rely on these safeguards and may,

[69] Recital 71 LED.
[70] See Section 3.4 above.
[71] The EDPB does not assess in these Guidelines the extent to which specific existing instruments meet the requirements of Article 37(1)(a) LED.
[72] See paragraph 46.
[73] All Member States are INTERPOL Members. When processing data in or from the INTERPOL Information System Member States and third countries members to this international organisation must apply INTERPOL's Constitution, its Rules on the Processing of Data (RPD), and other secondary law of this organisation and specific

in light of all the circumstances of the transfer, need to complement them with additional safeguards in order to meet the standard of an essentially equivalent level of protection with the LED and national law. These frameworks usually allow for the imposition of additional conditions or safeguards to the data transferred (e.g. no use of the data in judicial proceedings, limitation to specific purposes, data access restrictions, shorter retention periods for data, onward transfers etc).

Legislation and practices of the third country

84. A third country's legislation and the practice of its authorities may already provide some of the appropriate safeguards needed to ensure that the data transferred benefits from a level of protection essentially equivalent to that guaranteed under the LED and EU law, when processed in the third country. Article 36(2)(a) and (b) of the LED list some of the elements that may indicate or confirm the existence of appropriate safeguards in the third country.[74] The competent authority will still need to assess to what extent these safeguards may apply to the data transferred[75] and would be sufficient to meet the standard of essential equivalence, in light of all the circumstances of the transfer, and foresee additional safeguards to this end where needed.

85. The competent authority will need to monitor relevant developments in the third country and/or practice of its authorities and that may indicate that appropriate safeguards are not effectively applied. Appropriate safeguards must be applied in practice and not only formally. The competent authority should reassess transfers regularly and, on that basis, decide accordingly to provide additional safeguards or suspend the transfer.

Possible additional safeguards

86. To ensure that the data transferred is subject to an essentially equivalent level of protection to that guaranteed under EU or national law while it is processed in a third country or international organisation, the competent authority may add safeguards to those that may already exist. The competent authority should ensure that such additional safeguards are appropriately communicated to the receiving authority. The commitment of the receiving authority in the third country to respect and comply with these safeguards is necessary so that they are effective. International frameworks and commitments often contain provisions allowing their Parties or Members to impose additional safeguards in certain cases on the data they transfer.[76]

87. Some of the possible additional safeguards are the following:

---

provisions governing its databases, communications infrastructure and other services (Arts. 4 and 5 RPD). Member States will need to assess if in light all the circumstances of the transfer/category of transfers these safeguards need to be complemented with additional ones to ensure that the data meets the standard of essentially equivalent level of protection when processed in the third country/ies to which it was transferred via INTERPOL. (See Recital 25 LED).

[74] See also Chapter 2 and the EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021.

[75] For example, in some third countries, under their legislation and practices, some of these safeguards may only apply to nationals of that country and/or to specific categories of data or purposes of the processing.

[76] See for example the possibility under INTERPOL's Rules on the Processing of Data for Members to establish general or data-specific access restrictions to the data on other Interpol members (Articles 58 and 107-109RPD), special conditions for use on the data transferred (Articles 45 and 66 RPD), specific data processing purposes (Article 10(3)-(5) RPD) and shorter retention periods on the data recorded in INTERPOL's databases (Article 46(4)(a)RPD). Other possibilities may include, depending on the individual case, MoUs, exchange of letters or informal arrangements, etc.

- Restricting access to the data transferred at the level of the country, authority or data;[77]
- Restriction on the processing of the data to a specific purpose defined in the transfer (principle of specificity);[78]
- Establishing notification and authorisation mechanisms to the competent foreign authority from which the data originates for transfers among authorities within a country;
- Defining specific conditions for the processing or handling of the data;[79]
- Establishing specific data retention periods and mechanisms of automated deletion to ensure that the data is processed for the purposes for which it is provided and the validity of this purpose and the accuracy of the data is regularly checked;
- Setting out review processes and notification procedures between authorities to ensure that data remains accurate and up to date having regard to the purposes for which they are processed, and where necessary erased or rectified without delay;[80]
- Establishing specific data security safeguards through technical (e.g. agreed standards, logs, encryption, authentication mechanisms) and organisational measures (e.g. designation of data security officer or department, audits, internal and external oversight, disciplinary measures) to ensure its protection against unauthorised access or unlawful processing and against accidental loss, destruction or damage;[81]
- Providing for consultation and joint audit and review mechanisms of the processing of data and transparency measures such as access to logs of processing of transferred data by third country;
- Demanding commitments on the non-application of death penalty or any form of cruel and inhuman treatment.[82]

Sources of information:

88. To obtain information on the safeguards that may already exist for a transfer to a third country and ascertain if additional ones are needed, competent authorities may use sources such as the following:

- Existing EU adequacy decisions under the GDPR covering that country or one of its regions/sectors;

- Reports on third countries produced by the Commission (e.g. Progress Reports on candidate and potential candidates to the EU);

[77] See Recital 71 LED.
[78] *Ibid.*
[79] E.g. through the use of special handling codes providing for example that data may only be used for the purpose of preventing and combating specific criminal offences; that it may not be disclosed or used in judicial proceedings without the permission of the EU competent authority; that it may not be disseminated to other authorities in the third country without the permission of the EU competent authority; and others.
[80] Article 4(1)(d) LED.
[81] Article 4(1)(f) LED.
[82] Recital 71 LED.

- Case-law of the CJEU, the European Court of Human Rights and decisions of Member States' Courts and data protection supervisory authorities in relation to transfers to specific third countries;[83]

- Assessments already conducted by EU bodies or agencies (e.g. Europol, Eurojust, EPPO, Frontex) before concluding cooperation agreements with third countries.

- Reports or assessments produced by national Ministries of Foreign Affairs, Justice and Interior;

- Relevant legislation and case-law of that third country (including case-law of international human rights courts with jurisdiction over the third country), and decisions taken by independent administrative authorities competent on privacy and data protection matters;

- Reports of independent oversight or parliamentary bodies in that third country;

- Resolutions, reports and notifications from intergovernmental organisations on the third country on relevant aspects to data protection such as rule of law, human rights, and compliance with international rules on the processing of police data;

- Reports from other sources such as academia, civil society organisations (e.g. NGOs), etc.

4.3 What actions to take upon concluding on the appropriateness of the existing safeguards

4.3.1 Assuming enhanced accountability obligations by using Article 37(1)(b) LED

89. The fact that the transfer mechanisms provided in Articles 36-38 LED operate in cascade in general also affects the accountability obligations of the controller. In other words, the place in which the transfer mechanism is positioned in the order provided by LED is in general inversely proportional to the accountability obligations of the controller. For instance, for transfers based on adequacy decisions issued by the Commission, the controllers being bound by them should only monitor that the adequacy decision remains valid. For transfers based on appropriate safeguards under Article 37(1)(b) LED, the competent authorities should assess and, in the case of categories of transfers, regularly monitor, the appropriateness of the safeguards, which have to meet the standard of essential equivalence, and further document the details of the assessment and of the transfer.

90. This is reflected in Article 37(2) and 37(3) LED which indeed provide that the controllers have the obligation (i) to inform the supervisory authorities of categories of transfers taking place under the controller's assessment (Article 37(1)(b)); (ii) to document in detail such transfers, including as regards the assessment undertaken prior to the transfer and (iii) to make the documentation available to the supervisory authority on request. The documentation requirements are extensive and include all the elements provided for the documentation of transfers carried out under the regime of derogations, i.e. including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

91. The accountability obligations on the controller are enhanced because it is the controller alone who determines, based on its own assessment, whether appropriate safeguards exist. This involves higher risks of inconsistencies with other assessments of transfers, less transparency, and less legal certainty

[83] Some of these decisions may be found in the EDPB's registry of decisions taken under the one-stop-shop mechanism: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en. References to national decisions may be found in the national news section of the EDPB's website: https://edpb.europa.eu/news/news_en?news_type=2.

for data subjects in comparison with transfers legally framed by adequacy decisions or legally binding instruments. Therefore, transfers under 37(1)(b) LED should be documented in detail, including with regard to the initial assessment of the safeguards in place, while the supervisory authorities should be informed on the categories of such transfers in order to allow for an effective scrutiny.

92. With regard to the obligation imposed by Article 37(2) LED and taking into account the justifying reason for adopting this provision, the competent authorities should inform their data protection authorities in regular intervals about the categories of transfers that were carried out under 37(1)(b) LED. The information submitted should include the receiving competent authorities as well as the number of transfers per category. This would allow the supervisory authorities to have a general overview and to focus their action with regard to possible 'ex post' lawfulness control on specific categories of transfers.

4.3.2 Including categories of transfers in record of processing activities

93. In line with the provision of Article 24 LED the controller is under the obligation to maintain a record of all categories of processing activities under their responsibility, which shall contain the specific and detailed information provided in this provision. The duty of controllers to keep records on processing operations is one of the means to reinforce accountability. Knowing which data are processed about what kind of data subjects and for what purposes is a prerequisite for being able to be held accountable and the controller must be able to give account to the supervisory authority about the categories of data and data subjects and the purposes of its processing operations.

94. A further item to be documented under Article 24(1)(f) LED is the categories of transfers of data to 'a third country or an international organisation'. In such cases, the third country, or international organisation respectively, must be named in the records, but evidently not the identity of the recipient, as the provision does not add anything to point c) for cases of international data transfers. Hence, reference to the categories of recipients would be sufficient.

95. The wording of Article 24(1)(f) LED implies that there is no obligation to name the means by which the controller intends to ensure an adequate level of protection in case transfers of personal data are carried out. However, interpreted in conjunction with Article 37(2) LED which pertains to specific categories or sets of transfers which are defined by some common characteristics as well as to one-time transfers to third countries or international organisations, it would be optimal if the envisaged transfer mechanism is referred in the record. In this way, the obligation of the controller to inform the supervisory authority on the categories of transfers taking place under the controller's assessment of the existence of appropriate safeguards will be facilitated.

96. The information with regard to transfers included in the records should be kept up to date.

4.3.3 Preserving the assessments with regard to transfers, reviewing and updating them

97. One of the accountability obligations imposed on the controller in case Article 37(1)(b) applies is the detailed documentation of the transfer in line with Article 37(3) LED which should as minimum include the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred. Some of these documentation requirements, e.g. the date and time of the transfer, could be fulfilled by preserving logs as prescribed by Article 25 LED according to which the competent authority should, among other things, keep logs for the disclosure of personal data including transfers.

98. Taking into account that the obligation to document the transfers is set by the legislator in order to facilitate the 'ex post' lawfulness control by the supervisory authorities, the documentation should

include information that is sufficient and facilitates this control. To this end, the justification of the transfer refers to the assessment of the circumstances of the transfer that takes into account all the factors analysed above for defining the transfer categories (under Section 4.2.2) and for assessing whether appropriate safeguards are in place (under Section 4.2.3).

99. In more detail the documentation of the assessment of the circumstances should include:

i. A statement confirming that an adequacy decision or a legally binding agreement providing appropriate safeguards were not available.
ii. The definition of the categories / set of transfers or specific transfer which are/is subject to the assessment.
iii. The identification of the risks entailed to the rights of the data subjects by the categories / set of transfers or specific transfer. In identifying the risks the following factors should be, inter alia, taken into account: the country or countries to which the data is transferred; the categories of data subjects affected (suspects, convicted criminals, victims, witnesses, persons of interest, associates); the categories (in particular whether special categories are included) and the quantity of the data transferred; the specific purpose of the transfer; the competent authorities to which the data is transferred; the seriousness of the criminal offence in relation to which the transfer of data takes place; the authority at the origin of the transfer (judicial or law enforcement authority); the nature and conditions of execution of the criminal penalty provided in the third country for the criminal offence in relation to which the transfer of data takes place; the possible existence of the death penalty in relation to the criminal offence for which the data is transferred.
iv. The assessment on whether appropriate safeguards with regard to the risks identified (see point iii) offering an essentially equivalent level of protection are in place. Such assessment must be based on the relevant legal framework (international commitments and domestic legislation, be it a specific data protection law or any other source of applicable law such as criminal law or criminal procedure law) and practices in the country or countries to which the data is transferred.
v. The registration of the outcome of the assessment. In case it is negative, assess whether additional safeguards can be provided for in MOUs, exchanges of letters and other arrangements.
vi. In the latter case, any additional safeguards provided for in MOUs, exchanges of letters and other arrangements.

100. The controllers under the principle of accountability are obliged to monitor carefully if there have been or there will be any developments with regard to the factors taken into account for assessing the appropriateness of the existing safeguards that may affect the outcome of their assessment.

4.3.4 Cooperating with supervisory authorities

101. The LED integrates accountability as a fundamental data protection principle in the context of law enforcement (Article 4(4) LED). The controllers are not only responsible but they shall also demonstrate to the supervisory authorities compliance with the data protection principles provided in Article 4. To that end Article 26 LED establishes a legal obligation for controllers to cooperate with the supervisory authority when exercising its tasks. Such cooperation must be provided on request of the supervisory authority.

102. As regards the means of fulfilling this obligation, Article 24(3), 25(3) and 37(2) and (3) LED provide that the controllers should inform their supervisory authorities on categories of transfers carried out under 37(1)(b) and make available to them at their request the records of processing operations, their logs as well as the documentation required in cases where the controller has assessed the circumstances surrounding a transfer and concluded that appropriate safeguards are in place. However, there is nothing in the wording of the relevant provisions and in particular of Article 26 LED that limits the ways of cooperation. To the contrary the obligation to cooperate should be fulfilled as requested by the supervisory authority, which may include providing additional information (even originating from the destination country) and documentation, granting access to processing facilities, and explaining processing operations.

103. Violations of the obligation to cooperate with the supervisory authority could be sanctioned. In the context of the LED, the rules on penalties applicable to infringements of the provisions adopted pursuant to the LED are defined by the Member States and shall be effective, proportionate and dissuasive (Article 57 LED). Hence, infringement by a competent authority of the obligation to cooperate with its supervisory authority could lead to penalties, defined under national law, independently of the existence of other infringements of the provisions transposing the LED (such as the provisions with regard to transfers). The above considerations are without prejudice to the fact that the controllers are at every time under the obligation to implement binding decisions of their supervisory authorities exercising their corrective powers (e.g. heeding the warning with regard to a possible infringement of the data protection legal framework in case a specific transfer takes place or stop a set of transfers in case a ban is issued).