Toolbox on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries

Adopted on 14 March 2022

The European Data Protection Board

Having regard to Article 70(1)(u) and Article 50(a) 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 DOCUMENT

In the context of Article 50 GDPR concerning international cooperation with third countries competent data protection authorities, the following toolbox of essential data protection safeguards to be concluded in addition to or inserted in an enforcement cooperation agreement has been developed.

These safeguards can be either provided in an administrative arrangement or in an international agreement. Their wording will have to be adjusted accordingly depending on whether the tool developed will be an administrative arrangement or an international agreement, and on the specific circumstances of the transfers to be framed. As recalled in the guidelines 2/2020 of the EDPB concerning Article 46, 2) a) and Article 46, 3) b) of the GDPR[2], in administrative arrangements specific steps have to be taken to ensure effective individual rights, redress and oversight, preferably through assurances from the receiving party that its domestic law already provides for the essential safeguards. International agreements can establish safeguards directly within the international agreement or build on already existing elements in the national law of a third country.

The specific parts intended for administrative arrangements are highlighted in grey, while the specific parts for international agreements are highlighted in blue.

[1] References to "Member States" should be understood as references to "EEA Member States".
[2] 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

I- DEFINITIONS[3]

For purposes of this instrument:

(a) "Personal Data" means any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, location data, an identification number or to one or more factors specific to his/her physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(b) "Processing of Personal Data" ("**Processing**") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, Restriction of Processing, erasure or destruction;

(c) "Competent authority [of the parties][4]" means the authority competent to enforce data protection legislation, [X] within the EEA, and [Y] within the third country. Competent authorities under this instrument have regulatory mandates and responsibilities which include monitoring and enforcing the application of data protection rules, handling complaints, investigating possible infringements of data protection rules and imposing sanctions where necessary;

(d) "Receiving competent authority" means the competent authority receiving personal data transferred from the other competent authority;

(e) "Sharing of Personal Data" means the onward sharing of Personal Data by a competent authority receiving the data from the EEA competent data protection authority with a third party in its country consistent with [the enforcement cooperation agreement];

(f) "Onward Transfer" means the transfer of personal data by a receiving competent authority to a third party in another country;

(g) "Special categories of Personal Data/Sensitive Data" means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or data concerning a natural person's sex life or sexual orientation and data relating to criminal convictions and offences;

(h) [The **"National Applicable Data Protection Legislation"** means [the applicable legislation];]

[3] These definitions arise from the GDPR.
[4] In the context of an international agreement this shall be provided.

[(i) ["enforcement cooperation agreement" or "ECA"[5] means the enforcement cooperation agreement between the [third country competent authority] and the [European Economic Area Authority] to facilitate cooperation and the exchange of information;]][6]

(j) "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

(k) "Profiling" means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements:

(l) "Data Subject Rights" in this Agreement refers to the following:

- "Right of Information" means a Data Subject's right to receive information on the processing of Personal Data relating to him or her in a concise, transparent, intelligible and easily accessible form;

- "Right of access" means a Data Subject's right to obtain from a competent authority sending or receiving the data confirmation as to whether or not Personal Data concerning him or her are being processed 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, and where that is the case, to access Personal Data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing;

- "Right of rectification" means a Data Subject's right to have the Data Subject's inaccurate personal data corrected or complemented by a Party without undue delay;

- "Right of Erasure" means a Data Subject's right to have his or her Personal Data erased by a Party where the Personal Data are no longer necessary for the purposes for which they were collected or processed or where the data have been unlawfully collected or processed;

- "Right to Object" means a Data Subject's right to object at any time, on grounds relating to his or her particular situation, to processing of Personal data concerning him or her by a Party with the consequence that the Party shall no longer process the data unless the Party demonstrates compelling legitimate grounds for the processing that override the the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims;-

"Right of Restriction of Processing" means a Data Subject's right to restrict the processing of the Data Subject's Personal Data where the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data, where the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead , where a Party no longer needs the Personal Data for the purposes for which they

[5] The name of the agreement should be inserted here, as well as the name of the two concerned authorities in the EEA and in the third country.
[6] This definition should be provided in the context of an administrative arrangement, as an international agreement should include both the data protection safeguards and the relevant cooperation clauses.

were collected and the data subject opposes to the erasure but they are required by the data subject for the establishment, exercise or defence of legal claims;

- "Right not to be subject to automated decisions, including profiling" means a Data Subject's right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

II- PURPOSE AND SCOPE OF THE INSTRUMENT

The purpose of this instrument is to provide appropriate safeguards [and appropriate protection of confidentiality[7]] with respect to Personal Data transferred by [X] to [Y] pursuant to Article 46(3) of the GDPR and in the course of cooperation pursuant to [the ECA/this instrument]. The categories of personal data affected transferred and processed under [the ECA/this instrument] are listed in a dedicated annex by the Parties.

The Parties agree that the transfer of Personal Data, as set out in [the ECA/this instrument], between [X] and [Y] shall be governed by the provisions of this instrument for the Processing of Personal Data [in the exercise of their respective enforcement activities][8]/[as related to the exercise by competent authorities of the exercise of their respective enforcement activities.][9]. [This instrument is intended to supplement the ECA between the [X] and [Y].][10]

[[X] and [Y] confirm that they have the authority to act consistently with the terms of this instrument and that they have no reason to believe that existing applicable legal requirements prevent them from doing so.

[X) and [Y] confirm that they can fully comply with he safeguards set out in this Agreement on the basis of applicable legal requirements. [X] and [Y] provide safeguards to protect Personal Data through a combination of laws, regulations and their own internal policies and procedures.][11]

[Each party shall ensure that the competent authority will act consistently with the terms of this instrument and that no applicable legal requirements prevent the competent authority from doing so][12].

III – DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal Data transferred between [X] and [Y] may be processed by the receiving competent authority itself only to fulfil its enforcement functions in accordance with the GDPR for [X] and with [the applicable legislation of the third country] for [Y], for the purposes of enforcing data protection rules subject to the jurisdiction of [Y] and [X]. The onward Sharing as necessary for directly related investigations/court proceedings, including the purpose of such Sharing,

[7] See IIIa below concerning the protection of confidentiality and professional secrecy at the end of the document, to be inserted where necessary depending also on the legislation fo the third country.
[8] In the context of an Administrative arrangement.
[9] In the context of an international agreement.
[10] This would have to be foreseen in the context of an Administrative arrangement.
[11] This would have to be inserted in the context of an Administrative Arrangement.
[12] In the context of an international agreement this could be provided.

of such data by [Y], will be consistent with [the relevant applicable legislation of the third country] and by [X] will be consistent with the GDPR and the applicable national legislation, is governed by paragraph 7 below. [Y] will not process Personal Data it receives from [X] for any purpose other than as set forth in this instrument, and reciprocally, [X] will not process Personal Data it receives from [Y] for any purpose other than as set forth in this instrument.

2. Data quality and proportionality: The Personal Data transferred by [X] and [Y] must be accurate and must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and subsequently processed. A competent authority will inform the other competent authority if it becomes aware that previously transmitted or received information is inaccurate (incorrect or outdated) and/or must be updated. In such case, the competent authorities will make any appropriate corrections, having regard to the purposes for which the Personal Data have been transferred, which may include supplementing, erasing, restricting the processing of, correcting or otherwise rectifying the Personal Data as appropriate.

The Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further Processed, or for the time as required by applicable laws, rules and regulations provided [Y] has been informed by [X] of these applicable rules within the EEA and of the maximum period of retention for personal data provided in them, and that [X] has been informed of the applicable laws rules and regulations by [Y] as well as of the maximum period of retention for personal data provided in them and the maximum period is deemed proportionate and necessary in a democratic society, consistently with EU standards. These information shall be recorded in annex to this instrument. The Parties shall have in place appropriate procedures for the final destruction of the information received pursuant to this instrument.

3. Transparency: [X] and [Y] will provide general notice by publishing this instrument on their websites. Both [X and Y] will provide to Data Subjects information relating to the transfer and further Processing of Personal Data. Both [X and Y] will in principle provide general notice to Data Subjects about: (a) how and why it may Process and transfer Personal Data; (b) the type of entities to which such data may be transferred, (c) the rights available to Data Subjects under the applicable legal requirements, including how to exercise those rights; (d) information about any applicable delay or restrictions on the exercise of such rights, including restrictions that apply in the case of transfers of Personal Data; and (e) contact details for submitting a dispute or claim. This notice will become effective by publication of this information by both [X and Y] on their websites along with this instrument.

Individual notice will be provided to Data Subjects by [X] in accordance with the notification requirements and applicable exemptions and restrictions in the GDPR (as set forth in Articles 14 and 23 of the GDPR). Individual notice by [Y] in case of onward sharing and onward transfers will also be provided and reciprocally by [X] to [Y] in case of onward sharing and onward transfers. .

If after consideration of any applicable exemptions to individual notification and in the light of discussions with [Y], [X] concludes that it is required under the GDPR to inform a Data Subject of the sharing or of the transfer of his/her Personal Data to [Y], [X] will notify [Y] in advance of making such individual notification.

4. Security and confidentiality: [X] and [Y] acknowledge that in **Annex I**, [X] has provided information describing its technical and organizational measures in accordance with the GDPR and that [Y] has provided information describing its technical and organizational security measures deemed adequate by [X] to guard against accidental or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data. [Y] agrees to notify [X] of any change to the technical and organizational security measures that would adversely affect the level of protection afforded for Personal Data by this Agreement and will update the information in **Annex I** if such changes are made. In such case, [Y] provides such notification to [X] at least two months before the entry into force. Reciprocally [X] will notify [Y] under the same conditions and update the Annex I accordingly.

[Y] has provided to [X] a description of its applicable laws and/or rules relating to confidentiality and the consequences for any unlawful disclosure of non-public or confidential information or suspected violations of these laws and/or rules and reciprocally, [X] has provided the same information to [Y][13][14].

In the case where a receiving competent authority becomes aware of a Personal Data Breach affecting Personal Data that has been transferred under this instrument, it will inform the other competent authority without undue delay and, where feasible, not later than 24 hours after having become aware that it affects such Personal Data. The notifying competent authority shall also as soon as possible use reasonable and appropriate means to remedy the Personal Data Breach and minimize the potential adverse effects.

[X] and [Y] shall communicate 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 in order to allow him or her to take the necessary precautions. The communication shall describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects shall be made as soon as reasonably feasible, unless the competent authority has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, or it has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise, or it would involve disproportionate effort.

5. Data Subject Rights: A Data Subject whose Personal Data has been transferred to [Y] can exercise his/her Data Subject Rights as defined in Article I(j) with respect to the data received and processed under the instrument.

A Data Subject may make a request directly to [X] or [Y]:

Contact details for [X]:

- by e-mail to Xxx;

- by post to:

[13] See Annex I

[14] In the context of an international agreement: the international agreement may as well complement the laws and/or rules applicable to [Y] should they be missing or insufficient in [Y]'s legal framework, to provide the necessary safeguards to ensure the appropriate level of protection.

XXXxxx

Contact details for [Y]:

- by e-mail to Xxx;

- by post to:
XXXxxx

A data subject may also request that [X] identifies any Personal Data that has been transferred to [Y] and request that [X] confirms with [Y] that the Personal Data is complete, accurate and, if applicable, up-to-date and the Processing is in accordance with the Personal Data Processing principles in this Agreement. [Y] will address in a reasonable and timely manner any such request from [X] concerning any Personal Data transferred from [X] to [Y]. Upon receipt of a request from a Data Subject, [X] may also request from [Y] information related [Y]'s onward Sharing and onward transferring of such Personal Data in order for [X] to comply with its disclosure obligations to the Data Subject under [the GDPR and [national legislation applicable to [Y]]][15]/[this instrument][16]. Upon receipt of such a request from [X], [Y] shall provide to [X] any information that has been made available to [Y] concerning the processing of such Personal Data by a third party with whom [Y] has Shared or transferred such Personal Data. [Y] will also address in a reasonable and timely manner any such request from [X] concerning any Personal Data transferred from [X] to [Y].

[X] will also provide information to the data subject, once his/her personal data have been transferred, on the action taken on his/her request within one month. [X] will also inform the data subject 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. [X] and [Y] may take appropriate steps, such as charging reasonable fees to cover administrative costs or declining to act on a Data Subject's request that is manifestly unfounded or excessive.

The Data Subject Rights may be restricted to prevent prejudice or harm to supervisory or enforcement functions of the competent authorities acting in the exercise of the official authority vested in them; for important objectives of general public interest, as recognized in the [third country of Y] and [in the competent MS] or in the European Union, including in the spirit of reciprocity of international cooperation. The restriction should be necessary, proportionate and provided by law, and will apply only for as long as the reason for the restriction continues to exist.

Any dispute or claim brought by a Data Subject concerning the processing of his or her Personal Data pursuant to this instrument may be made to [X], [Y] or both, as applicable and as set out in Section 8.

[X] and [Y] agree that they will not take a legal decision concerning a Data Subject based solely on automated processing of Personal Data, including Profiling, without human involvement.

6. Special categories of Personal Data/Sensitive Data: Special categories of Personal Data/Sensitive Data, as defined in clause I (e), shall not be transferred by [X] to [Y] unless they are necessary for handling complaints, investigating possible infringements of data protection rules and imposing corrective measures where necessary. If they are transferred, additional safeguards shall be put in

[15] In the context of an administrative arrangement
[16] In the context of an international agreement

place by [Y] to be determined on a case by case basis, such as, for instance, access restrictions, restrictions of the purposes for which the information may be processed, restrictions on onward transfers, or specific safeguards, e.g. additional security measures, requiring specialized training for staff allowed to access the information.

7. Onward Sharing of Personal Data: [Y] will only Share Data received from [X] with those entities identified in[17] [the ECA][18]/[this instrument][19] and as required for the purpose of the specific enforcement action.

In the event that [Y] intends to Share any Personal Data with any third party identified [the ECA][20]/[this instrument][21] , [Y] will request the prior written authorisation of [X] and will only Share such Personal Data if the third party provides a commitment to respect the same data protection principles and safeguards as in this instrument. When requesting such prior written authorisation, [Y] should indicate the type of personal data that it intends to Share and the reasons and purposes for which [Y] intends to Share Personal Data. If [X] does not provide its written authorisation to such Sharing within a reasonable time, not to exceed ten days, [Y] will consult with [X] and consider any objections it may have.If [Y] decides to Share the Personal Data without [X] written authorisation, [Y] will notify [X] of its intention to Share. [X] may then decide whether to suspend the transfer of Personal Data.

[Y] may Share personal data with a third party without prior written authorisation and appropriate assurances in exceptional cases , where necessary to comply with legal obligations applicable to [Y] or in the context of legal proceedings within the limits that this sharing is also in addition for important reasons of public interest, as recognized in the [third country of Y] and in [the Member State of X] or in the European Union, or if the sharing is necessary for the establishment, exercise or defense of legal claims. In such cases, [Y] will periodically inform [X] of the nature of Personal Data Shared and the reason it was Shared if [Y] has Shared any Personal Data subject to this instrument with [third parties], if providing such information will not risk jeopardizing an ongoing investigation. Such restriction regarding information related to an ongoing investigation will continue only for as long as the reason for the restriction continues to exist.

Reciprocally, [Y] may request that [X] applies the same rules and safeguards for the further sharing of data received from [Y] in the context of this instrument.

8. Onward transfers of Personal Data: [Y] will only transfer Personal Data received from [X] to competent authorities in third countries only for the same purposes for which data have been transferred to it.

In the event that [Y] intends to Transfer any Personal Data to a third party in a third country , [Y] will request the prior written authorisation of [X] and will only Transfer such Personal Data where the level of protection of personal data will not be undermined, e.g. the third party provides a commitment to respect the same data protection principles and safeguards as in this Agreement or a relevant

[17] See Annex II as well.
[18] In the context of an administrative arrangement.
[19] In the context of an international agreement.
[20] In the context of an administrative arrangement.
[21] In the context of an international agreement.

adequacy decision is in place[22]. When requesting such prior written authorisation, [Y] should indicate the type of personal data that it intends to Transfer and the reasons and purposes for which [Y] intends to Transfer Personal Data. If [X] does not provide its written authorisation to such transfer within a reasonable time, not to exceed ten days, [Y] will consult with [X] and consider any objections it may have. Reciprocally, [Y] may apply the same procedure with [X] concerning onward transfers of data received by [X] from [Y] in the context of this instrument.

9. Effective Redress: [Y] shall provide information to [X] concerning its applicable law providing for redress to Data Subjects and reciprocally, [X] shall provide information to [Y] concerning its applicable law providing for redress to Data Subjects. This information shall be recorded in annex to the instrument. Any dispute or claim brought by a Data Subject concerning the processing of his or her Personal Data pursuant to this instrument may be made to [X], [Y], or both, as may be applicable. Each competent authority will inform the other competent authority about any such dispute or claim, and will use its best efforts to amicably settle the dispute or claim in a timely fashion[23].

[Any complaint will be handled by [X] in accordance with the GDPR and its national law. [Y] and [X] may provide each other with a detailed description of the complaint-handling mechanism and of the procedure applicable to it.

For example:

Any concerns or complaints regarding the Processing of Personal Data by [Y] may be reported directly to [Y internal organ/service for Enforcement/Referrals/Complaints], specifically through the [dedicated channel for complaints], where information may be provided through an online form on the web site, or via electronic mail, letter or telephone, or, alternatively to [X] by sending such information to its complaint department, as well as to its DPO. [Y] will inform [X] of reports it receives from Data Subjects on the Processing of his/her Personal Data that was received by [Y] from [X] and will consult with [X] on a response to the matter. Reciprocally, [X] will inform [Y] of complaints it receives from Data Subjects on the Processing of his/her Personal Data that was received by [X] from [Y] and will consult with [Y] on a response to the matter. [X] and [Y] and will respond in a reasonable and timely manner to requests from data subjects.][24]

A Data Subject has the right to obtain judicial redress (including to obtain access to and correction or deletion of personal data, and to obtain compensation for damages) according to [this instrument][25] / [the GDPR and the national law of [X]] and to [the national applicable legislation] for requests addressed against [Y]][26] if the safeguards laid down in this instrument are not complied with. In situations where [X] is of the view that [Y] has not acted consistent with the safeguards set out in this

[22] « Relevant adequacy decision » means an adequacy of the EU which recognizes that the data to be onward transferred will benefit from a level of protection substantially equivalent to the one provided within the EU when processed by the recipients in the third country.

[23] In the context of an international agreement: the international agreement may as well complement the laws and/or rules applicable to [Y] should they be missing or insufficient in [Y]'s legal framework, to provide the necessary safeguards to ensure the appropriate level of protection.

[24] This will have to be provided in the context of an administrative arrangement. In the context of an international agreement, more precise rules shall be provided to ensure that complaints concerning violations of the agreement will be handled by the competent authorities and how.

[25] In case of an international agreement

[26] In case of an administrative arrangement

instrument, [X] may suspend the transfer of Personal Data under this instrument until the issue is satisfactorily addressed and may inform the Data Subject thereof. Before suspending transfers, [X] will discuss the issue with [Y] and [Y] will respond without undue delay. Reciprocally, [Y] may suspend the transfers under this instrument on the same grounds and in the same manner.

10. Oversight: [X] and [Y] will conduct periodic reviews of its own policies and procedures that implement the safeguards over Personal Data described in the instrument. Upon reasonable request from the other competent authority, a competent authority will review its policies and procedures to ascertain and confirm that the safeguards specified in this instrument are being implemented effectively and send a summary of the review to the other competent authority[27].

IV- ENTRY INTO EFFECT AND TERMINATION

This instrument comes into force from the date of signature [and shall remain in force only during the period the ECA is also in force][28]. The Parties may consult and revise the terms of this instrument [under the same conditions as set forth in the ECA][29].

This instrument may be terminated by either Party at any time. In particular, this instrument should be terminated as soon as one of the competent authorities is no longer in a position to ensure the safeguards provided in this instrument. This competent authority should also inform the other competent authority of this termination. Similarly, this instrument should be terminated as soon as one of the competent authority becomes aware that the other competent authority is no longer in a position to ensure the safeguards provided in this instrument are respected. This competent authority should also inform the other competent authority of this termination. After termination of this instrument, the competent authorities shall continue to maintain as confidential [, consistent with the ECA][30], any information provided under [this instrument][31][the ECA][32]. After termination of this instrument, any Personal Data previously transferred under this instrument will continue to be handled by [Y] according to the safeguards set forth in this instrument.

[27] Considering the requirement for competent authorities to be independent, should this requirement be fulfilled according to the criteria recalled by the CJEU and the ECHR, no external oversight might be required. Nevertheless, should the competent authority of the third country lack the guarantees of independence required in the EU, a reference to the need to have an (external) independent oversight shall be provided.

[28] In case of an administrative arrangement.

[29] In case of an administrative arrangement this reference shall be inserted, while in the context of an International agreement this should be detailed here.

[30] In case of an administrative arrangement. For an international agreement reference to the international agreement itself shall be provided here.

[31] In case of an international agreement.

[32] In case of an administrative arrangement.

V- OTHER

This instrument, including its annexes, shall be drawn up in […] and in […], both/all texts being equally authentic.

*

* *

If necessary to provide a dedicated clause on confidentiality and professional secrecy, depending on the analysis of legal framework in the country of the receiving authority:

IIIa (to be inserted before IV). Confidentiality and professional Secrecy of information received by (Y)

(1) (Y) will treat all information received pursuant to this instrument as confidential by:

(i) treating any information received or requests for assistance pursuant to this Arrangement - which includes that another Authority is considering, has launched, or is engaged in, an enforcement investigation - as confidential, and, where necessary, making additional arrangements to comply with the domestic legal requirements of the sending party;

(ii) ensuring that, where (Y) receives an application from a third party (such as an individual, judicial body or other law enforcement agency) for the disclosure of confidential information received from (X) pursuant to this Arrangement, (Y) should:
   a. maintain the confidentiality of any such information;
   b. notify (X) that supplied the information forthwith
   c. obtain (X)'s consent for the disclosure of the information in question;
   d. inform (X), if there are domestic laws that nevertheless oblige the disclosure of the information.

(iii) upon withdrawal from this Arrangement, maintaining the confidentiality of any confidential information shared with it by (X) pursuant to this Arrangement, return, and delete the information.

(iv) ensuring that all appropriate technical and organizational measures are taken so that any information provided to it under this Arrangement is kept secure. This includes returning or handling the information, in accordance with the consent of (X).

(2) (X) may ask that the information provided under this Arrangement will be used or disclosed only according to specific conditions which (X) will have specified. When (Y) intends to use this possibility, it shall inform (X) and if (X) accepts these conditions, it shall respect them. Otherwise, (X) might refuse to answer the request.

(3) The member or members and the staff of (Y) shall be subject to a duty of professional secrecy or obligation of confidentiality both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of their national relevant applicable legal framework.

*

* *

Annexes to the instrument

Annex: Description of the processing, purpose, categories of data, recipients.

For instance :

X: [*Identity and contact details of X]*

1. Name: …

Address: …

Contact person's name, position and contact details: …

Signature and date: …

Y: [*Identity and contact details of Y]*

1. Name: …

Address: …

Contact person's name, position and contact details: …

Signature and date: …

Description of the transfer :

Categories of data subjects whose personal data is transferred

……..

Categories of personal data transferred

……..

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

……..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

……..

Nature of the processing

……..

Purpose(s) of the data transfer and further processing

……..

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

……..

Annex I: Description of applicable legislation and relevant technical and organizational security measures

The technical and organisational measures must be described in specific (and not generic) terms. It is also necessary to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by X and Y to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

Annex II: List of entities with whom [Y] is permitted to onward share confidential information

Annex III: Description of Applicable Legal Framework on Redress