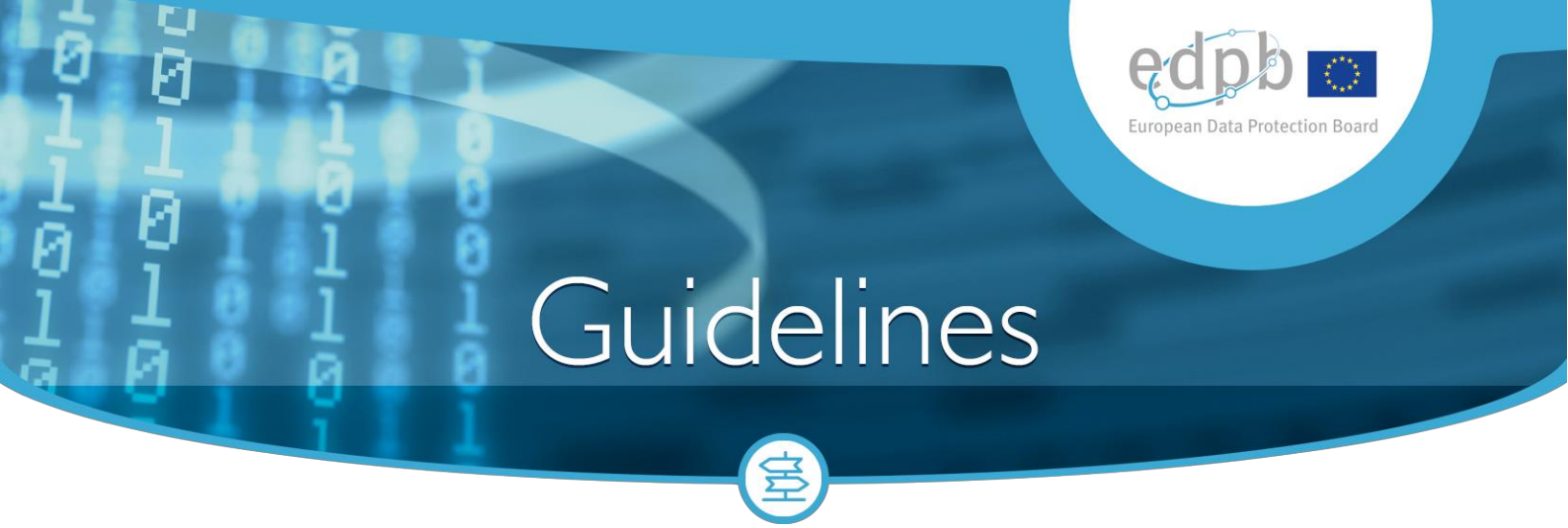


# Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies

## Version 2.0

## Adopted on 15 December 2020

## Version history

| | | |
|---|---|---|
| Version 2.0 | 15 December 2020 | Adoption of the Guidelines after public consultation |
| Version 1.0 | 18 February 2020 | Adoption of the Guidelines for public consulation |

# Table of contents

## The European Data Protection Board

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

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

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

**HAS ADOPTED THE FOLLOWING GUIDELINES**

[1] References to "Member States" made throughout these guidelines should be understood as references to "EEA Member States".

# 1 GENERAL

## 1.1 Purpose

1. This document seeks to provide guidance as to the application of Articles 46 (2) (a) and 46 (3) (b) of the General Data Protection Regulation (GDPR) on transfers of personal data from EEA public authorities or bodies (hereafter "public bodies") to public bodies in third countries or to international organisations, to the extent that these are not covered by an adequacy finding adopted by the European Commission[2]. Public bodies may choose to use these mechanisms, which the GDPR considers more appropriate to their situation, but are also free to rely on other relevant tools providing for appropriate safeguards in accordance with Article 46 GDPR.

2. The guidelines are intended to give an indication as to the expectations of the European Data Protection Board (EDPB) on the safeguards required to be put in place by a legally binding and enforceable instrument between public bodies pursuant to Article 46 (2) (a) GDPR or, subject to authorisation from the competent supervisory authority (SA), by provisions to be inserted into administrative arrangements between public bodies pursuant to Article 46 (3) (b) GDPR.[3] The EDPB strongly recommends parties to use the guidelines as a reference at an early stage when envisaging concluding or amending such instruments or arrangements.[4]

3. The guidelines are to be read in conjunction with other previous work done by the EDPB (including endorsed documents by its predecessor, the Article 29 Working Party[5] ("WP29")) on the central questions of territorial scope and transfers of personal data to third countries[6]. The guidelines will be reviewed and if necessary updated, based on the practical experience gained from the application of the GDPR.

4. The present guidelines cover international data transfers between public bodies occurring for various administrative cooperation purposes falling within the scope of the GDPR. As a consequence and in accordance with Article 2 (2) of the GDPR, they do not cover transfers in the area of public security, defence or state security. In addition, they do not deal with data processing and transfers by competent authorities for criminal law enforcement purposes, since this is governed by a separate specific instrument, the law enforcement Directive[7]. Finally, the guidelines only focus on transfers between public bodies and do not cover transfers of personal data from a public body to a private entity or from a private entity to a public body.

---

[2] For example Japanese public bodies, which are not covered by the Japan Adequacy Decision as it only covers private sector organisations.

[3] These guidelines use the term "international agreements" to refer to legally binding and enforceable instruments pursuant to Article 46(2)(a) GDPR and to administrative arrangements pursuant to Article 46(3)(b) GDPR.

[4] Art. 96 GDPR states that agreements that were concluded prior to 24 May 2016 shall remain in force until amended, replaced or revoked.

[5] The Working Party of EU Data Protection Authorities established under Article 29 of the Data Protection Directive 95/46/EC.

[6] See Article 29 Working Party, Adequacy Referential (WP254 rev.01, endorsed by the EDPB on 25 May 2018), EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 and EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

[7] Directive (EU) 2016/680 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.

## 1.2 General rules applicable to international transfers

5. According to Article 44 of the GDPR the data exporter transferring personal data to third countries or international organisations must, in addition to complying with Chapter V of the GDPR, also meet the conditions of the other provisions of the GDPR. In particular, each processing activity must comply with the data protection principles in Article 5 GDPR, be lawful in accordance with Article 6 GDPR and comply with Article 9 GDPR in case of special categories of data. Hence, a two-step test must be applied: first, a legal basis must apply to the data processing as such together with all relevant provisions of the GDPR; and as a second step, the provisions of Chapter V of the GDPR must be complied with.

6. The GDPR specifies in its Article 46 that "*in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available*". Such appropriate safeguards may be provided for by a legally binding and enforceable instrument between public bodies (Article 46 (2) (a) GDPR) or, subject to authorisation from the competent SA, by provisions to be inserted into administrative arrangements between public bodies which include enforceable and effective data subject rights (Article 46 (3) (b) GDPR). As clarified by the Court of Justice of the European Union (CJEU), such appropriate safeguards must be capable of ensuring that data subjects whose personal data are transferred are afforded a level of protection essentially equivalent to that which is guaranteed within the EEA.[8]

7. Aside from this solution and in its absence, Article 49 of the GDPR also offers a limited number of specific situations in which international data transfers may take place when there is no adequacy finding by the European Commission[9]. In particular, one exemption covers transfers necessary for important reasons of public interest recognised in Union law or in the law of the Member State to which the controller is subject, including in the spirit of reciprocity of international cooperation[10]. However, as explained in previous guidance issued by the EDPB, the derogations provided by Article 49 GDPR must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive[11].

## 1.3 Definition of a public authority or body

8. The GDPR does not define what constitutes a 'public authority or body'. The EDPB considers that this notion is broad enough to cover both public bodies in third countries and international organisations.[12] With respect to public bodies in third countries, the notion is to be determined under domestic law. Accordingly, public bodies include government authorities at different levels (e.g. national, regional and local authorities), but may also include other bodies governed by public law (e.g. executive agencies, universities, hospitals, etc.).[13] In accordance with Article 4 (26) GDPR, 'international

[8] Court of Justice of the European Union, Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems ("Schrems II"), para. 96.
[9] For further information on Article 49 and its interplay with Article 46 in general, please see EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.
[10] See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, page 10.
[11] See EDPB Guidelines on derogations of Article 49 under Regulation 2016/679, page 5.
[12] See also recital 108 of the GDPR.
[13] See, e.g. the definition of 'public sector body' and 'body governed by public law' in Article 2 (1) and (2) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public-sector information (OJ L 345, 31.12.2003, page 90).

organisation' refers to an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two countries.

9. The EDPB recalls that the application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of international organisations. At the same time, it is important to recall that any EEA public body transferring data to international organisations has to comply with the GDPR rules on transfers to third countries or international organisations.[14]

# 2 GENERAL RECOMMENDATIONS FOR THE APPROPRIATE SAFEGUARDS UNDER BOTH ARTICLES 46 (2) (a) AND 46 (3) (b) GDPR

10. Unlike Article 26 (2) of the 95/46/EC Directive, Article 46 of the GDPR provides for additional appropriate safeguards as tools for transfers between public bodies:

    (i) a legally binding and enforceable instrument, Article 46 (2) (a) GDPR or
    (ii) provisions to be inserted into administrative arrangements, Article 46 (3) (b) GDPR.

    These instruments and arrangements may be of bilateral or multilateral nature.

11. The following section provides some general recommendations to help ensure that legally binding instruments or administrative arrangements (hereinafter "international agreements") between public bodies are in compliance with the GDPR.

12. Although Article 46 and recital 108 of the GDPR do not provide specific indications on the guarantees to be included in such international agreements, taking into account Article 44 of the GPDR[15] and the recent CJEU case law[16] the EDPB hereby has elaborated a list of minimum safeguards to be included in international agreements between public bodies falling under Articles 46 (2) (a) or 46 (3) (b) GDPR. These safeguards aim to ensure that the level of protection of natural persons under the GDPR is not undermined when their personal data is transferred outside of the EEA and that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the EU by the GDPR.[17]

13. In accordance with the recent CJEU case law[18], it is the responsibility of the transferring public body in a Member State, if needed with the help of the receiving public body, to assess whether the level of protection required by EU law is respected in the third country, in order to determine whether the list of safeguards included in the international agreement can be complied with in practice, taking into account the possible interference created by the third country legislation with compliance with these safeguards.

---

[14] See EDPB Guidelines 3/2018 on the territorial scope of the GDPR, p. 23.
[15] Article 44 of the GDPR states: "*All provisions of this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"
[16] CJEU, July 16, 2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II").
[17] CJEU, July 16, 2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), para 105.
[18] Idem.

14. In this respect, it should also be noted that, to ensure the safeguards listed in these guidelines, international agreements can build on already existing elements in the national law of a third country or the internal rules/regulatory framework of an international organisation.

## 2.1 Purpose and scope

15. International agreements should define their scope and their purposes should be explicitly and specifically determined. In addition, they should clearly state the categories of personal data affected and the type of processing of the personal data which is transferred and processed under the agreement.

## 2.2 Definitions

16. International agreements should contain definitions of the basic personal data concepts and rights in line with the GDPR relevant to the agreement in question. By way of example, such agreements should, if referenced, include the following important definitions: “personal data”, “processing of personal data”, “data controller”, “data processor", “recipient” and “sensitive data”.

## 2.3 Data protection principles

17. International agreements shall contain specific wording requiring that the core data protection principles are ensured by both parties.

### 2.3.1 Purpose limitation principle

18. International agreements need to specify the purposes for which personal data is to be transferred and processed including compatible purposes for further processing, as well as to ensure that the data will not be further processed for incompatible purposes. Compatible purposes may include storing for archiving purposes in the public interest, as well as processing for scientific or historical research purposes or statistical purposes. It is recommended, for better clarity, that the specific purposes for the processing and transferring of the data are listed in the international agreement itself.

19. To avoid any risk of a “function creep”, such agreements should also specify that transferred data cannot be used for any purpose other than those expressly mentioned in the agreement, except as set out in the paragraph below.

20. If both parties to the international agreement wish to allow the receiving public body to make another compatible use of the transmitted personal data, further use by the receiving public body shall only be permitted if compatible with the original one and previously notified to the transferring public body which may oppose for specific reasons.

### 2.3.2 Data accuracy and minimisation principles

21. The international agreement must specify that the data transferred and further processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are transmitted and further processed.

22. In practice, this data minimisation principle is important to avoid the transfer of personal data when they are inadequate or excessive.

23. Moreover, data should be accurate and up to date, having regard to the purposes for which they are processed. An international agreement must therefore provide that the transferring party will ensure

that the personal data transferred under the agreement is accurate and, where applicable, up to date. In addition, the agreement should provide that, if one of the parties becomes aware that inaccurate or out of date data has been transmitted or is being processed, it must notify the other party without delay. Finally, the agreement should ensure that, where it is confirmed that data transmitted or being processed is inaccurate, each party processing the data shall take every reasonable step to rectify or erase the information.

### 2.3.3 Storage limitation principle

24. Parties must ensure that the international agreement contains a data retention clause. This clause should specify in particular that personal data shall not be retained indefinitely but shall be kept in a form which permits identification of data subjects only for the time necessary for the purpose for which it was transferred and subsequently processed. That may include storing it for as long as necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that appropriate technical and organisational measures are put in place to safeguard the rights and freedoms of the data subjects, such as additional technical measures (e.g. security measures, pseudonymisation) and access restrictions. When a maximum retention period is not already set in national legislation or the internal rules/regulatory framework of an international organisation, a maximum retention period should be set in the text of the agreement.

### 2.3.4 Security and confidentiality of data

25. The parties should commit to ensure the security and the confidentiality of the personal data processing and transfers they carry out.
In particular, the parties should commit to having in place appropriate technical and organisational measures to protect personal data against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. These measures may include, for example, encryption including in transit, pseudonymisation, marking information as personal data transferred from the EEA, restricting who has access to personal data, providing secure storage of personal data, or implementing policies designed to ensure personal data are kept secure and confidential.
The level of security should take into consideration the risks, the state of the art and the related costs.

26. The international agreement may furthermore specify that, if one of the parties becomes aware of a personal data breach, it will inform the other party (ies) as soon as possible and use reasonable and appropriate means to remedy the personal data breach and minimise the potential adverse effects, including by communicating to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person.
It is recommended that the notification timeline for a personal data breach as well as the procedures for communication to the data subject are defined in the international agreement.

## 2.4 Rights of the data subjects

27. The international agreement must ensure enforceable and effective data subject rights as specified in article 46 (1) and recital 108 of the GDPR.

28. The rights available to the data subjects, including the specific commitments taken by the parties to provide for such rights, should be listed in the agreement. To be effective, the international agreement must provide for mechanisms that ensure their application in practice. Moreover, any breach of data subject rights must carry an appropriate remedy.

### 2.4.1 Right to Transparency

29. Parties must ensure that the international agreement contains clear wording describing the transparency obligations of the parties.

30. Such obligations should include on the one hand, a general information notice with, as a minimum, information on how and why the public bodies may process and transfer personal data, the relevant tool used for the transfer, the entities to which such data may be transferred, the rights available to data subjects and applicable restrictions, available redress mechanisms and contact details for submitting a dispute or claim.

31. However, it is important to recall that, for the transferring public body, a general information notice on the website of the public body concerned will not suffice. Individual information to data subjects should be made by the transferring public body in accordance with the notification requirements of Articles 13 and 14 GDPR[19].
The international agreement can also provide for some exceptions to such individual information. These exceptions are limited and should be in line with the ones provided under Article 14 (5) GDPR, for example where the data subject already has the information or where the provision of such information proves impossible or would involve a disproportionate effort.

32. The parties must commit to make the international agreement available to data subjects on request and to make the international agreement or the relevant provisions providing for appropriate safeguards publicly available on their website. To the extent necessary to protect sensitive or other confidential information, the text of the international agreement may be redacted prior to sharing a copy or making it publicly available. Where necessary to allow the data subject to understand the content of the international agreement, the parties must provide a meaningful summary thereof.

### 2.4.2 Rights of access, to rectification, erasure, restriction of processing and to object

33. The international agreement should safeguard the data subject's right to obtain information about and access to all personal data relating to him/her that are processed, the right to rectification, erasure and restriction of processing and where relevant the right to oppose to the data processing on grounds relating to his or her particular situation.

34. As regards the right of access, the international agreement should specify that individuals shall have the right vis-à-vis the receiving public body to obtain confirmation as to whether or not personal data concerning him/her is being processed, and if that is the case, access to that data; as well as to specific information concerning the processing, including the purpose of the processing, the categories of personal data concerned, the recipients to whom personal data is disclosed, the envisaged storage period and redress possibilities.

35. The agreement should furthermore specify when these rights can be invoked and include the modalities on how the data subjects can exercise these rights before both parties as well as on how the parties will respond to such requests. For example, with respect to deletion, the international agreement could state that data is to be deleted when the information has been processed unlawfully or is no longer necessary for the purpose of processing. Moreover, the international agreement should stipulate that the parties will respond in a reasonable and timely manner to requests from data subjects. The international agreement could also state that the parties may take appropriate steps,

[19] See EDPB Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, pages 13 to 22.

such as charging reasonable fees to cover administrative costs where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character.

36. The international agreement should also allot an obligation of the transferring public body to provide information to the data subject, once his/her personal data have been transferred, on the action taken on his/her request under the rights provided for by the international agreement without undue delay by setting an appropriate time limit (e.g. one month). Finally, information should be provided to the data subject, if the parties do not take action on the request of the data subject, without delay by setting an appropriate time limit (e.g. within one month of receipt of the request), of the reasons for not taking action and on the possibility of lodging a complaint and of seeking a judicial remedy.

37. The international agreement can also provide for exceptions to these rights. For example, exceptions to the right of access and deletion such as the ones provided under Article 15 (4) and 17 (3) GDPR could be provided. Similarly, exceptions to individual rights could be foreseen where personal data is processed for scientific or historical research purposes, statistical purposes, or archiving purposes, in so far as such rights would be likely to render impossible or seriously impair the achievement of these specific purposes, and provided that appropriate safeguards are put in place (e.g. technical and organisational measures, including pseudonymisation). Finally, the agreement may provide that the parties may decline to act on a request that is manifestly unfounded or excessive.

### 2.4.3 Automated individual decision-making

38. If relevant to the agreement in question, international agreements should as a general principle contain a clause stating that the receiving public body will not take a decision based solely on automated individual decision-making, including profiling, producing legal effects concerning the data subject in question or similarly affecting this data subject. Where the purpose of the transfer includes the possibility for the receiving public body to take decisions solely on automated processing in the sense of Article 22 GDPR, this should only take place under certain conditions set forth in the international agreement, such as the need to obtain the explicit consent of the data subject. If the decision does not comply with such conditions, the data subject should have the right not to be subject to it. Where it allows automated individual decision-making, the international agreement should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision and obtain human intervention.

### 2.4.4 Right to Redress

39. The safeguarded data subject rights have to be enforceable and effective. Therefore, the data subject must have access to redress. Different examples of ways to offer redress mechanisms are indicated below under sections 2.7 and 3.

### 2.4.5 Restrictions to the Rights of the data subjects

40. The international agreement can also provide for restrictions to the rights of data subjects. These restrictions should be in line with the restrictions envisaged by Article 23 GDPR. Such a restriction has to be a necessary and proportionate measure in a democratic society to safeguard important objectives of public interest, in line with the ones listed in Article 23(1) GDPR, including the rights and freedom of others, national security, defence or the prevention, investigation, detection or prosecution of criminal offences. It needs to be provided by law or, in the case of international

organisations, the applicable internal rules/regulatory framework, and shall continue only for as long as the reason for the restriction continues to exist.

### 2.5 Restrictions on onward transfers and sharing of data (including disclosure and government access)

41. Onward transfers by the receiving public body or international organisation to recipients not bound by the agreement should, as a rule, be specifically excluded by the international agreement. Depending on the subject matter and the particular circumstances at hand, the parties may find it necessary to allow onward transfers. In this case, under the condition that the purpose limitation principle is respected[20], the international agreement should foresee that such onward transfers can only take place if the transferring public body has given its prior and express authorisation and the receiving third parties commit to respect the same data protection principles and safeguards as included in the international agreement. This should include a commitment to provide to data subjects the same data protection rights and guarantees as provided in the international agreement in order to ensure that the level of protection will not be diminished if data are onward transferred.

42. As a rule, the same safeguards as for onward transfers should apply to sharing of personal data within the same country, i.e. the international agreement shall exclude this onward sharing and exemptions should in general only be allowed if the transferring public body has given its prior and express authorization and the receiving third parties commit to respect the same data protection principles and safeguards as included in the international agreement.

43. It is recommended that before requesting the express authorisation of the transferring public body the receiving public body or international organisation provides sufficient information on the type of personal data that it intends to transfer/share, the reasons and purposes for which it considers it to be necessary to transfer/share the personal data as well as, in case of onward transfers, the countries or international organisations to which it intends to onward transfer personal data so as to be able to assess the third country legislation or, in the case of international organisations, the applicable internal rules/regulatory framework.

44. In cases where it is necessary to allow sharing of personal data with a third party in the same country of the receiving public body or another international organisation, the sharing could be allowed in specific circumstances either with prior and express authorization of the transferring public body or as long as there is a binding commitment from the receiving third party to respect the principles and guarantees included in the international agreement.

45. In addition, the international agreement could specify exceptional circumstances in which onward sharing could take place without prior authorisation or the abovementioned commitments in line with the derogations listed in Article 49 of the GDPR, for example when this specific sharing would be necessary in order to protect the vital interests of the data subject or other persons or necessary for the establishment, exercise or defence of legal claims. Such exceptional circumstances could also arise if the onward sharing is required under the law of the receiving party, as necessary for directly related investigations/ court proceedings.

46. In the cases mentioned in the paragraph above, the international agreement should clearly state the specific and exceptional circumstances under which such data sharing is allowed. The receiving public body or international organisation should also be obliged to notify the transferring public body prior to the sharing and include information about the data shared, the receiving third party and the legal

[20] See above under 2.3.1.

basis for the sharing. In its turn the transferring public body should keep a record of such notifications from the receiving public body or international organisation and provide its SA with this information upon request. Where providing such notification prior to the sharing will impinge on confidentiality obligations provided for by law, e.g. to preserve the confidentiality of an investigation, the specific information should be provided as soon as possible after the sharing. In such a case, general information on the type of requests received over a specified period of time, including information about the categories of data requested, the requesting body and the legal basis for disclosure, should be provided to the transferring body at regular intervals.

47. In all of the above scenarios, the international agreement should only allow disclosures of personal data to other public authorities in the third country of the receiving public body that do not go beyond what is necessary and proportionate in a democratic society to safeguard important objectives of public interest in line with the ones listed in Article 23 (1) GDPR and in accordance with the jurisprudence of the CJEU. In order to assess a possible access by third country public authorities for surveillance purposes, the transferring public authority should take into account the elements recalled in the four European Essential Guarantees[21]. These include the availability of an effective remedy for data subjects in the third country of the receiving public body if their personal data is accessed by public authorities.[22] In case of transfers to international organisations, any such access must be in compliance with international law and without prejudice in particular to the privileges and immunities of the international organisation.

48. Depending on the case at hand, it may be useful to require to include an annex to the international agreement enumerating the laws governing onward sharing with other public bodies including for surveillance purposes in the destination country. Any changes to this annex should be notified to the transferring party within a set period of time.

### 2.6 Sensitive data

49. If an international agreement provides for the transfer of sensitive personal data within the meaning of Article 9 (1) of the GDPR, additional safeguards addressing the specific risks, to be implemented by the receiving public body or international organisation, should be included. These could, for example, include restrictions as access restrictions, restrictions of the purposes for which the information may be processed, restrictions on onward transfers, etc. or specific safeguards, e.g. additional security measures, requiring specialized training for staff allowed to access the information.

### 2.7 Redress mechanisms

50. In order to guarantee enforceable and effective data subjects rights the international agreement must provide for a system that enables data subjects to continue to benefit from redress mechanisms after their data has been transferred to a non EEA country or an international organisation. These redress mechanisms must provide recourse for individuals who are affected by non-compliance with the provisions of the chosen instrument and thus the possibility for data subjects whose personal data have been transferred from the EEA to lodge complaints regarding such non-compliance and to have these complaints resolved. In particular, the data subject must be ensured an effective route to complain to the public bodies that are parties to the international agreement and (either directly or

[21] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
[22] See EDPB Recommendations 02/2020, Guarantee D, p. 13 and seq.

after having addressed the relevant party) to an independent oversight mechanism. Moreover, a judicial remedy should, in principle, be available.

51. First, the receiving public body should commit to put in place a mechanism to effectively and timely handle and resolve complaints from data subjects concerning compliance with the agreed data protection safeguards. Moreover, data subjects should be provided with the possibility to obtain effective administrative redress before an independent oversight body, including, where available, an independent data protection authority[23].

52. Second, the agreement should allow for a judicial remedy including compensation for damages - both material and non-material - as a result of the unlawful processing of the personal data. If there is no possibility to ensure effective judicial redress, for example due to restrictions in the domestic law or the specific status of the receiving public body, e.g. international organisations, the international agreement must provide for alternative safeguards. Those alternative safeguards must offer the data subject guarantees essentially equivalent to those required by Article 47 of the Charter of Fundamental Rights of the European Union (EU Charter)[24].

53. In that case, the international agreement could create a structure which enables the data subject to enforce its rights outside the courts, for example through quasi-judicial, binding mechanisms such as arbitration or alternative dispute resolution mechanisms such as mediation, which would guarantee an independent review and bind the receiving public body[25]. Moreover, the public body transferring the personal data could commit to be liable for compensation of damages through unlawful processing of the personal data which are testified by the independent review.
Exceptionally, other, equally independent and effective redress mechanisms could be put in place by the agreement, for instance effective redress mechanisms implemented by international organisations.

54. For all of the abovementioned redress mechanisms, the international agreement should contain an obligation for the parties to inform each other of the outcome of the proceedings, in particular if a complaint of an individual is dismissed or not resolved.

55. The redress mechanism must be combined with the possibility for the transferring public body to suspend or terminate the transfer of personal data under the international agreement where the parties do not succeed in resolving a dispute amicably until it considers that the issue has been satisfactorily addressed by the receiving public body. Such a suspension or termination, if carried out, must be accompanied by a commitment from the receiving public body to return or delete the personal data. The transferring public body must notify the suspension or termination to the competent national SA.

[23] See also section 2.8 on supervision mechanism.
[24] CJEU, July 16,2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), paras 96, 186 and seq.
[25] CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner ("Schrems"), paras 41 and 95; ECJ July 16,2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), paras 186,187,189, 195 and seq.

## 2.8 Supervision mechanisms

56. In order to make sure that all obligations created under the international agreement are fulfilled, the international agreement must provide for independent supervision monitoring the proper application of the agreement and interferences with the rights provided under the agreement.

57. First, the agreement should provide for internal supervision ensuring compliance with the agreement. Each party to the agreement should conduct periodic internal checks of the procedures put in place and of the effective application of the safeguards provided in the agreement. The periodic internal checks should also verify any changes in legislation that would prevent the party (ies) to comply with the data protection principles and safeguards included in the international agreement. Moreover, it could be provided that a party to the agreement can also request from another party to the agreement to conduct such a review. The international agreement must require that the parties must respond to inquiries from the other party concerning the effective implementation of the safeguards in the agreement. Each party conducting a review should communicate the results of the checks to the other party (ies) to the agreement. Ideally, such communication should also be made to the independent oversight mechanism governing the agreement.

58. In addition, the international agreement must include the obligation that a party informs the other party without delay if it is unable to effectively implement the safeguards in the agreement for any reason. For this case the international agreement must foresee the possibility for the transferring public body to suspend or terminate the transfer of personal data under the international agreement to the receiving public body until such time as the receiving public body informs the transferring public body that it is again able to act consistent with the safeguards. The transferring body must notify the change of situation as well as the suspension of transfers or termination of the agreement to the competent national SA.

59. Secondly, the agreement must provide for independent supervision in charge of ensuring that the parties comply with the provisions set out in the agreement. This follows directly from the EU Charter[26] and the European Convention of Human Rights (ECHR)[27] in accordance with the jurisprudence of the European Court of Human Rights (ECtHR) and in the terms established in primary law [28] as well as the corresponding case law.

[26] Articles 7, 8 and 47 of the EU Charter.
[27] Article 8 ECHR.
[28] Article 6 Lisbon Treaty
"1.*The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.*
*The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties.*
*The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.*
*2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.*
*3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law*."

60. The CJEU, has, since 2015[29], reiterated the necessity of having an independent redress and supervision mechanism.[30] Likewise, the ECtHR has frequently highlighted in its rulings that any interference with the right to respect for private life as enshrined in Article 8 ECHR needs to be subject to an effective, independent and impartial oversight system[31].

61. The agreement could, for example, invoke oversight by a competent supervisory authority, if there is one in the country of the public body receiving the EEA personal data, even if the GDPR does not specify that the competent supervisory authority needs to be the external oversight body. Moreover, the agreement could include the voluntary commitment of the receiving party to cooperate with the EEA SAs.

62. In the absence of a supervisory authority specifically in charge with the supervision of data protection law in the third country or at the international organisation, the need for an independent, effective and impartial supervisory oversight mechanism needs to be fulfilled by other means. The type of independent supervision mechanism put in place may depend on the case at hand.

63. The agreement could, for example, refer to existing oversight bodies in the third country other than a supervisory authority in the area of data protection. In addition, if no external independent oversight can be ensured from a structural or institutional point of view, e.g. because of the privileges and immunities of certain international organisations, oversight could be guaranteed through functionally autonomous mechanisms. The latter must be a body that, while not external itself, carries out its functions independently, i.e. free from instructions, with sufficient human, technical and financial resources, etc. The receiving party shall be bound by the decisions of the oversight body.

### 2.9 Termination clause

64. The international agreement should envisage that any personal data transferred from the EEA pursuant to the international agreement prior to its effective termination shall continue to be processed in accordance with the provisions of the international agreement.

[29] CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner ("Schrems"), paras 41 and 95.
[30] CJEU, July 27, 2017, Opinion 1/15 on the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data, 26 July 2017, para. 228 and seq.; CJEU, 30 April 2019, Opinion 1/17 on the Comprehensive Economic and Trade agreement between Canada and the European Union, para. 190 and seq.
[31] ECtHR, September 6, 1978, Klass, v. Germany, para. 55 and 56. The requirement stemming from the ECtHR also apply to any interference with Articles 7 and 8 of the EU Charter since, according to Article 52 (3) EU Charter, the meaning and scope of these fundamental rights shall be the same as those laid down by Article 8 ECHR.

# 3 SPECIFIC INFORMATION ON ARTICLE 46 GDPR

## 3.1 Specific information on legally binding and enforceable instruments - Article 46 (2) (a) GDPR

65. Article 46 (2) (a) GDPR allows EEA public bodies to base transfers to public bodies in a third country or an international organisation on instruments concluded between them without obtaining prior authorisation from a SA. Such instruments have to be legally binding and enforceable. Therefore, international treaties, public-law treaties or self-executing administrative agreements may be used under this provision.

66. Any legally binding and enforceable instrument should encompass the core set of data protection principles and data subject rights as required by the GDPR.

67. The parties are obliged to commit themselves to putting sufficient data protection safeguards for transferring data into place. As a consequence, the agreement should also set out the way in which the receiving public body will apply the core set of basic data protection principles and data subject rights to all transferred personal data in order to ensure that the level of protection of natural persons under the GDPR is not undermined.

68. If there is no possibility to ensure effective judicial redress in legally binding and enforceable instruments so that alternative redress mechanism have to be agreed upon, EEA public bodies should consult the competent SA before concluding these instruments.

69. Even if the form of the instrument is not decisive as long as it is legally binding and enforceable, the EDPB considers that the best option would be to incorporate detailed data protection clauses directly within the instrument. If, however, this solution is not feasible due to the particular circumstances, the EDPB strongly recommends incorporating at least a general clause setting out the data protection principles directly within the text of the instrument and inserting the more detailed provisions and safeguards in an annex to the instrument.

## 3.2 Specific information on administrative arrangements - Article 46 (3) (b) GDPR

70. The GDPR in its Article 46 (3) (b) also provides for alternative instruments in the form of administrative arrangements, e.g. Memorandum of Understanding “MOU”, providing protection through the commitments taken by both parties in order to bring their common arrangement into force.

71. In this respect, Article 46 (1) and recital 108 of the GDPR specify that these arrangements have to ensure enforceable data subject rights and effective legal remedies. Where safeguards are provided for in administrative arrangements that are not legally binding, authorisation by the competent SA has to be obtained.

72. It should be carefully assessed whether or not to make use of non-legally binding administrative arrangements to provide safeguards in the public sector, in view of the purpose of the processing and the nature of the data at hand. If data protection rights and redress for EEA individuals are not provided for in the domestic law of the third country or the internal rules/regulatory framework of the international organisation, preference should be given to concluding a legally binding agreement. Irrespective of the type of instrument adopted, the measures in place have to be effective to ensure the appropriate implementation, enforcement and supervision.

73. In administrative arrangements specific steps have to be taken to ensure effective individual rights, redress and oversight. In particular, to ensure effective and enforceable rights, a non-binding instrument should contain assurances from the public body receiving the EEA personal data that individual rights are fully provided by its domestic law and can be exercised by EEA individuals under the same conditions as is the case for citizens and residents of the concerned third country. The same applies if administrative and judicial redress is available to EEA individuals in the domestic legal framework of the receiving public body. Similarly, international organisations should provide assurances about individual rights provided by their internal rules, as well as the available redress mechanisms.

74. If this is not the case, individual rights should be guaranteed by specific commitments from the parties, combined with procedural mechanisms to ensure their effectiveness and provide redress to the individual. These specific commitments and procedural mechanisms must make it possible, in practice, to ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR.
Such procedural mechanisms may, for example, include commitments of the parties to inform each other of requests from EEA individuals and to settle disputes or claims in a timely fashion.

75. In addition, in case such disputes or claims cannot be resolved in an amicable way between the parties themselves, independent and effective redress to the individual must be provided by alternative mechanisms, for example through a possibility for the individual to have recourse to an alternative dispute resolution mechanism, such as arbitration or mediation. Such alternative dispute resolution mechanism must be binding[32].

76. Depending on the case at hand, a combination of all or some of the above measures should be provided for in the administrative agreement in order to ensure effective redress. Other measures not included in these guidelines could also be acceptable as long as they provide for independent and effective redress.

77. Each administrative arrangement developed in accordance with Article 46 (3) (b) GDPR will be examined by the competent SA on a case by case basis, followed by the relevant EDPB procedure, if applicable. The competent SA will base its examination on the general recommendations set out in these guidelines, but might also ask for more guarantees depending on the specific case.

[32] CJEU, July 16, 2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), paras 189, 196 and seq.

# 4 PROCEDURAL QUESTIONS

78. Administrative arrangements established under Article 46 (3) (b) GDPR will be examined on a case-by-case basis due to the requirements for an authorisation by the competent SA which, according to Article 46 (4) GDPR shall apply the consistency mechanism pursuant to Article 64 (2) GDPR. When integrating alternative redress mechanisms in binding and enforceable instruments pursuant to Article 46 (2) (a) GDPR, the EDPB recommends also seeking advice from the competent SA. The EDPB strongly advises to consult the competent SA at an early stage.

For the European Data Protection Board

The Chair

(Andrea Jelinek)