The transfer of personal data to third countries and international organisations by EU institutions and bodies

Position paper

Brussels, 14 July 2014

Executive summary

This paper provides guidance to EU institutions and bodies on how to interpret and apply the rules laid down in Regulation (EC) No 45/2001 in the context of international transfers of personal data.

EU institutions and bodies increasingly need to transfer personal data to third countries or international organisations for different reasons, including cross-border cooperation and the use of transnational services.

The "principle of adequate protection" (Article 9.1 and 9.2) has to be respected when transferring data internationally. This principle requires that the fundamental right to data protection is guaranteed even when personal information is transferred outside the EU or to bodies not subject to EU law. Controllers should analyse the level of protection provided by the recipient of the data - adequacy should be determined by the nature of the data protection rules applicable at the destination, and the means for ensuring their effective application (supervision and enforcement).

In cases where the European Commission has adopted an "Adequacy Decision" (Article 9.5), it is not necessary to further analyse the need for adequacy. Transfers are also allowed when the controller develops specific mechanisms that provide for appropriate safeguards (Article 9.7). Finally, transfers without special safeguards are allowed in exceptional circumstances, provided that a specific derogation is applicable (Article 9.6).

Where EU institutions or bodies are required by EU legislation or bilateral agreements to conduct international transfers, acting as controllers, and the country of destination has not been declared adequate by the Commission, the instrument should ideally provide for the appropriate measures necessary to ensure compliance with Article 9 of the Regulation. To this end, the EDPS should be consulted in accordance with Article 28.2 of the Regulation before this kind of legal instrument is adopted.

The EDPS might intervene in a supervisory role, depending on how the transfers are conducted, particularly if there has been no EDPS consultation or prior authorisation, in cases where this could have been expected. We may also conduct inspections or use our enforcement powers, as appropriate.

Contents

The transfer of personal data to third countries and international organisations by EU institutions and bodies

1. Introduction

In the course of their tasks, EU institutions and bodies increasingly need to transfer personal data to third countries[1] or international organisations, for reasons such as cross-border cooperation[2] and the use of transnational services.[3] The rapid development of technology, including cloud computing and mobile applications[4], creates new challenges, which have to be addressed to ensure that the fundamental rights of individuals are fully respected. Article 9 of Regulation (EC) No 45/2001 (hereinafter "the Regulation") sets out the rules for these types of transfers, in the light of Articles 25 and 26 of Directive 95/46/EC (hereinafter "the Directive").

This paper aims to provide technical and practical guidance to the controllers of EU institutions and bodies on how to interpret and apply these transfer rules.

The existing EU data protection legal framework, including the Directive, is currently under revision. In the proposal submitted by the European Commission, the rules on international transfers have been considerably developed. Chapter V of the proposal can be seen as a positive contribution towards more global data protection[5] as it not only develops the principle of "adequate protection"[6], but also introduces greater flexibility in providing adequate safeguards for data transfers[7]. This opens up broader possibilities for the use of specific solutions (e.g. Binding Corporate Rules) allowing meaningful progress towards more practical ways of guaranteeing protection to individuals.

The current regime laid down by the Regulation is not yet directly affected by the revision of the data protection legal framework, although the EDPS has proposed that at least it should be amended to enter into force at the same time[8]. The Regulation will

[1] Countries that are not members of the European Economic Area (EEA)

[2] See EDPS Prior checking Opinions: Fraud investigations at the EIB (2009-0459), Transmission of BFT inspection reports (2011-0615), Commission Asset freezing (2010-0426), OLAF internal and external investigations (2005-418, 2007-47, 2007-48, 2007-49, 2007-50, 2007-72), FRONTEX Joint Return Operations (2009-0281), available at: https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/priorchecking/OpinionsPC .

[3] See: Consultation on Transfer of personal data to American Express Corporate Travel SA (AMEX) - EFSA (2009-390), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Consultations/2010/10-12-21_EFSA_AMEX_EN.pdf , Consultation on EIB staff data transfers to OECD (2013-0089), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Consultations/2013/13-03-21_Consultation_EIB_FR.pdf

[4] Specific guidance on cloud computing and mobile devices is currently in preparation.

[5] For detailed EDPS comments, see: Opinion of the European Data Protection Supervisor of 7 March 2012 on the data protection reform package (henceforth EDPS Opinion on the reform package), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf)

[6] See Articles 40 and 41 of the proposal

[7] See Articles 42 and 43 of the proposal.

[8] EDPS Opinion on the reform package (see footnote 5)

therefore continue to provide the rules on international transfers over the next few years. However, this paper will consider proposed developments, where appropriate.

For example, the principle of accountability, which is implicit in the existing rules, will very likely be reinforced in the new data protection framework. In the light of this, we already apply this principle in advising on the obligations of institutions and bodies, in accordance with our policy on consultations in the field of supervision and enforcement.[9]

As a result, when an EU institution or body transfers personal data under Article 9 of the Regulation, it should ensure that it fully respects its obligations under the Regulation before the transfer or set of transfers takes place. In such cases, controllers should consult their DPOs from the outset and obtain their advice. In the meantime, the EDPS has developed advice on how to interpret and apply the existing rules,[10] which has been given to controllers in a number of practical cases. This paper builds on this experience so as to provide practical tools for controllers to assess the best solution.

2. General overview

As further discussed below, Article 9 of the Regulation lays down the general "principle of adequate protection". This is the main principle applying to international data streams and is also enshrined in Articles 25 and 26 of the Directive. Article 9 also outlines how the level of protection afforded by a third country or international organisation should be assessed, which obligations are imposed on the controller to inform the Commission and/or the EDPS, and which derogations apply to the general principle.[11]

The principle of adequate protection requires that the fundamental right to data protection is guaranteed even when personal data are transferred to a party outside the scope of the Regulation and the Directive. Although there is a growing consistency and convergence of data protection principles and practices around the world, full adequacy cannot be assumed in all cases. In many cases, the level of data protection offered by third countries and international organisations is much lower than that of the European Union, or does not exist at all. For this reason, before a transfer to a third country or international organisation takes place, the controller should ensure that data subjects are adequately protected.

Article 9.1 allows personal data exchanges with third countries and international organisations when an adequate level of protection is guaranteed. Transfers are also allowed when the controller develops specific mechanisms that provide for appropriate safeguards (Article 9.7). Finally, transfers without special safeguards are

[9] Policy on Consultations in the field of Supervision and Enforcement, 23 November 2012, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/12-11-23_Policy_on_Consultations_EN.pdf

[10] See the list of consultations submitted to the EDPS in Annex 3.

[11] See full text of Article 9 in Annex 1.

allowed in exceptional circumstances, provided that a specific derogation is applicable (Article 9.6).[12]

3. Preliminary issues

3.1. Notion of "transfer of personal data"

The term "transfer of personal data" has not been defined, neither in the Directive nor in the Regulation. In the latter, the term has also been used in other provisions dealing with data flows within or between EU institutions or bodies and to recipients in the EU which are also subject to the Directive[13]. Under these circumstances, it can be assumed as a starting point, that the term is used in its natural meaning, i.e. that data "move" or are allowed to "move" between different users. However, in reality this issue is not always so straight forward.

The EDPS has called for a definition of this notion in the data protection reform[14], as it has proved to be a problematic issue in certain cases, which so far have been left for the Court of Justice or for the legislator to resolve.

The only case-law of the Court of Justice that has discussed the notion of "transfer", the Lindqvist case[15], has a limited scope. It analyses, among other things, whether the *mere fact* of uploading personal data onto an Internet page which is stored by a hosting provider who is established in the same State (as Ms Lindqvist) or in another Member State is a transfer in terms of Article 25 of the Directive. The Court concluded that "*71. (...) there is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country".*

This conclusion of the Court has to be put in the context of the case. The Court made its evaluation taking into account the *"circumstances such as those in the case in the main proceedings".* The Court did not express itself on other types of processing activities - different, for instance, in terms of their scale, their intention, their target, their risks, etc. - than the one of uploading personal data onto an Internet page in the circumstances of the case, which was otherwise intended to be very local in nature (Ms Lindqvist wishing to inform her fellow parishioners). The conclusion of the Court on the notion of "transfer" should therefore not simply and automatically be applied to cases with different characteristics.

There are obviously also cases, where personal data is communicated to a recipient in a third country with the *intention* to make this information available to that recipient. By the same token, there might be cases, where the publication of personal data on the internet is made with the *objective* of informing the public in general, not only locally

[12] See a short checklist in Annex 2.
[13] See Articles 7 and 8 of the Regulation.
[14] EDPS Opinion on the reform package (footnote 5), page 18, point 108.
[15] Case C-101/01, *Lindqvist* [2003] ECR I-12971.

or within the EU, but also in third countries, such as the case of the Commission staff directory which is available on line. These cases may be treated in different ways, as we will see,[16] but they have in common that certain information is *deliberately* made available to recipients in a third country and they both go beyond the mere uploading of that information for more limited purposes.

Against this background and although there is not yet a formal definition of "transfer of personal data", controllers should consider that this term would normally imply the following elements: *communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient(s) will have access to it*.[17]

The term would therefore cover both "deliberate transfers" and "permitted access" to data by recipient(s).[18] The conditions of "knowledge" and "intention" would exclude cases of access through illegal actions (e.g. hacking). On the other hand, the mere fact that information might or will cross international borders to its destination due to the way in which networks are structured would not automatically trigger the concept.

International transfers of personal data can thus take place in different environments (physical and digital), for example:

- sending of personal data by an EU institution or body (data controller) to a non-EU recipient by post or e-mail;

- "push" of data from an EU data controller's data base to a non-EU recipient;

- granting access of an EU data controller's data base ("pull") to a non-EU recipient;

- direct on-line collection of individual's data in the EU by a non-EU processor acting on behalf of an EU data controller;

- publication of personal data on the internet by an EU data controller.

The term "transfer" would thus, in any case, also include certain processing activities mentioned in Article 2(b) of the Regulation, such as "disclosure by transmission" and "dissemination or otherwise making available". This means that "transfer of personal data" should not only comply with Article 9, but also with other relevant provisions of the Regulation, such as the provisions on data quality and lawful processing (see also point 3.3 below).

[16] See below from point 6 onwards.

[17] These elements would not only apply to transfers to third countries and international organisations (Article 9), but also to transfers within or between Community institutions or bodies (Article 7), and transfers to recipients subject to the Directive (Article 8).

[18] Push and pull systems: these are two different methods of Internet-based communication. In the "push" system, the communication is initiated by the publisher or central server (data controller). This could be seen as a "deliberate transfer" of personal data. In the "pull" system, the request for the transmission of information is initiated by the recipient. This could be seen as "permitted access" to personal data.

Considering the state of discussions regarding this concept and the impact on concrete cases, controllers are advised to consult the EDPS in case of serious doubt.

3.2. Scope of Article 9

Article 9 applies to transfers of personal data to recipients (other than EU institutions and bodies), which are not subject to the Directive. As such, it does not cover recipients established in European Economic Area (EEA) countries[19] unless the transfers occur in fields excluded by the Directive (former second and third pillar of EU law. See point 7 below).

The Regulation contains - as already briefly mentioned - two other provisions related to transfers: Articles 7 and 8. Both provisions do not have parallel rules in the Directive. Article 7 is applicable to transfer of personal data within or between EU institutions. This would be the case of a transfer, for instance, between two Directorates General of the Commission, both located in Brussels. It would also be the case of a transfer between the European External Action Service and any of the EU delegations around the world (even if these delegations are established in third countries, they are part of EU institutions and therefore subject to the Regulation). Article 8 is applicable to transfers to recipients, other than EU institutions and bodies, subject to Directive 95/46/EC.

It has to be noted that after the adoption of the Lisbon Treaty the reference to community institutions and bodies in the Regulation has to be read as a reference to an EU institution or body (for instance in Article 3). This is not the case for those institutions or bodies that are currently subject to a specific data protection legal regime, as in the case of Europol and Eurojust (see below point 7).

3.3. Respect for other legal conditions

Transfers of data are considered as processing activities, and must therefore be lawful, as specified in Chapter II of the Regulation.

Article 5 stipulates the different grounds under which personal data may be processed. This implies that before a transfer may take place, the controller should determine whether one of the specified legal bases is applicable. This relies on two separate steps: (a) the processing activity prior to the transfer must be lawful (collection, storage, etc.); and (b) the transfer itself must also be lawful (it must have a proper legal basis and be consistent with the original purpose of the processing).

Controllers should also comply with the data quality principle (Article 4). This includes requirements relating to purpose limitation, data minimisation, time limits for conservation of data, and accuracy of the data transferred.

Other relevant provisions of the Regulation should also be respected, such as:

[19] EEA countries are the EU Member States plus Iceland, Liechtenstein and Norway.

- the general prohibition on processing special categories of data, except where a derogation applies;
- the obligation to inform the data subject about the recipients;
- compliance with the rights of the data subject at all stages of the transfer process, including the rights of access, rectification and erasure before the transfer takes place;
- the security of the processing (assessing the level of risk associated with the transfer, and adopting appropriate security and organisational measures);
- the question of whether a prior check is required (see point 8 below).

3.4. Monitoring of transfers as best practice

On a general level, and as best practice, EU institutions and bodies should create an internal monitoring and registration system of Article 9 transfers.[20] This should not only include transfers based on adequacy but also – and more importantly - transfers based on derogations (Article 9.6 and 9.7. See below point 6). This will be helpful in supporting internal management of international transfers and in ensuring effective accountability and compliance with the Regulation.

4. Adequate protection

4.1. Applicability

Article 9.1 of the Regulation stipulates that *"[p]ersonal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out"*. [21]

This general principle indicates that personal data cannot be transferred from an EU institution or body to a third country or international organisation[22], unless an adequate level of protection can be ensured. The rule also adds that the transfer should take place *"solely to allow tasks covered by the competence of the controller"*. This is a more restrictive approach than in the Directive, based on the specific nature of the public institutions and bodies covered by the Regulation, who are not permitted to act beyond their competences.

[20] Some institutions or bodies might be advised to keep a central register of transfers. For instance, given the sensitivity of the data and purpose of processing, the EDPS has advised OLAF to keep a central register of transfers (Working Document *OLAF Operations: International Transfers of Personal Data*, 13 February 2006).

[21] See also Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJEU L 350/60, 30.12.2008), Article 13.1(d).

[22] Articles 25 and 26 of the Directive do not mention transfers to international organisations, only transfers to third countries.

By way of derogation, if an adequate level of data protection does not exist in the recipient's country, such transfers can occur only if adequate safeguards are adopted by the controller (see further point 6.2), or if one of the exceptions foreseen in Article 9(6) applies (see further point 6.1).

4.2. Notion of "adequacy"

Article 9 does not define "adequacy" or "adequate level of protection". However Article 9.2 provides some elements that should be taken into account when assessing "adequacy". It specifies that the level of protection afforded by a third country or international organisation shall be assessed in the light of *"all circumstances surrounding a data transfer operation or set of data transfer operations"*. It also requires that: *"(...) particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the rules of law, both general and sectoral, in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation"*. This list is not exhaustive; other elements could also be relevant depending on the actual case.

The assessment of adequacy therefore requires an evaluation or "risk assessment" of the intended processing activity itself (e.g. nature of the data, purpose and duration of the processing operation/s), and of the legal regime or measures applicable to the recipient (e.g. general and sectoral rules of law, professional requirements and security measures).[23] "Adequacy" is a functional concept, so any adequacy assessment must take into account the rules applicable in the target destination, and the means for ensuring their effective application. These principles represent the "core" of data protection, and have been described by the Article 29 Data Protection Working Party as follows[24]:

"1) **the purpose limitation principle** - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive (*analogous to Article 20 of the Regulation*).

2) **the data quality and proportionality principle** - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not

[23] Determining these risks will be particularly relevant in cases where no general adequacy decision has been adopted, and where it is the data controller who conducts the adequacy assessment or adduces adequate safeguards. The higher the risk, the stricter the requirement for protection analysis.

[24] See: Article 29 Working Party, "Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", adopted on 24 July 1998, available at: http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf.
The Article 29 Data Protection Working Party has played an active role in the identification of the elements to be evaluated in the recipient's legal regime. This document has been the basis for all the adequacy decisions adopted by the European Commission as well as for instruments providing for "adequate safeguards" in the absence of adequacy, such as the Standard Contractual Clauses (SCC) and the Binding Corporate Rules (BCR).

excessive in relation to the purposes for which they are transferred or further processed.

3) **the transparency principle -** individuals should be provided with information as to the purpose of the processing and the identity of the controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11.2 and 13 of the directive (*analogous to Article 12.2 and 20 of the Regulation, respectively*).

4) **the security principle -** technical and organisational security measures should be taken by the controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the controller, including a processor, must not process data except on instructions from the controller.

5) **the rights of access, rectification and opposition -** the data subject should have a right to obtain a copy[25] of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive (*analogous to Article 20 of the Regulation*).

6) restrictions on onward transfers - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive (*analogous to Article 9.6 of the Regulation*)."

Furthermore, procedural and enforcement mechanisms must be guaranteed. In this sense, the objectives of a data protection system or a well developed privacy policy are essentially threefold:

"1) to deliver a **good level of compliance** with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

2) to provide **support and help to individual data subjects** in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

3) to provide **appropriate redress** to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication

[25] According to Article 13 of the Regulation, the right of access *may* imply the right to obtain a copy of the data (this footnote is not part of WP12).

or arbitration which allows compensation to be paid and sanctions imposed where appropriate."

To sum up, an adequate system recognises these principles both in substance and in practical implementation, including enforcement where necessary. This can be guaranteed not only by the existence of legal rules and procedures, including judicial or data protection authorities, with remedial powers to re-establish compliance in the interest of the data subjects, but also by other "measures" that create a safer data protection environment, such as codes of conduct, internal rules, security controls and audit mechanisms, provided that all essential elements mentioned above are covered.

5. Assessment of adequacy

The assessment of the level of protection in a certain country or sector may be carried out at different levels and with different legal effects, whether by controllers themselves, data protection authorities or the European Commission. In the latter case, this leads to decisions on adequacy or inadequacy that are binding on the Member States (MS) and the EU institutions and bodies (see Articles 25.4 and 25.6 of the Directive).

In the absence of a binding decision, the Directive allows for different solutions: a majority of MS are subject to a centralised assessment by a data protection authority, while other MS expect data controllers to make at least a first evaluation, as also provided for in Article 9 of the Regulation. The EU institution or body, in its role as controller, is therefore accountable and must assess adequacy before conducting a data transfer. This will be further discussed below.

5.1. Adequacy Decision adopted by the European Commission

Article 9.5 of the Regulation states that: *"The Community institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article 25(4) and (6) of Directive 95/46/EC, that a third country or an international organisation ensures or does not ensure an adequate level of protection"*.

According to Article 25.6 of the Directive: *"The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, (...)"*. An Adequacy Decision adopted in the light of Article 25.6 is binding on all Member States, resulting in a "free flow of data" to the third country in question. These types of decisions also apply to EU institutions and bodies.

The European Commission has already adopted a number of adequacy decisions, so data controllers who need to transfer data to a third country should first check the list of adequate countries[26].

[26] The list of adequate countries (or sectors within a third country, as the case of the US Safe Harbour) is available in the following website:
http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm .

At the time of adoption of this paper, these countries are: Andorra, Argentina, Canada (private sector), Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, US Safe Harbor (certain activities within the private sector) and Uruguay.

The scope of adequacy decisions can vary. Some cover the data protection regime of a country (e.g. Argentina or Switzerland), whilst others only cover certain categories of processing of personal data (e.g. US Safe Harbor, Canada). This should be taken into account before a transfer is made.

To sum up, if the level of protection in the receiving destination is "adequate", there is a free flow of personal data and the controller does not need to take additional measures in relation to the data transfer, providing that all other aspects of the Regulation are respected.

5.2. Adequacy assessed by the controller

Where there is no Commission decision on adequacy, the controller should in principle conduct a specific adequacy assessment of the data protection system (legal rules and other measures), taking into account all the circumstances of the case. The analysis should focus on the specific characteristics (guarantees and/or risks) of the transfer or set of transfers in question. This will include the types of data, purposes and duration of the proposed processing operation, and the recipients in the country or international organisation of destination.

As noted above, the adequacy assessment also requires that both the substance and actual practice should be taken into account (objective and functional approach). This means that some verification of the implemented measures has to be conducted, before it is possible to determine whether an adequate level of protection is effectively ensured. This is the controller's responsibility. However, in practice, it will not always be feasible for the controller to conduct a complete assessment of adequacy for a third country or international organisation. In such cases, the controller should assume that the level of adequacy is inadequate and consider other options discussed below.

In any case, these specific adequacy assessments should be clearly differentiated from the adequacy decisions adopted by the Commission. This is because the former do not affect any future assessment by the Commission of the third country or international organisation's data protection framework or adequacy. Furthermore, they do not apply across the board.

In the light of the accountability principle, the data controller should where relevant thoroughly document the steps taken to ensure adequacy, and to conduct a suitable risk assessment.[27]

5.3. Role of the EDPS in assessing adequacy

[27] Where the third country government or competent authority has provided explanations and/or assurances as to how their (hard or soft) law is to be interpreted and implemented, this can have a decisive influence on the adequacy assessment. However, the assessment has to state that it is based on these explanations and assurances, and is therefore conditional upon them being respected.

- Adequacy Decision adopted by the European Commission

No specific procedure has to be followed by data controllers when the Commission has made a declaration of adequacy under Article 25.4 of the Directive, and the EDPS does not need to be informed. However, in the framework of our monitoring and supervisory duties and in accordance with Article 9.5, we might decide to request information from data controllers on a case-by-case basis.

- Adequacy assessed by the data controller

Any analysis conducted by the controller should be clearly documented, and made available to the EDPS upon request.

In the light of the policy on consultations in the field of supervision and enforcement, the DPO of the EU institution or body should always be consulted and involved in the analysis. Furthermore, data controllers are encouraged to submit a consultation to the EDPS when the matter presents: (a) a certain novelty or complexity (where the DPO or the institution has a genuine doubt), or (b) a clear impact on data subjects' rights (either due to the processing activities' risks etc.)[28].

6. Derogations

In certain cases, even if the receiving country or international organisation does not present an adequate level of protection, transfers can take place if one or more of the situations provided for in Article 9.6 and/or 9.7 of the Regulation apply.

The first type of derogation is mentioned in Article 9.6, and involves a restrictive list of specific situations. In this case, in principle, no other measures are required when one of the listed situations applies (see below point 6.1).

The second type of derogation is mentioned in Article 9.7, and relates to transfers to a destination that does not ensure an adequate level of protection. Such transfers may only take place where the controller adduces adequate safeguards (see below point 6.2).

6.1. Specific derogations (exceptions to adequacy requirement)

Article 9.6 outlines different situations in which a transfer to a destination that is not adequate could take place. These situations should be interpreted and applied restrictively.

It should be noted that the use of *exceptions* does not ensure, *per se*, that the rights of the data subject will be protected in the recipient country or international organisation. As such, it is recommended that controllers *"favour solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental*

[28] Footnote 9 supra.

rights and safeguards to which they are entitled as regards processing of their data in the EU once this data has been transferred".[29]

In particular, transfers of personal data which might be qualified as *"repeated, mass or structural"*[30] should be carried out within a specific legal framework rather than via the exceptions. The exceptions should only be used, in principle, for occasional transfers.

In any event, use of the exceptions should never lead to a situation where fundamental data subject rights might be breached. For this reason, in those limited cases where the use of exceptions is legitimate, the controller should take precautions to ensure the recipient respects certain data protection principles. These guarantees could take different forms (Memorandum of Understanding, exchange of letters, etc.). The content of the guarantees will also depend on the circumstances of the transfer, such as the different levels of risk.

There are however situations in which the use of other solutions (such as the adoption of Adequacy Decisions or adequate safeguards) is inappropriate or impossible, and therefore the data controller has to use the exceptions foreseen in Article 9.6 of the Regulation. The specific derogations mentioned in this provision are clearly designed as alternative options and can be presented as follows:

(a) "the data subject has given his or her consent unambiguously to the proposed transfer"

> This basis, along with Article 5(d) of the Regulation, is normally of limited use for EU institutions and bodies. This is because they should have specific legal mandates to process personal data, which should only be transferred to allow tasks for which the controller is competent. Therefore, considering the definition of "data subject's consent" laid down in Article 2(h) of the Regulation, "freely given, specific and informed indication of his or her wishes" would only be given in exceptional circumstances. Furthermore, in the field of employment, the "freely given"[31] consent has to be safeguarded based on strict criteria. However, this does not completely exclude its use. For instance, the data subject himself could ask the EU institution or body to make a transfer (e.g. transfer of evaluation reports to a future employer located outside the EU). "Specific" consent implies that the consent cannot cover several processing purposes at the same time. The data subject also has to be informed about the details of the transfer in compliance with Article 11 of the Regulation, and of any potential risks.

(b) "the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request"

---

[29] Article 29 Data Protection Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995", page 8.
[30] Opinion of the EDPS on the data protection reform package, adopted on 7 March 2012.
[31] Article 29 Data Protection Working Party Opinion 8/2001 of 13 September 2001 on the processing of personal data in the employment context.

The EU institutions and bodies (controllers) may sign contracts in different fields such as research projects, traineeships, translation, technical assistance, consultancy, conference and publicity services. This may involve contracts with natural persons. Transfers to a third country or international organisation may be required in those cases for the performance of the contract with the data subject. For instance, in the case of a contract with a researcher, a transfer might take place, in the case of a mission abroad, where the EU institution or body needs to send personal information to a research partner established in a third country. Another example might be the payment of funds to a person at a foreign bank account. Similar transfers are allowed at a pre-contractual stage, provided that they are necessary for the implementation of measures taken at the request of the data subject.

(c) "the transfer is necessary for the conclusion or performance of a contract entered into in the interest of the data subject between the controller and a third party"

This might be the case, for instance, in data transfers under *ad hoc* insurance transportation contracts with private companies which are established in a third country. In this case, the data subject is not a party to the contract, but it has to be signed in his or her interest (e.g. an official who goes on mission).

(d) "the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims"

The "important public interest ground" should correspond to a policy interest or legal obligation of the *sender* (EU institution or body) and not just the recipient. When there is no specific legal obligation, the public interest ground has to be "important" and the transfer "necessary" for this derogation to apply. This should be determined on a case-by-case basis. This situation would apply, for instance, when an EU body such as OLAF is conducting a fraud investigation and needs to transfer personal data (such as evidence) to a third country. Considering the sensitivity of the data, the use of this exception in such cases would be limited, in principle, to exceptional or occasional transfers. If the transfers could be qualified as "repeated, mass or structural", (even if related to a single investigation or case), a more systemic and protective solution would be required to avoid disproportionate risks to the fundamental rights and freedoms of the data subject. As such, it would be advisable to base the transfers on Article 9.7 "adequate safeguards" (see below point 6.2).

The EDPS received a consultation from OLAF on a set of Standard Clauses (SC) to be used for Administrative Cooperation Agreements (ACAs) with third country authorities or international organisations. These SC are based on the Standard Contractual Clauses adopted by the Commission (see below point 6.2). The EDPS concluded that these SC should in principle also be used for transfers covered by the exceptions of Article 9(6) where there are specific risks for the data subjects. For example, this could be due to the nature of the data involved (e.g. sensitive), the purpose of the processing (e.g. investigations

which could result in criminal prosecution) or the legal framework in the country of destination (e.g. absence or low level of data protection rules).

The European Aviation Safety Agency (EASA) performs some activities (especially in the field of certification) that result in the payment of fees and charges by applicants. Aspects of these activities may be conducted fully or partly outside the territory of the Member States. The payment invoiced to the applicant also includes the experts' travel costs. The applicants ask EASA to make available the names of the experts and the date of travel in order to relate the expenses to each individual. The EDPS advised that since the performance of these services is one of the core activities of EASA, the data transfers could be considered necessary for the functioning of this body, and therefore qualify for a derogation under Article 9.6(d). However, where an exception is applied, no safeguards are necessarily ensured. For this reason, the EDPS recommended the inclusion of a clause specifying that the recipient (a) is legally authorised to request this data, and (b) will limit the use of the data for the sole purposes motivating the transfer. [32]

The establishment, exercise or defence of legal claims is another possible base for derogation. This might apply, for instance, when a judicial procedure takes place in a third country and evidence containing personal data is requested from an EU institution or body. The controller has to be able to demonstrate the necessity of the transfer.

(e)"the transfer is necessary in order to protect the vital interests of the data subject"

This derogation would be applicable, for instance, if a staff member suffers an accident during a mission, and a third country hospital asks the EU institution's medical service to provide certain medical data necessary to take care of him/her. The controller has to be able to demonstrate the necessity of the transfer.

The European Parliament (EP) runs a database, the Security Support System, which provides support to external missions in case of medical emergencies. This may involve a possible transfer to third country health services. The personal data processed includes, among other things, medical information (in case of an emergency if the participant is found unconscious, e.g. medication needed, allergy information, blood group). The EDPS found that this processing activity would fall under Article 9.6(e) (as well as under Article 9.6(a) taking into account that the information is provided by the data subject on a voluntary basis).[33]

[32] See for instance the EDPS Letter of 4 October 2010 to Data Protection Officer of the European Aviation Safety Agency concerning international transfers, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2010/10-10-04_Letter_DPO_EASA_EN.pdf

[33] See: EDPS Prior Check Opinion adopted on 29 September 2009 (Case 2009-0225) on the European Parliament's "Security Support System".

(f) "the transfer is made from a register which, according to Community law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest(...)".

> This would apply, for instance, to a request for access to a public register managed by an EU institution or body, submitted by a citizen of the EU, from outside the EU.[34] However, this would more generally also be the case of the publication on the internet of certain personal data for consultation by the public, such as the Commission directory. In that case, the focus of analysis should therefore not be on the notion of "transfer", but on the question whether the publication of personal data is legitimate and proportionate.

6.2. Adequate safeguards

As noted above, there are cases where there is no adequate level of protection in the country or international organisation of destination, or where it is at least doubtful. In some of these cases, derogations may not be applicable. In these situations, the data controller should introduce safeguards to ensure the protection of personal data, in accordance with Article 9.7 of the Regulation.

The concept of "adequate safeguards" is defined neither in the Directive, nor in the Regulation. "Adequate safeguards" should therefore be understood as data protection guarantees which are created for the specific situation, and which do not already exist in the recipient's legal system. Typical examples of adequate safeguards are the Standard Contractual Clauses (SCC)[35] adopted by the Commission, or Binding Corporate Rules (BCR)[36]. The purpose of these instruments is to create the protection that is lacking in the data's destination.

6.2.1. Content of the adequate safeguards

Although Article 9.7 does not specify what would classify safeguards as "adequate", the adequacy elements described under point 4.2 above should be carefully considered. Any instrument created to serve as an "adequate safeguard" should clearly include a description of the data protection principles that have to be respected by the

[34] Article 2.1 of Regulation (EC) n. 1049/2001 reads: "Any citizen of the Union, and any natural and legal person residing or having its registered office in a Member State, has a right of access to documents of the institutions, subject to the principles, conditions and limits defined in this Regulation".

[35] Commission Decision 2001/497/EC and 2004/915/EC (controller to controller), and Commission Decision 2002/16/EC (controller to processor). Decision 2004/915/EC is a revised version of Decision 2001/497/EC. The latest one has been submitted by a coalition of business associations, and it presents some differences from the first. For instance, it includes more flexible auditing requirements and more detailed rules on the right of access. (See also Preamble of Decision 2004/915/EC).

[36] See Overview on Binding Corporate rules, available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

importer (recipient) as well as the means to ensure the necessary mechanisms to make this protection effective.

Potential supervision and enforcement mechanisms could include the following (some of which are only relevant in the field of private law - see point 6.2.2.):

- a third party beneficiary clause (to enable the data subject to enforce any breach of the importer or exporter's contractual obligations);
- clarification of the exporter and importer's obligations (e.g. requirement to respond to enquiries, provide a copy of the clauses to the data subject, submission to reviewing, auditing, etc.);
- a liability clause (different solutions are foreseen in the SCC adopted by the Commission, depending on whether the contracts are controller/ controller, or controller/ processor);
- obligation of the importer to communicate security breaches to the exporter;
- mediation and jurisdiction details in case a dispute is not amicably resolved;
- details of governing law (the clauses shall be governed by the law of the country where the EU institution or body is established. This type of clause is included to regulate the civil law issues that might arise between the parties in case of enforcement);
- information about cooperation with supervisory authorities;
- power of the data protection authority to block or suspend the transfers.

Furthermore, as with the SCC, a clause describing the details of the transfers or set of transfers has to be included. This should specify the categories of data, purposes, retention period, detailed security measures, mechanisms to provide information, and exercise of data subjects' rights (access, deletion, objection, etc.).

When, depending on the type of transfer or recipient, a contract is not the appropriate instrument[37] (see further below point 6.2.2.), other commitments on supervision and enforcement need to be adopted involving both the controller and the recipient, such as:

- direct verification by authorities (e.g. joint inspections, audits by independent bodies, etc.) or by the controller (e.g. audits);
- the obligation to designate an independent data protection officer;
- independent investigation of complaints (designation of contact points for enquiries);
- dissuasive sanctions, appropriate redress and compliance with Court decisions;
- an accountability clause (obligation to provide evidence of compliance to the EDPS, either upon request or at regular intervals);
- transparency of the safeguards (e.g. publication of the instruments on the internet);
- termination of the agreement, arrangement, etc. in case of breach.

[37] This may particularly be the case for international organisations where privileges and immunities clauses may not allow them to commit to direct verification by authorities, compliance with EU court decisions, etc. The development of "adequate safeguards" will then require more creativity as most instruments so far have been developed for commercial environments.

When the recipient is a public body, it could be asked to adopt internal binding rules to ensure that the commitments are respected.

Furthermore, the measures should include a reference to EDPS powers to prohibit or suspend data flows to third countries or international organisations in order to protect individuals in cases where:

> (a) the law to which the data importer is subject, requires him to derogate from relevant data protection safeguards, beyond the restrictions necessary in a democratic society as provided for in Article 20 of the Regulation, and where those requirements are likely to have a substantial adverse effect on the guarantees provided by the "adequate safeguards",[38] or
> (b) there is convincing evidence or a substantial likelihood that the "adequate safeguards" are not being or will not be complied with, and the continuation of transfer would create an imminent risk of grave harm to the data subjects.

These measures are without prejudice to EDPS powers to enforce compliance with the Regulation as to EU institutions or bodies involved (see point 9).

6.2.2. Form and nature of the instrument(s) reflecting the adequate safeguards

The Regulation does not require the instrument reflecting the safeguards to take any particular format. Depending on the circumstances, the safeguards could be part of a contract, or a binding declaration or decision, for example. The nature of the legal instrument will vary depending on whether the EU institution or body is acting in the field of private or public law.

If the EU institution or body is acting in the field of private law (for instance, outsourcing mission trips management, IT services or training), and the recipient of the data is established in a third country which has not been declared adequate, the EU institution or body could enter into a contract with the recipient which provides for adequate safeguards.[39] One of the Commission's sets of Standard Contractual Clauses ("SCC") could be used. In these cases, reference to the Directive has to be replaced by reference to the Regulation where appropriate.[40]

The SCC were initially drafted for the business sector, so their application by public authorities might be limited. If the EU institution or body is acting in a field of public law (for instance, creating a data exchange system with third countries, or transferring law enforcement/ customs data), a contract is not an appropriate legal instrument, so a

[38] See for instance, LIBE Committee Inquiry on electronic mass surveillance of EU citizens, Public Hearing, Strasbourg, 7 October 2013, Contribution of Peter Hustinx (EDPS), available at: http://www.europarl.europa.eu/document/activities/cont/201310/20131009ATT72609/20131009ATT72609EN.pdf

[39] As well as a contract, other means might also be possible (e.g. the recipient could adopt a privacy policy and make a unilateral declaration creating a self-binding legal obligation, either per se under national law or in effect via the principle of legitimate expectations).

[40] For instance, as to the SCC adopted on 15 June 2001 (Commission Decision 2001/497/EC), notably: reference in Clause 1.a); Appendix 2, reference in the introductory paragraphs, in principle 5, in principle 6, in principle 7 and in principle 9. As to clause 10 "Governing law", it has to be completed with reference to the Member State where the EU institution or body is established.

different mechanism will have to be considered. This should ensure respect for the adequacy principles and also ensure that the safeguards are binding on the recipient and can be effectively enforced.

The first step should be to include the adequate safeguards in the text of the main international agreement, if this creates the mandate for the transfer (see point 8).

In certain cases, due to the nature of the international organisation or law instrument concerned, it may not be possible to adopt "adequate safeguards" in the form of a "binding instrument". In such cases, another type of protective instrument should be considered. For instance, a Memorandum of Understanding could be appropriate under certain exceptional circumstances.

The EDPS has already expressed that "*(...) the possibility of using non-legally binding instruments to provide appropriate safeguards should be clearly justified and limited only to cases where the necessity to rely on this type of non-binding measure has been demonstrated. (...) The necessity to have recourse to non-legally binding safeguards in the public sector should be carefully assessed, in view of the purpose of the processing and the nature of the data. (...)*"[41]. Irrespective of the type of instrument adopted, the measures in place have to be sufficient to ensure the appropriate implementation (and enforcement where necessary) of the safeguards described in point 6.2.1 above.

6.3. Role of the EDPS in dealing with derogations

Article 9.8 of the Regulation states that *"The Community institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where they have applied paragraphs 6 and 7"*. The provision of information will take different forms depending on the nature of the case, as it is explained below.

- Article 9.6 derogations

When an EU institution or body needs to use one of the derogations mentioned in Article 9.6, it is not required to inform the EDPS *ex-ante* (before the transfer is conducted). However, the controller should provide information to the EDPS upon request, in the context of supervision or enforcement activities. In any event, the DPO of the EU institution or body should always be consulted and involved when deciding whether to apply a derogation.

Furthermore, in the light of the policy on consultations in the field of supervision and enforcement, data controllers are encouraged to submit a consultation to the EDPS under certain circumstances already mentioned under point 5.3 (second bullet point) above.

- Article 9.7 derogations

[41] EDPS Opinion on the reform package (see footnote 5).

Again, the DPO of the EU institution or body has to be involved in the analysis process that takes place before adequate measures are adopted.

EDPS ex-ante involvement: there are three scenarios which need to be considered when deciding whether or not to involve the EDPS:

- No need for prior authorisation or consultation:
  Where Standard Contractual Clauses (SCC) are used.

- No need for prior authorisation, but consultation might be necessary: (check the EDPS Policy on consultations in the field of supervision and enforcement). For example, when a specific binding instrument (as opposed to SCC), is developed by the EU institution or body to be used in either private or public law.

- Need for prior authorisation:
  In exceptional cases where the transfers are based on specific safeguards and are not incorporated in a legally binding instrument.[42]

When an instrument containing specific safeguards is submitted for consultation and/or prior authorisation, a thorough description of the "adequacy" analysis should be presented to the EDPS together with relevant documentation and confirmation of the draft instrument(s) /measures that are intended to provide the adequate safeguards.

After receiving the consultation or the request for authorisation, the EDPS will evaluate the factual and legal aspects of the case and issue recommendations where necessary. Where an authorisation is required, we might adopt a decision authorising the transfer or set of transfers when satisfied with the adequacy of the safeguards adduced by the data controller. If we do not find the proposed safeguards fully adequate, we will issue recommendations for compliance with the Regulation. A follow-up phase will then be commenced.

7. Transfers outside the scope of Directive 95/46/EC

The title of Article 9 is "Transfer of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC". These recipients could be established in the EEA countries, but may conduct types of activities that are excluded from the application of the Directive. Indeed, Article 3.2 of the Directive states that "*This Directive shall not apply to the processing of personal data: - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State*

[42] See: EDPS Decision of 13 February 2014 concerning the transfers of personal data carried out by OLAF through the Investigative Data Consultation Platform pursuant to Article 9(7) of Regulation (EC) No 45/2001, available at:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_EN.pdf

in areas of criminal law, (...)". This would be the case, for instance, in transfers made to police or judicial authorities.

Those exclusions were necessary before the adoption of the Lisbon Treaty, but they are now in principle inconsistent with Article 16 thereof[43], as well as with Article 8 of the European Union Charter on Fundamental Rights.

Member states are subject to Convention 108[44], and they have often implemented the Convention beyond the scope of the Directive.[45] The Directive has been applied to the whole legal system, not just to the former first pillar areas. In those cases, it could be considered that an "adequate" (or even "equivalent") level of protection exists in the areas of the former second and third pillar of EU law at national level. Therefore, transfers can take place under Article 9 as long as they respect Article 8 of the Regulation.

As mentioned above, all MS have ratified Council of Europe Convention No. 108. This ratification provides for a presumption of adequacy, which has to be verified in practice with the MS concerned.[46] This will involve checking the concrete measures required of the recipient.[47] For instance, are the police subject to specific data protection obligations, in line with Convention No. 108? Do they have a sufficient level of awareness about their data protection obligations? Are enforcement mechanisms applied when there is a breach? This analysis has to be documented by the controller.

This verification is also recommended because (a) the EU data protection instrument currently applicable to police and judicial authorities (Framework Decision 2008/977) does not cover all the elements relevant for an adequacy evaluation as described in the Article 29 Working Document WP12 nor does it cover purely domestic situations[48];

---

[43] See EDPS Opinion of 14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "A comprehensive approach on personal data protection in the European Union", point 33

[44] The Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) is currently under revision. For more information on the process, see: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

[45] See "Analysis and impact study on the implementation of Directive EC95/46 in Member States" accompanying the "First report on the implementation of the Data Protection Directive (95/46/EC)", COM(2003) 265 FINAL, available at: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf. See also Annex 3 "Data protection in the areas of police and judicial co-operation in criminal matters" of the Impact Assessment accompanying the data protection reform package, SEC(2012) 72 FINAL, Brussels 25.1.2012, p. 36 available at: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf.

[46] Article 9.2 of Convention n. 108 stipulates that it is possible to derogate from certain principles of the instrument when "(...) the derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences".

[47] Convention 108 does not create subjective rights for the data subject *per se*, nor is it directly enforceable by the European Court of Human Rights.

[48] See EDPS Opinion of 14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "A comprehensive approach on personal data protection in the European Union", point 35, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf.

and (b) there is presently no EU data protection legal instrument covering Common Foreign and Security Policy[49].

As to Europol and Eurojust, it has to be noted that they are not subject to the Directive, and have a special data protection regime.[50] For this reason, although they are now EU institutions, an adequacy assessment would be required.

Nevertheless, as it is often the case for MS in the former second and third pillar, there is a presumption of adequacy, because their data protection legal framework is broadly in line with the Directive and the Regulation. In this case, the controller should conduct an adequacy assessment (as mentioned in point 5.2 above) to check effective compliance.

8. EU legislation and bilateral agreements

EU institutions and/or bodies might be required by EU legislation or bilateral agreements to conduct international transfers, acting as controllers.[51] When this is the case, the instrument should ideally include the appropriate framework necessary to ensure compliance with Article 9 of the Regulation.

Before this kind of legal instrument is adopted, the EDPS should be consulted, in accordance with Article 28.2 of the Regulation.

If the country of destination (in the case of a bilateral agreement) has not been declared adequate by the Commission, the instrument has to state whether adequacy exists (as described in point 5.2 above), or whether "adequate safeguards" have been developed (as described in point 6.2 above). In the latter case, the adequate safeguards should be an integral part of the instrument, taking the form of an Annex, for instance. This is an example of a special kind of binding legal instrument, which addresses not only the material substance of the agreement itself, but also the relevant personal data protection aspects.

There are cases where the legislation or bilateral agreement in question is already in force. However, it may not include the appropriate framework for compliance with

---

[49] See EDPS Opinion of 24 November 2010 on the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges, point 31, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-11-24_EU_counter-terrorism_EN.pdf

[50] Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), available at: https://www.europol.europa.eu/sites/default/files/council_decision.pdf Rules of procedure on the processing and protection of personal data at Eurojust (2005/C 68/01), available at: http://eurojust.europa.eu/doclibrary/Eurojust-framework/dataprotection/Eurojust%20Data%20Protection%20Rules/Eurojust-Data-Protection-Rules-2005-02-24-EN.pdf

[51] See for instance the Agreements containing provisions on Mutual Assistance in Customs Matters concluded with third countries (See annex 3).

Article 9, or only a very general provision which (even if it contains some positive elements) is insufficient to conduct a lawful transfer. [52]

In these cases, it is common practice to include a standard clause referring to confidentiality and personal data protection, especially in certain types of bilateral agreements, for instance in the Customs cooperation area. These clauses generally include a statement that personal data may be exchanged only when the recipient undertakes to protect the data in at least an equivalent manner as the exporting party.

"Equivalence" is notably the result of harmonisation, as with national data protection legislation after the transposition of the Directive. Although the principle of "adequacy" does not impose the need for a harmonised regime, it does require respect for the core principles, as described under point 4.2. Moreover, it cannot be assumed that the level of "equivalent" protection (as stated in the Agreement) will be ensured in practice.

As a result, the "equivalence" clause included in these bilateral Agreements does not ensure *per se* compliance with Article 9. In those cases, the controller should adopt complementary measures to ensure compliance with Article 9 before the transfer or set of transfers take place.

9. Supervision and enforcement

As described in the EDPS Policy paper "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001"[53] (hereinafter "the policy paper on compliance"), there are a number of supervision and enforcement tools available to the EDPS, to enable him to carry out his compliance monitoring function. These tools can be used in the scenarios of Article 9, depending on the type of processing activities (in particular the level of risk).

- Supervision tools

- Prior checks

In certain cases, the type of processing operations involved in transfers may fall under the criteria described in Article 27.2 of the Regulation. In such cases, the controller would have to submit a prior checking notification to the EDPS, clearly describing all relevant aspects of the process.

A prior check might be required in these cases, irrespective of whether the recipient has been declared adequate. For instance, if the processing is related to health data

[52] See for instance Article 17 of the Agreement between the European Community and the Republic of India on customs cooperation and mutual administrative assistance in customs matters (OJ L 304/25, 30.09.2004), available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22004A0930(01)&rid=8

[53] Policy paper "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001", adopted on 13.12.2010, available at:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_EN.pdf

which is to be transferred to an adequate country (e.g. Switzerland), the processing still has to be submitted for a prior check.

In other cases, the EDPS might have to deal with both a consultation (as described under point 6.3), and a prior check due to the nature of the underlying processing activity.

A prior check notification may also have to be submitted in light of Article 27(1) of the Regulation, if the processing operations are likely to present specific risks to the rights and freedoms of data subjects. This might apply, for instance, to information processed by cloud computing services, in certain specific situations to be defined in subsequent guidance, due to the complexity and sensitivity of the data.[54] In this environment, clients' data are often transferred to cloud providers' servers and data centres located in various parts of the world. As there is no stable location for the data, the EDPS might have to verify that any adequate safeguards effectively comply with Article 9, and cover all the potential recipients that might be involved in the cloud environment. However, this also depends on the conditions to be agreed with cloud computing service providers more generally. At this stage, there are therefore no additional requirements for prior checking.

- Consultations, complaints handling, inspections

The EDPS has other supervision tools to ensure compliance, such as conducting consultations, as mentioned above. The policy on consultations is fully applicable to Article 9 transfers.

Any data subject affected by the transfers can submit a complaint to the EDPS, as stated in Articles 32 and 33 of the Regulation, if they consider that (their) data protection rights have been breached.

The EDPS might also decide to carry out inspections to check compliance with Article 9 of the Regulation or to collect evidence in the context of complaints.

- Enforcement tools

The enforcement powers of the EDPS are set out in Article 47 of the Regulation and are fully discussed in the policy paper on compliance. EDPS practice is that the most effective action will be chosen based on the results it is intended to achieve. For Article 9 data transfers, the EDPS has the power to:

* refer the matter to the controller in the event of an alleged breach of the Regulation and, where appropriate, propose how the breach can be remedied;

* warn or admonish the controller;

[54] See : Opinion of the European Data Protection Supervisor of 16 November 2012 on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe', available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

* impose a temporary or definitive ban on processing;

* refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;

* refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;

* intervene in actions brought before the Court of Justice of the European Communities.

These powers will be exercised in view of the specific circumstances relating to the recipient's legal system, or to any of their processing practices that might endanger individuals' protection (see point 6.2.1 on the EDPS powers to prohibit or suspend data flows).

ANNEX 1

Article 9 of Regulation (EC) No 45/2001

Transfer of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC

1. Personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out.
2. The adequacy of the level of protection afforded by the third country or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the rules of law, both general and sectoral, in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation.
3. The Community institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider the third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 2.
4. The Commission shall inform the Member States of any cases as referred to in paragraph 3.
5. The Community institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article 25(4) and (6) of Directive 95/46/EC, that a third country or an international organisation ensures or does not ensure an adequate level of protection.
6. By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if:
(a) the data subject has given his or her consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract entered into in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which, according to Community law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in Community law for consultation are fulfilled in the particular case.
7. Without prejudice to paragraph 6, the European Data Protection Supervisor may authorise a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection within the meaning of paragraphs 1 and 2, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
8. The Community institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where they have applied paragraphs 6 and 7.

ANNEX 2

Checklist before carrying out a transfer

Controllers should involve their Data Protection Officers from the outset, and request their advice and guidance for compliance. The following actions and legal checks should be carried out before international transfer(s) take place:

Q. 1) Is an adequate level of protection ensured in the country of the recipient or within the recipient international organisation?

Check the list of Adequacy Decisions adopted by the Commission: Andorra, Argentina, Canada (private sector), Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, US Safe Harbour (certain activities within the private sector) and Uruguay.

A: **Yes** - the transfer can take place as long as the other rules of Regulation 45/2001 are respected.

A: **No or not sure** - go to question 2....

EDPS involvement: no need to inform, consult or request authorisation from the EDPS.

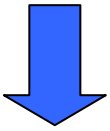
2) Are there other reasons to believe that an adequate level of protection is afforded by the recipient in the third country or international organisation?

The controller must carry out an assessment to verify whether there is an adequate level of protection for the specific transfers in question. This should be limited to the specific purposes and recipients in the country or international organisation of destination.

A: **Yes** - the transfer can take place as long as the adequacy assessment is clearly documented, and the other rules of Regulation 45/2001 are respected.

A: **No** - go to question 3...

EDPS involvement: no need to request authorisation from the EDPS. We might be consulted in certain circumstances (check the EDPS Policy on consultations in the field of supervision and enforcement).



3) Does a derogation apply?

Is the transfer *not* repeated, massive or structural, and does one of the following circumstances apply?

(a) the data subject has given his or her consent to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller; or
(c) the transfer is necessary for the conclusion or performance of a contract entered into in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which is intended to provide information to the public.

A: **Yes** - the transfer can take place as long as it is not repeated, massive or structural. One of the conditions in Article 9.6 of Regulation 45/2001 should also be met, and all the other rules of the Regulation respected.

A: **No** - go to question 4...

EDPS ex-ante involvement: no need to request authorisation from the EDPS. We might be consulted in certain circumstances (check the EDPS Policy on consultations in the field of supervision and enforcement).

4) Can the controller adduce "adequate safeguards"?

"Adequate safeguards" are data protection guarantees that are created *ad hoc*, and that do not already exist in the recipient's legal system or practice at the destination. The purpose of these safeguards is to create protection where it

may be lacking in the country or international organisation of destination of the data, in cases where derogations are not applicable.

A: **Yes** - the transfer can take place as long as the other rules of Regulation 45/ 2001 are respected.

A: **No** - the transfer cannot take place.

EDPS involvement: there are three scenarios which need to be considered when deciding whether or not to involve the EDPS:

- No need for prior authorisation or consultation:
  Where Standard Contractual Clauses (SCC) are used.

- No need for prior authorisation, but consultation might be necessary: (check the EDPS Policy on consultations in the field of supervision and enforcement). For example, when a specific binding instrument (as opposed to SCC), is developed by the EU institution or body to be used in either private or public law scenarios..

- Need for prior authorisation:
  In exceptional cases where the transfers are based on specific safeguards, which are not incorporated in a legally binding instrument.

The EDPS might also decide that authorisation is needed in other cases submitted for consultation, depending on the level of risk of the transfer scheme.

When prior authorisation is requested, a thorough analysis on "adequacy" (and draft instrument(s)) should be presented to the EDPS.

5) Check if the underlying processing activity is subject to prior check, and notify this to the EDPS where appropriate.

ANNEX 3

List of requests for authorisation (Article 9.7), administrative consultations (Article 28.1 and 46(d)), and selected legislative consultations (Article 28.2) submitted to the EDPS in relation to Article 9

-Requests for authorisation (Article 9.7)

- EDPS Decision of 13 February 2014 concerning the transfers of personal data carried out by OLAF through the Investigative Data Consultation Platform pursuant to Article 9(7) of Regulation (EC) No 45/2001, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_EN.pdf ; Annex - Draft Administrative Cooperation Arrangement between the "European Anti-Fraud Office" (OLAF) and [The Partner], available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_Annex_EN.pdf

Administrative consultations (Article 28.1 and 46(d))

- Answer of 16 July 2012 to a consultation on OLAF revised Model Data Protection Contractual Clauses to be used in Administrative Cooperation Agreements (ACAs) concluded with third country authorities or international organisations (Case 2012-0086), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-07-16Model%20Data%20Protection%20Clauses_OLAF_D-1051_EN.pdf

- Answer of 3 April 2012 to a consultation on OLAF revised Model Data Protection Contractual Clauses to be used in Administrative Cooperation Agreements (ACAs) concluded with third country authorities or international organisations (Case 2012-0086), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-04-03%20Model%20Data%20Protection%20Clauses_OLAF_D-746_EN.pdf

- Answer of 4 October 2010 to Data Protection Officer of the European Aviation Safety Agency concerning international transfers, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2010/10-10-04_Letter_DPO_EASA_EN.pdf

- Answer of 21 December 2010 to a consultation regarding transfer of personal data of EFSA external experts by EFSA to American Express Corporate Travel SA (AMEX). (Case 2009-390), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Consultations/2010/10-12-21_EFSA_AMEX_EN.pdf

- Answer of 2 July 2009 to a consultation on transfers of personal data to third countries: 'adequacy' of signatories to Council of Europe Convention 108, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-07-02_OLAF_transfer_third_countries_EN.pdf

- Answer of 6 May 2009 on a consultation on questions concerning the treatment of personal data transfers by OLAF, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-05-06_OLAF_transfers_EN.pdf

Selected legislative consultations (Article 28.2)

- Opinion of 14 March 2014 on the proposal for a Council Decision on the position to be adopted, on behalf of the European Union, in the EU-China Joint Customs Cooperation Committee regarding mutual recognition of the Authorised Economic Operator Programme in the European Union and the Measures on Classified Management of Enterprises Program in the People's Republic of China, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-14_EU-China_Customs_EN.pdf

- Opinion of 20 February 2014 on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf

- Opinion of 9 February 2012 on the Proposal for a Council decision on a Union position within the EU-US Joint Customs Cooperation Committee regarding mutual recognition of the Authorised Economic Operator Programme of the European Union and the Customs-Trade Partnership Against Terrorism Program of the United States, OJ C 160/01, 06.06. 2012, p.1, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-02-09_EU_US_Joint_Customs_EN.pdf

- Opinion of 12 March 2010 on the Proposal for a Council Decision on a Union position within the EU-Japan Joint Customs Cooperation Committee concerning the mutual recognition of Authorised Economic Operator programmes in the European Union and in Japan, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-12_EU-Japan_EN.pdf