18/EN

WP 254 rev.01

Article 29 Working Party

Adequacy Referential

Adopted on 28 November 2017

As last Revised and Adopted on 6 February 2018

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Introduction

The Working Party of EU Data Protection Authorities[1] (the WP29) has previously published a Working Document on transfers of personal data to third countries (WP12)[2]. With the replacement of the Directive by the EU General Data Protection Regulation (GDPR)[3], WP29 is revisiting WP12, its earlier guidance, to update it in the context of the new legislation and recent case law of the European Court of Justice (CJEU)[4].

This working document seeks to update Chapter One of WP12 relating to the central question of adequate level of data protection in a third country, a territory or one or more specified sectors within that third country or in an international organization (hereafter: "third countries or international organizations"). This document will be continuously reviewed and if necessary updated in the coming years, based on the practical experience gained through the application of the GDPR. Chapters 2 (*Applying the approach to countries that have ratified Convention 108*) and 3 (*Applying the approach to industry self-regulation*) of the WP12 document should be updated at a later stage.

This working paper is focused solely on adequacy decisions, which are implementing acts[5] of the European Commission, according to article 45 of the GDPR. Other aspects of transfers of personal data to third countries and international organizations will be examined in following working papers that will be published separately (BCRs, derogations).

This document aims to provide guidance to the European Commission and the WP29 under the GDPR for the assessment of the level of data protection in third countries and international organizations by establishing the core data protection principles that have to be present in a third country legal framework or an international organization in order to ensure essential equivalence with the EU framework. In addition, it may guide third countries and international organizations interested in obtaining adequacy. However, the principles set out in this working document are not addressed directly to data controllers or data processors.

The present document consists of 4 Chapters:

Chapter 1: Some broad information in relation to the concept on adequacy

Chapter 2: Procedural aspects for adequacy findings under the GDPR

Chapter 3: General Data Protection Principles. This chapter includes the core general data protection principles to ensure that the level of data protection in a third country or international organization is essentially equivalent to the one established by the EU legislation.

Chapter 4: Essential guarantees for law enforcement and national security access to limit the interferences to fundamental rights. This Chapter includes the essential guarantees for law enforcement and national security access following the CJEU Schrems judgment in 2015 and based on the Essential Guarantees WP29 working document adopted in 2016.

---

[1]As established under Article 29 of the EU Data Protection Directive 95/46/EC

2 WP12 , 'Working Document: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive' adopted by the Working Part on 24 July 1998.

3 Regulation (EU) 2016/679 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 (General Data Protection Regulation) (Text with EEA relevance)

4 Including Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015

[5] See relevant articles 45(3) and 93(2) of the GDPR for further information on the implementing acts

Chapter 1: Some broad information in relation to the concept of adequacy

Article 45, paragraph (1) of the GDPR sets out the principle that data transfers to a third country or international organization shall only take place if the third country, territory or one or more specified sectors within that third country or the international organization in question, ensures an adequate level of protection.

This concept of "adequate level of protection" which already existed under Directive 95/46, has been further developed by the CJEU. At this point it is important to recall the standard set by the CJEU in Schrems, namely that while the "*level of protection*" in the third country must be "*essentially equivalent*" to that guaranteed in the EU, "*the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]*"[6]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation.

The purpose of adequacy decisions by the European Commission is to formally confirm with binding effects on Member States[7] that the level of data protection in a third country or an international organization is essentially equivalent to the level of data protection in the European Union[8]. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organization, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules.

Article 45, paragraph (2) of the GDPR, establishes the elements that the European Commission shall take into account when assessing the adequacy of the level of protection in a third country or international organization.

For example, the Commission shall take into consideration the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organization has entered into.

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

The 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, which could be seen as a minimum requirement for protection to be adequate, are derived from the EU Charter of Fundamental Rights and the GDPR. In addition, consideration should also be given to other international agreements on data protection, e.g. Convention 108.[9]

Attention must also be paid to the legal framework for the access of public authorities to personal data. Further guidance on this is provided in Working paper 237 (i.e. the Essential Guarantees document)[10] on safeguards in the context of surveillance.

General provisions regarding data protection and privacy in the third country are not sufficient. On the contrary, specific provisions addressing concrete needs for practically relevant aspects of the right to

---

[6] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 73, 74);

[7] Article 288 (2) TFEU

[8] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 52);

9 Recital 105 of the GDPR

[10] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN WP 237, 13 April 2016

data protection must be included in the third country's or international organization's legal framework. These provisions have to be enforceable.

Chapter 2: Procedural aspects for adequacy findings under the GDPR

For the EDPB to fulfil its task in advising the European Commission according to Article 70(1) (s) of the GDPR the EDPB should be provided with relevant documentation, including relevant correspondence and the findings made by the European Commission. Where the legal framework is complex, this should include any report prepared on the data protection level of the third country or international organization. In any case, the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country. The EDPB will provide an opinion on the European Commission's findings in due time and, identify insufficiencies in the adequacy framework, if any. The EDPB will also endeavor to propose alterations or amendments to address possible insufficiencies.

According to Article 45 (4) of the GDPR it is upon the European Commission to monitor – on an ongoing basis - developments that could affect the functioning of an adequacy decision.

Article 45 (3) of the GDPR provides that a periodic review must take place at least every four years. This is, however, a general time frame which must be adjusted to each third country or international organization with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.

Given the mandate to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organization, no longer ensures an adequate level of protection, the EDPB must, in due time, receive meaningful information regarding the monitoring of the relevant developments in that third country or international organization by the EU Commission. Hence, the EDPB should be kept informed of any review process and review mission in the third country or to the international organization. The EDPB would appreciate to be invited to participate in these review processes and missions.

It should also be noted that according to article 45 (5) of the GDPR the European Commission has the right to repeal, amend or suspend existing adequacy decisions. The procedure to repeal, amend or suspend should consequently involve the EDPB by requesting its opinion pursuant art. 70(1) (s).

Furthermore, as now recognized in article 58 (5) of the GDPR and according to the CJEU's Schrems ruling, data protection authorities must be able to engage in legal proceedings if they find a claim by a person against an adequacy decision well founded: *"It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity*"[11].

[11] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§ 65)

Chapter 3: General Data Protection Principles to ensure that the level of protection in a third country, territory or one or more specified sectors within that third country or international organization is essentially equivalent to the one guaranteed by the EU legislation

A third country's or international organisation's system must contain the following basic content and procedural/enforcement data protection principles and mechanisms:

A. Content Principles:

1) Concepts

Basic data protection concepts and/or principles should exist. These do not have to mirror the GDPR terminology but should reflect and be consistent with the concepts enshrined in the European data protection law. By way of example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data".

2) Grounds for lawful and fair processing for legitimate purposes

Data must be processed in a lawful, fair and legitimate manner.

The legitimate bases, under which personal data may be lawfully, fairly and legitimately processed should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interest of the data controller or of a third party which does not override the interests of the individual.

3) The purpose limitation principle

Data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.

4) 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 excessive in relation to the purposes for which they are processed.

5) Data Retention principle

Data should, as a general rule, be kept for no longer than is necessary for the purposes for which the personal data is processed.

6) The security and confidentiality principle

Any entity processing personal data should ensure that the data are processed in a manner that ensures security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The level of the security should take into consideration the state of the art and the related costs.

7) The transparency principle

Each individual should be informed of all the main elements of the processing of his/her personal data in a clear, easily accessible, concise**,** transparent and intelligible form. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to him/her and other information insofar as this is necessary to ensure fairness. Under certain conditions, some exceptions to this right for information can exist, such as for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

8) The right of access, rectification, erasure and objection

The data subject should have the right to obtain confirmation about whether or not data processing concerning him / her is taking place as well as access his/her data, including obtaining a copy of all data relating to him/her that are processed.

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

The data subject should also have the right to object on compelling legitimate grounds relating to his/her particular situation, at any time, to the processing of his/her data under specific conditions established in the third country legal framework. In the GDPR, for example, such conditions include when the processing is necessary for the performance of a task carried out in the public interest or when it is necessary for the exercise of official authority vested in the controller or when the processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party.

The exercise of those rights should not be excessively cumbersome for the data subject. Possible restrictions to these rights could exist for example to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

9) Restrictions on onward transfers

Further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.

B. <u>Examples of additional content principles to be applied to specific types of processing:</u>

1) Special categories of data

Specific safeguards should exist where 'special categories of data are involved[12]. These categories should reflect those enshrined in Article 9 and 10 of the GDPR. This protection should be put in place, through more demanding requirements for the data processing such as for example, that the data subject gives his/her explicit consent for the processing or through additional security measures.

[12] Such special categories are also known as "sensitive data" in recital 10 of the GDPR.

2) Direct marketing

Where data are processed for the purposes of direct marketing, the data subject should be able to object without any charge from having his/her data processed for such purposes at any time.

3) Automated decision making and profiling

Decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. In the European framework, such conditions include, for example, the need to obtain the explicit consent of the data subject or the necessity of such a decision for the conclusion of a contract. If the decision does not comply with such conditions as laid down in the third country legal framework, the data subject should have the right not to be subject to it. The law of the third country should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision where it has been adopted on an incorrect factual basis.

C. <u>Procedural and Enforcement Mechanisms:</u>

Although the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union[13], a system consistent with the European one must be characterized by the existence of the following elements:

1) Competent Independent Supervisory Authority

One or more independent supervisory authorities, tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions in the third country should exist. The supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In that context, the supervisory authority should have all the necessary and available powers and missions to ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able, on its own initiative, to conduct investigations.

2) The data protection system must ensure a good level of compliance

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

3) Accountability

A third country data protection framework should oblige data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority. Such measures may include for example data

[13] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, para. 74.

protection impact assessments, the keeping of records or log files of data processing activities for an appropriate period of time, the designation of a data protection officer or data protection by design and by default.

4) **The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms**

The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to ensure compliance. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling any infringements of the right to data protection and respect for private life to be identified and punished in practice.

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

Chapter 4: Essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights

When assessing the adequacy of the level of protection, under Art 45(2)(a) the Commission is required to take into account "*relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data as well as the implementation of such legislation…*".

The CJEU in Schrems, noted that the "*term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter*". Even though the means to which that third country has recourse, in this connection, may differ from those employed within the European Union, those means must nevertheless prove, in practice, effective[14].

In this context, the court also noted critically that the previous Safe Harbor decision did "*not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives, such as national security.*"

The WP29 has identified in the opinion WP237, adopted on 13 April 2016, essential guarantees reflecting the jurisprudence of the CJEU and the ECHR in the field of surveillance. While the recommendations detailed in WP237 remain valid and should be taken into account when assessing the adequacy of a third country in the field of surveillance, the application of these guarantees may differ in the fields of law enforcement and national security access to data. Still those four guarantees need to be respected for access to data, whether for national security purposes or for law enforcement purposes, by all third countries in order to be considered adequate:

1) **Processing should be based on clear, precise and accessible rules (legal basis)**

2) **Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated**

3) **The processing has to be subject to independent oversight**

4) **Effective remedies need to be available to the individuals**

[14] Case C 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, paragraph 74.