TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS. AN OVERVIEW OF THE EUROPEAN LEGAL REGIME

Lecturer Dana VOLOSEVICI, PhD.
Petroleum-Gas University Ploiesti
dana.volosevici@vplaw.ro

Abstract
The protection of personal data is a strategic issue at European level and state of art legal tools are provided for data transfers and international data protection instruments. The paper aims to be an overview of the European legal regime applicable to the transfers of personal data to third countries or international organisations.
Keywords: *Data protection, European Union, transfer*

The protection of personal data is a strategic issue at European level and is enshrined in Article 8 of the EU Charter of Fundamental Rights. The Regulation 679/2016 [1] applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. As an important number of personal data is transferred outside the EU, from its inception data protection legislation has provided several mechanisms enabling international data transfers aiming to ensure that when the personal data of Europeans are transferred abroad, the legal protection follows with the data.

Thus, any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions laid down the Regulation 679/2016 are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

The aim of the regulation is that to ensure that the level of protection of natural persons guaranteed by the Regulation 679/2016 is not undermined. Hence, data exporter transferring personal data to third countries or international organizations must meet both the conditions stated for the transfer, but alsp of the other provisions of the GDPR. Each processing activity must comply with the relevant data protection provisions, in particular with Articles 5 and 6.

Transfers of personal data to third countries or international organisations may take place in three main cases: (1) where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection (2) in the absence of a decision of the Commission, where a controller or processor has provided appropriate safeguards and (3) if the transfers fall inside the scope of a derogation.

Transfers outside the EU with adequate protection. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation (Art. 45 (1). The Commission "adequacy decision" establishes that a non-EU country provides a level of data protection that is "essentially equivalent" to that in the EU. As is was pointed out by the case law, “in order for the Commission to adopt a decision […], it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order” [2].

The adoption of an adequacy decision involves a number of steps: a proposal from the European Commission; an opinion of the European Data Protection Board; an approval from representatives of EU countries; the adoption of the decision by the European Commission. As confirmed in 2015 by the Court of Justice in the Schrems ruling, the adequacy standard does not require a point-to-point replication of EU rules[3].

The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an

adequate level of protection. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation.

The list of the third countries, territories and specified sectors within a third country and international organisations for which the Commission has decided that an adequate level of protection is or is no longer ensured shall be published in the Official Journal of the European Union.

As per December 1st, 2019, The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.

Appropriate safeguards. Where the Commission has not decide that a certain country ensured an adequate level of protection, the transfer of data to a third country or an international organisation may be performed if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The Regulation 679/2019 provides five types of appropriate safeguards which can be provided without requiring any specific authorisation from a supervisory authority: legally binding and enforceable instrument between public authorities or bodies; binding corporate rules; standard data protection clauses; approved code of conducts; approved certification mechanisms.

Subject to the authorisation from the competent supervisory authority, the appropriate safeguards may also be provided for contractual clauses or provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Legally binding and enforceable instrument between public authorities or bodies. Data exporter may assure the legality of a transfer using a legal instrument between two public authorities or bodies provided that the legal instrument provides ‘appropriate safeguards’ for the rights of the individuals whose personal data is being transferred and it is legally binding and enforceable. The ‘appropriate safeguards’ must include

enforceable rights and effective remedies for the individuals whose personal data is transferred.

Binding corporate rules (BCRs). BCRs are an internal code of conduct operating within a multinational group, which applies to restricted transfers of personal data from the group's EEA entities to non-EEA group entities. The BCRs are to be approved by the competent supervisory authority provided that they meet the conditions set forth in the Article 47 (2). Thus, the BCRs should be legally binding and apply to and be enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees. Data subjects should enjoy expressly provided enforceable rights with regard to the processing of their personal data. Moreover, the Regulation and the documents of Article 29 WP [4] provide the elements and principles to be found in Binding Corporate Rules.

BCRs can be used both for arrangements among entities of the same corporate group, and by a group of enterprises engaged in a joint economic activity, but not necessarily forming part of the same corporate group.

Standard contractual clauses (SCCs). Models of standard contractual clauses are laid down by the Commission, in order to ensure adequate safeguards for the transfer of data to third countries. By the Decision of 15 June 2001 [5] and Decision of 27 December 2004 [6] the Commission issued two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or European Economic Area. The Decision of 5 February 2010 [7] established one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA.

Moreover, standard data protection clauses may be adopted by a supervisory authority and approved by the Commission pursuant to an examination procedure.

Approved codes of conduct. The codes of conduct are defined as „voluntary accountability tools which set out specific data protection rules for categories of controllers and processors" [8]. The codes are prepared, amended or extended by associations and other bodies representing categories of controllers or processors. As provided by the non-exhaustive list stated by the Article 40(2), codes of conduct may cover topics such as fair and transparent processing; legitimate interests pursued by

controllers in specific contexts; the collection of personal data; the pseudonymisation of personal data; the information provided to individuals and the exercise of individuals' rights; the information provided to and the protection of children (including mechanisms for obtaining parental consent); technical and organisational measures, including data protection by design and by default and security measures; breach notification; data transfers outside the EU; or dispute resolution procedures. A code is approved, registered and published by the supervisory authority.

Approved certification mechanisms. Certification mechanisms may be used as an element to demonstrate compliance with specific obligations of the controllers and processors concerning the implementation and demonstration of appropriate technical and organisational measures and the sufficient guarantees. Regulation 679/2016 does not define "certification", but the European Data Protection Board cites the definition of International Standards Organisation (ISO): "the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements"[9].

Article 42(5) provides that certification shall be issued by an accredited certification body or by a competent supervisory authority. The certification bodies issue, review, renew, and withdraw certifications (Article 42(5), (7)) on the basis of a certification mechanism and approved criteria (Article 43(1)).

The EDPB considers that when assessing a processing operation, the following three core components must be considered, where applicable: 1. personal data (material scope of the GDPR); 2. technical systems- the infrastructure, such as hardware and software, used to process the personal data; and 3. processes and procedures related to the processing operation(s)[10].

Derogations. Article 49 (1) states that in the absence of an adequacy decision or of appropriate safeguards, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only under certain conditions. This article shall be interpreted in line with the provisions of the Article 44, which requires all provisions governing the transfer to be applied in such a way as to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

Therefore, the Article 49 shall be strictissimae interpretationis et applications and should never lead to a situation where fundamental rights might be breached [11].

The consent of the of the data subject is the first case stated by the Article 49. As regards the consent a two-step test must be applied: first, the consent shall meet all the conditions stated in the Article 7, as it has been interpreted by the WP 29 [12]; and as a second step, the provisions of Chapter V must be complied with.

Article 49 (1) (a) states that a transfer of personal data to a third country or an international organization may be made in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, on the condition that 'the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards'.

According to Article 4(11) of the GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The consent shall be "explicit", which means that that the data subject must give an express statement of consent [13]. Even if a written and signed statement is a unequivocal way to prove that the consent is explicit, it is not the only way to obtain explicit consent. Filling in an electronic form, sending an email, uploading a scanned document carrying the signature of the data subject, using an electronic signature are considered valid and sufficient ways to obtain explicit consent [14].

The data subject must have been informed before the transfer. As regards the information, we are again in a case of a two-layer obligation. The general obligation of information, stated by the Articles 13 and 14, of the specific circumstances of the transfer, such as the data controller's identity, the purpose of the transfer, the type of data, the existence of the right to withdraw consent, the identity or the categories of recipients etc, completed by the obligation to be also informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection

and that no adequate safeguards aimed at providing protection for the data are being implemented.

After having been informed, the data subject must provide a consent specific for the particular data transfer or set of transfers. Therefore, a consent expressed in general terms cannot meet the conditions provided by the Regulation. As general rules regarding consent apply, the consent provided by a data subject can be withdrawn at any time and with no cause.

Another derogation refers to a transfer necessary for the performance of a contract between the data subject and the controller or for the implementation of precontractual measures taken at the data subject's request. In accordance with the recital (111) data the transfer shall be occasional and necessary in relation to a contract".

The occasional character of a transfer shall be established on a case by case basis.

Since the "necessity" requirement is also stipulated in the derogations set forth in Article 49 (1) (c) to (f), it may be relevant to point out some aspects regarding the necessity test. (Does this processing actually help to further that interest? Is it a reasonable way to go about it? Is there another less intrusive way to achieve the same result?). In all case, necessity shall be justified on the basis of objective evidence.
Moreover, the case law envisaged that necessity is a concept which has its own independent meaning in European law and which must be interpreted in a manner which fully reflects the objective of the relevant law provisions [15].

It is important to point out that the performance of a contract cannot be used when a corporate group has, for business purposes, centralized its payment and human resources management functions for all its staff in a third country as there is no direct and objective link between the performance of the employment contract and such transfer, which constitutes a common practice for multinational corporations [16]. For this specific case, it is advisable to use other grounds provided by the Regulation, such as standard contractual clauses or binding corporate rules.

When a transfer is occasional and necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person, it falls under the provisions of the Article 49 (1) c). The above-

mentioned considerations regarding the necessity test and the occasional character of the transfer shall be applicable.

Another derogation, known as “important public interest derogation provides that a transfer shall take place only where it is necessary or legally required on important public interest grounds. The recital 112 clarify the scope of this derogation, through an enumeration which covers both public and private entities: “in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health”. No matter the public or private nature of the entity, the requirement for the applicability of this derogation is the existence of an important public interest.

The establishment, exercise or defence of legal claims constitutes another legitimate ground for a transfer, if the transfer is occasional and necessary. This derogation can apply to activities carried out by public authorities in the exercise of their public powers.

Since the transfer is related to “legal claims”, the procedure shall have legal grounds, but it is not limited to a procedure in front of a court of justice.

Another derogation refers to a transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent. To exemplify, this derogation is applicable when data is transferred in the event of a medical emergency and where it is considered that such transfer is directly necessary in order to give the medical care required. As it has been pointed out by the European Data Protection Board, this derogation cannot be used to justify transferring personal medical data outside the EU if the purpose of the transfer is not to treat the particular case of the data subject or that of another person’s but, for example, to carry out general medical research that will not yield results until sometime in the future [17]. The data subject must physically or legally incapable of giving consent and the proof of the incapacity may be done by reference to legal provisions or by producing relevant official documents.

Article 49 (1) (g) and Article 49 (2) allow the transfer of personal data from registers, if the conditions stated by the two articles are met. Thus, the register should, according to Union or Member State law, be intended to provide information to the public,

therefore, the registers kept for private entities are outside of the scope of the derogation. Moreover, the registers should be open to consultation either by the public in general or by any person who can demonstrate a legitimate interest. Transfers from these registers may only take place if and to the extent that, in each specific case, the conditions for consultation that are set forth by Union or Member State law are fulfilled.

The transfer shall be limited to relevant date and it cannot involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients. This derogation can also apply to activities carried out by public authorities in the exercise of their public powers.

Finally, Article 49 (1) § 2 introduces a new derogation which allows the transfer under a number of specific conditions and if it is necessary for the purposes of compelling legitimate interests pursued by the data exporter. This derogation applies only if a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation is applicable. Therefore, the data exporter must be able to prove it was impossible to frame the transfer by appropriate safeguards or to apply one of the derogations provided by the Article 49 (1) § 1.

As regards the conditions expressly enumerated by the Article 49 (1) § 2, they refer to transfer and to the data exporter. The transfer shall be non-repetitive, shall concern only a limited number of data subjects and shall be necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. In order to reach this objective, the recital 113 provides that “the controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data”.

As regards the data export, it should have assessed all the circumstances surrounding the data transfer and provided suitable safeguards with regard to the protection of personal data. Moreover, the data export shall inform the supervisory authority of the transfer and provide a complete information to the data subject.

The protection of personal data has been central to EU law for more than 20 years, from the Data Protection Directive in 1995 ("the 1995 Directive") to the adoption of the General Data Protection Regulation (GDPR) and the Police Directive in 2016. As the demand for protection of personal data is not limited to Europe, countries and regional organisations outside the EU are adopting new or updating existing data protection legislation to respond to the growing demand for stronger data security and privacy protection. The European legal provisions regulating the transfers of personal data to third countries or international organisations take into account the compatibility with different data protection systems that facilitate international flows of personal data and adapt constantly its legal mechanism in order to ensure flexible and commercial wise instruments.

REFERENCES:

[1] 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), published in the Official Journal of the European Union, L 119/4.5.2016.
[2] Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, point 96.
[3] Idem, point 74.
[4] Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, Adopted on 6 February 2018 (WP 256); Article 29 Working Party Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, Adopted on 29 November 2017 (WP 257).
[5] Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC), published in the Official Journal of the European Union, L 181/ 04.07.2001.
[6] Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, (2004/915/EC), published in the Official Journal of the European Union, L 385/29.12.2004.
[7] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, published in the Official Journal of the European Union, L 39/ 12.2.2010.
[8] European Data Protection Board, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Adopted on 12 February 2019, p.6.
[9] European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, Adopted on 25 May 2018, p.5.
[10] Idem, p. 11.

[11] Article 29 Working Party, WP 114, p.9, and Article 29 Working Party Working Document on surveillance of electronic communications for intelligence and national security purposes (WP228), p.39.
[12] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679 (WP259).
[13] Idem, p. 18.
[14] Ibidem.
[15] Judgment of the European Court of Justice of 16 December 2008 in case C-524/06 (Heinz Huber v Bundesrepublik Deutschland), para 52.
[16] European Data Protection Board, Guidelines on Article 49 of Regulation 2016/679, Adopted on 6 February 2018 (WP 261), p. 8.
[17] Idem, p. 13.