Arribat – International Journal of Human Rights
Volume: 1, Issue: 2, September 30th, 2021 | Published by CNDH Morocco

Processing data to Third Countries or International Organizations

Martina BOSSI
LUISS Guido Carli University
Rome, Italy
mbossi@luiss.it
martinabossi2@gmail.com

Abstract

The EU General Data Protection Regulation has dealt explicitly with transferring data from the EU to Third Countries or International Organizations.

It contains the core discipline of these peculiar data transfers. The EU has chosen to dedicate a whole Chapter to this matter due to the risks involved in these kinds of data processing and the sensitivity of the transferred information. We will discuss which methods the GDPR prescribes to protect sensitive information in these cases.

Furthermore, we will analyze the potential legal conflicts that may arise because of the EU law's primacy granted to data protection that views it as a fundamental right in relation to the international treaties applicable to a specific Third Country or an IO. This may result in uncertainties regarding which law should have precedence over the other - the GDPR or the International law – causing troubles to data controllers and data processors to carry out international data transfers safely.

Keywords— General Data Protection Regulation, international data transfers, legal framework, potential legal conflicts.

I. INTRODUCTION

In the latest years, data protection has become a more and more analyzed and regulated sector. Having significantly increased our use of digital devices, it is crucial that their access to our data, the way they store it, and which authority may have access to them, for how long, and for which purpose must be strictly regulated. If not, the risk of fundamental human rights violations would exponentially increase.

In an attempt to provide an updated and more comprehensive regulation, the EU adopted Regulation n.2016/679 – came into effect on May 25th, 2018 – commonly known as General Data Protection

Regulation (GDPR). Adopting this text has been an essential step towards setting minimum international standards applicable to everyone, regardless of origin. Furthermore, it would contribute to increasing the overall protection that can be granted when accessing digital space.

This article will delve into the legal framework that the EU has set to deal with the international transfer of data towards third countries or international organizations (IOs). These rules apply independently from the national level of data protection which those countries' citizens are entitled to, in some cases, contribute to improving the national standards.

Since data and information exchange with third countries or IOs is frequent nowadays, knowing which rules apply in these cases could improve international cooperation, continually granting fundamental human rights.

II. A LAYERED APPROACH

The transfer of personal data to third countries or IOs has explicitly been dealt with in Chapter V of the GDPR [1], from Article 44 to Article 50.

These Articles contain the core regulations of these particular data transfers. The EU has chosen to dedicate a whole Chapter to this matter due to the risks involved in these kinds of data processing and the sensitiveness of the transferred information.

The GDPR prescribes three different methods to protect sensitive information in these cases, provided that the general provisions contained in Art. 5 and 6 of the GDPR have been met.

Namely, Article 5 described the fundamental principles that have to occur when dealing with data (i.e., lawful processing, purpose specification and limitation, accountability). Then, Article 6 set out the conditions without which data processing could not be considered fair.

Articles 45 – 47 describe these three different methodologies, formally known as "provisions for cross-border data flows".

These provisions set out to verify that the rules prescribed by the GDPR would be respected, turning to a multi-level analysis.

Article 45 regulates the first step to be taken when checking for compliance of a third country or IOs with the GDPR provisions: checking whether the EU Commission has decided that the specific third country or the IO in question ensures an "adequate level of protection".

As clarified by the EU Commission [2], before it may adopt such a decision, an administrative procedure has to be followed.

First, there should be a proposal from the EU Commission itself, which must immediately be submitted to the European Data Protection Board (EDPB) to acquire its opinion about the Country or the IO.

Following the EDPB opinion, the proposal has to be submitted to the EU Countries' representatives to acquire their approval.

Once each of the previously described steps has received positive feedback, the EU Commission can adopt its definitive decision that falls under Article 45 of the GDPR.

Nevertheless, given the "subordinate position" of the EU Commission in respect of the EU Parliament and Council, these two institutions may, at any time, request for the Commission to maintain, amend or withdraw the adequacy decision "on the grounds that its act exceeds the implementing powers provided for in the regulation".

Prior to submitting the proposal to the EDPB, Article 45 prescribes that the Commission should deeply investigate whether that third country or IO complies with:

- "The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral […], as well as the implementation of such legislation, data protection rules, professional rules and security measures […], as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- the existence and effective functioning of one or more

independent supervisory authorities in the third country or to which an international organization is subject […] for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States;

- the international commitments the third country or international organization concerned has entered into […], in particular in relation to the protection of personal data".

Once the Commission has expressed its decision and released the subsequent implementing act, it must be submitted for periodic review – every four years – where all relevant developments that occurred within the third country or the IO will be taken into account.

If the Commission concludes that the third country or the IO is no longer secure during the review, it has to enter into consultations with the involved subject to try solving the issue.

Whether the negotiation is not possible or has ended up being unfruitful, the third country or the IO will be removed from the list of the subjects in which adequate warranties protecting the privacy of the data subjects are granted with no retroactive effect. An exception to this can only be made when there are "duly justified imperative grounds of urgency".

As prescribed by Article 45(8) of the GDPR, the EU Commission has published the list of the third countries that ensure an adequate level of personal data protection.

Nowadays, these are Andorra, Argentina, Canada (commercial organizations included), Faroe Islands, Guernsey, Israel, Isle of Man, Japan (only covering private sector organizations [3]), Jersey, New Zealand, Switzerland, Uruguay, and the United States of America (even if limited to the Privacy Shield framework [4]).

Currently, adequacy talks are ongoing with South Korea, but an outcome from these negotiations is far to reach. Discussions are at a more advanced stage with Morocco, for example. In fact, in 2018, the National Commission for the Control of the Personal Data Protection CNDP (the Moroccan data protection authority) presented the results of a study that it led with the European Union delegation in

Morocco. This study recommended a scenario that "aims to integrate a "moderate" GDPR. This scheme would involve a certain number of amendments to the law to reduce the gaps with the GDPR while considering local specifications." [5]

The EU Commission does not always gather all the necessary information to declare that a third country or an IO could grant high personal data protection. In these cases, an adequacy decision cannot be adopted.

Given the difficulty of collecting information in some of these countries – or related to IOs working within these countries –, binding the possibility to transfer personal data only if the subject has met all the strict criteria set for in Article 45 of the GDPR could risk discriminatory exclusion of an otherwise reliable party.

For this reason, the GDPR in its Article 46 prescribes that failing to meet the conditions set out in Article 45, a data controller or processor may still transfer personal data whether:

-It has provided "appropriate safeguards";

-Enforceable data subject rights and effective legal remedies for data subjects are available.

Article 46 then describes the appropriate safeguards that a Third Country or an IO must provide to comply with the GDPR conditions.

The requested safeguards differ according to whether a specific authorization from a supervisory body is needed.

If this authorization is not needed, the safeguards which a data controller or processor may provide in order to be considered appropriate are:

- A legally binding and enforceable instrument between public authorities or bodies [6];
- Binding corporate rules;
- Standard data protection clauses adopted by the EU Commission [7];
- Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure;

- An approved code of conduct, together with binding and enforceable commitments of the controller or processor in the Third Country that applies appropriate safeguards to protect data subjects' rights;
- An approved certification mechanism, together with binding and enforceable commitments of the controller or processor in the Third Country, that applies appropriate safeguards to protect data subjects' rights.

Furthermore, article 46 provides for two other appropriate safeguards under the condition that a competent supervisory authority authorizes them. Namely, these safeguards are:

- "contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights".

The latest safeguard applies to severely limited circumstances. Indeed, a cross-border transfer can be made using this safeguard only if: (i) both the transferor and the transferee are public authorities or bodies; (ii) both parties enter into an administrative arrangement that provides for the data subjects rights; and (iii) the administrative arrangement is approved by a supervisory authority.

Suppose it is not possible to adopt an adequacy decision or an appropriate safeguard. In that case, the GDPR still allows the transfer of personal data to third countries and IOs if the following conditions are met:

- An explicit consent of the data subject has been acquired, and this consent has to be: (i) fully informed and entirely given; (ii) obtained at the time of collection or as soon as possible; (iii) genuinely and freely given; (iv) the data subjects vulnerability is taken into account [8]; (v) documented, so that it will be possible to demonstrate at any time that the data subject has effectively provided his/her consent [9];

- The transfer is necessary for the performance of a contract between the data subject and the controller;
- The transfer is necessary for a contract's conclusion or performance in the interest of data subjects between the controller and another natural or legal person;
- The transfer is necessary for the critical reason of public interest;
- The transfer is necessary for legal claims;
- The transfer is necessary to protect vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent;
- The transfer originated from a register.

Moreover, article 49(5) of the GDPR states that the EU or a Member State law could limit the transfer of specific categories of personal data to a third country or an IO. This often happens when an adequacy decision is absent, and restricting the transfer is fundamental for important reasons of public interest.

Even though there is a disciplined legal framework for transferring personal data to third countries or IOs, as we have seen, there still are some uncertainties regarding the interpretation of some principles.

As we will investigate in the next paragraph, legal conflicts may potentially arise from the strict application of the GDPR principles.

I. POTENTIAL LEGAL CONFLICTS AND THE CJEU APPROACH

One of the main potential legal conflicts is contained in Article 44 of the GDPR, which requires data controllers and data processors that carry out international data transfers to conduct such transfers following the principles contained within the GDPR.

Potential legal conflicts may arise because of EU law's primacy granted to data protection, seeing it as a fundamental right. This may originate uncertainties regarding which law should have precedence over the other, whether the GDPR or International Law.

Article 44's wording indeed infers three possible scenarios:

1) An IO established in the EU which transfers data to an IO which is based in a third country;

2) An IO established in a third country receives personal data from an IO based in the EU and then transfers them to another party (different from an IO) based outside the EU territory;

3) An IO established in a Third Country receives personal data from an IO based in the EU and then transfers them to another IO based outside the EU territory [10].

Given the intrinsic international nature of the IOs, those IOs which transfer personal data to a third country or another IO may consider themselves bound by the rules set for them by the UN Charter [11], treaty rules, customary International Law, or even their own internal rules instead of those established by the EU data protection law.

Taking a closer look at the first scenario represented, the IO, which should be subject to the GDPR rules, may rebut that they do not need to comply with them because of the privileges and immunities granted to them by international law.

As for the second scenario, the same remark could be made, but the potential conflict may be more severe this time because one of the subjects involved in the transaction could be subject to a law different from that applied within the EU.

The third scenario then is the one that could give rise to most of the conflicts because if privileges and immunities are granted to the IOs based outside the EU territory, there would be an opposition between the EU data protection law and Public International Law.

The fear for the above said potential legal conflicts to arise is based on the fact that data protection is categorized as a fundamental right by the EU legal system [12] and that, according to Article 6(1) of the Treaty on European Union, it acquires the status of primary law. Furthermore, in a CJEU ruling [13], it has been clearly stated that precedence must be granted to primary law over International Law, including international treaties.

Since International Law is essential for the EU legal order, the most followed interpretation suggests that this possibility for the GDPR to override international law should be limited only to those cases

where the core principles of data protection are in danger.

Nevertheless, following this interpretation, another question may arise: what can be defined as a core principle?

The CJEU has attempted to solve this problem in numerous rulings, the most famous of which being Schrems [14].

On that occasion, the Court stated that third countries must provide a level of protection that is "essentially equivalent" to that under EU law.

The Court, indeed, specified 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 under 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".

Even though this interpretation is unambiguous, it may raise other doubts about the core values against which the required equivalence must be measured.

The Article 29 Working Party [15] reiterates the CJEU position stating that: in a third country or an IO, a set of "core data principles" have to be present to ensure essential equivalence to those contained within the EU legal framework [16].

Different from the definition of "core" of the right to data protection is the "essence" of this right.

Article 52(1) of the EU Charter of Fundamental Rights includes this latest notion, stating that: "Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms."

The Article even foresees the possibility of limiting those rights and freedoms under the condition that: "Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."

As may be inferred by comparing the concept of core with the wording of this Article, the term "core" is precisely used to describe the main principles of data protection set forth within the GDPR. On the other hand, the term "essence" is stricter and has a specific legal meaning, which does not apply to the term "core".

Further proof of the breadth of the GDPR concept of core of the right to data protection may be extrapolated by looking at the vagueness of the language used in the Chapter here discussed.

III. CONCLUSION

Summing up all of the above, it could be inferred that the core of the right to data protection – which overruled the International Law typically applied to third countries and IOs – are: lawful processing, purpose specification and limitation, data quality, fair processing and accountability.

Nonetheless, several provisions included in the GDPR do not embody this core of the right to data protection, although they handle the details of how these rights should be implemented.

This Regulation is a good starting point for setting out a clear and defined practice for a sector, which will continue to grow in the following years. For this reason, this legal framework represents just the beginning: adjustments have to be done both at the EU and the international levels so that the discipline of a sector, which borders could not limit, could be unified and harmonized.

This would substantially improve the general international protection of fundamental human rights when it comes to data transfers.

IV. REFERENCES

[1] European Union. (2016). EU Regulation 2016/679 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. *Official Journal of the European Union.*

[2] European Commission. (2019). Adequacy decisions - How the EU determines if a non-EU country has an adequate level of data protection.

[3] European Commission. (2019). Commissioner for Justice, Consumers and Gender Equality, EU Japan Adequacy Decision - Fact sheet.

[4] U.S. Department of Commerce. (2016). EU-US Privacy Shield Framework.

[5] Chenaoui, H. (2018). Moroccan data protection law: Moving to align with EU data protection?

https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/.

[6] Vollmer, N. (2021, July 2). *Recital 108 EU General Data Protection Regulation (EU-GDPR). Privacy/Privazy according to plan.* Nicholas Vollmer. https://www.privacy-regulation.eu/en/recital-108-GDPR.htm

[7] Recital 109 - Standard Data Protection Clauses. (2019, September 3). General Data Protection Regulation (GDPR). https://gdpr-info.eu/recitals/no-109/

[8] International Organization for Migration (IOM). (2010). *Data protection Manual*.

[9] Kuner, C. & Marelli, M. (2017). Handbook on Data Protection in Humanitarian Action.

[10] EUR-Lex - 52012PC0011 - EN - EUR-Lex. (n.d.). EUR-Lex. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012PC0011

[11] United Nations. Art. 103 of the UN Charter. https://www.un.org/en/sections/un-charter/un-charter-full-text/

[12] European Union. Art. 8 of the Charter of Fundamental Rights of the European Union. https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[13] InfoCuria. Joined Cases C-402 & 415/05P, Kadi, 2008 ECR 1-6351. http://curia.europa.eu/juris/liste.jsf?num=C-402/05&language=en.

[14] InfoCuria. Case C-362/14, Maximilian Schrems vs Data Protection Commissioner. http://curia.europa.eu/juris/liste.jsf?num=C-362/14.

[15] European Data Protection Board. The Article 29 Working Party. https://edpb.europa.eu/our-work-tools/article-29-working-party_en.

[16] European Commission. Article 29 Working Party, "Adequacy referential" (updated). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.