The GDPR and International Organizations

Kuner, Christopher

Published in:
American Journal of International Law Unbound

DOI:
10.1017/aju.2019.78

Publication date:
2020

doi:10.1017/aju.2019.78

SYMPOSIUM ON THE GDPR AND INTERNATIONAL LAW

THE GDPR AND INTERNATIONAL ORGANIZATIONS

*Christopher Kuner**

The entry into application of the EU General Data Protection Regulation (GDPR) on May 25, 2018 has raised questions about its impact on data processing by intergovernmental organizations that operate under public international law (referred to here as international organizations or IOs). EU data protection law can have impact beyond EU borders, and the global reach of EU law is a well-recognized phenomenon.[1] The GDPR contains numerous references to IOs but does not state whether it applies to them, and this uncertainty has led to tensions between IOs and the European Commission. The issues surrounding IOs' processing of personal data show how the GDPR can give rise to unexpected questions under public international law, and illustrate the need for greater engagement between EU law and international law.

IOs and Data Protection

IOs increasingly need to process and transfer personal data in order to fulfil their mandates. This can be seen, for example, in the work of IOs in the humanitarian sector, which use data-intensive technologies such as data analytics, drones and unmanned aerial vehicles, biometrics, cloud services, and mobile messaging apps to deliver essential aid to vulnerable individuals.[2]

Their use of new technologies also makes it necessary for IOs to implement rules to protect the processing of personal data. In some sectors, the misuse of personal data may have life and death consequences. (For example, the disclosure of a simple list of names of asylum seekers by a humanitarian IO may endanger their lives.) Data protection laws can provide "rules of the road" for the processing of personal data that are derived from regional and international human rights standards, and can also help to build trust with the individuals and organizations to whom IOs are accountable.

For these reasons, a number of IOs have already adopted their own internal data protection rules, including the International Organization for Migration,[3] the International Committee of the Red Cross (ICRC),[4] the UN High

* *Professor of Law and Co-Chair of the Brussels Privacy Hub, Vrije Universiteit Brussel (VUB), Brussels; Visiting Professor, Maastricht University; Associate, Centre for European Legal Studies, University of Cambridge*

[1] *See, e.g.*, EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law (Marise Cremona & Joanne Scott eds., 2019).

[2] *See* Alexander Beck & Christopher Kuner, *Data Protection in International Organizations and the New UNHCR Data Protection Policy: Light at the End of the Tunnel?*, EJIL: Talk! (Aug. 31, 2015); Christopher Kuner & Massimo Marelli, *Creating International Frameworks for Data Protection: The ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action*, EJIL: Talk! (July 13, 2017).

[3] Int'l Org. for Migration, IOM Data Protection Manual (2010).

[4] Int'l Comm. of the Red Cross, ICRC Rules on Personal Data Protection (2015).

Commissioner for Refugees,[5] the International Criminal Police Organization (INTERPOL),[6] and the World Food Programme,[7] among others. In December 2018, the United Nations also approved a set of personal data protection and privacy principles for processing personal data by or on behalf of UN organizations.[8]

Legal Issues

I have provided elsewhere a detailed analysis of the relevant legal issues concerning application of the GDPR to IOs,[9] and will not repeat that discussion here. However, the two main positions that have been asserted in this regard can be summarized as follows.

One position is that the GDPR does not apply to IOs. The GDPR seems to equate IOs with third countries as entities subject to a body of law other than EU law, which could indicate that IOs were intended to fall outside the scope of the GDPR. The EU is bound to observe international law in its entirety,[10] indicating that the GDPR was not meant to apply to subjects of international law like IOs. This is bolstered by the view that, as Advocate General Szpunar of the Court of Justice of the European Union (CJEU) has stated, EU law has extraterritorial effects only "in extreme situations of an exceptional nature."[11] The European Commission has also stated informally that the GDPR does not apply to IOs directly since they generally enjoy privileges and immunities under international law, though the Commission also maintains that the GDPR's rules on international data transfers do apply to transfers from the EU to IOs.

A contrary view is that application of the GDPR to IOs should be determined under its material and territorial scope, considered in light of any privileges and immunities that an IO may enjoy and the status of international law in the EU legal order. The GDPR contains several exemptions from its material scope, and the GDPR legislator could have mentioned IOs among them if it had meant to exclude them. The fact that IOs are mentioned throughout the GDPR, and that under Article 44(1) transfers of EU data between IOs can only be carried out subject to the rules of the GDPR, indicate the legislator's concern about their processing of personal data. While "pure" extraterritoriality may be rare in EU law, it is relatively common for EU data protection law to apply based on a territorial connection with the EU.[12] The CJEU has also found that EU law can take precedence over international law when EU fundamental rights (which include data protection) are involved.[13] Finally, the lack of an agreed definition of IOs in public international law and the wide variety of organizations considering themselves to be one (which can range from those working for the global public good to those that act more as interest groups

[5] UN High Commissioner for Refugees, Policy on the Protection of Personal Data of Persons of Concern to UNHCR (2015).

[6] Int'l Criminal Police Org., Rules on the Processing of Personal Data (2016).

[7] World Food Programme, WFP Guide to Personal Data Protection and Privacy (2016).

[8] United Nations, Personal Data Protection and Privacy Principles, adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on Oct. 11, 2018.

[9] Christopher Kuner, *International Organizations and the EU General Data Protection Regulation*, 19 Int'l Orgs. L. Rev. 158 (2019).

[10] Case C-366/10, Air Transport Association of America v. Secretary of State for Energy and Climate, ECLI:EU:C:2011:864, para. 101 (Eur. Ct. Justice, Dec. 21, 2011).

[11] Case C-507/17, Google LLC v. CNIL, Opinion of Advocate General Szpunar, ECLI:EU:C:2019:15, para. 53 (Eur. Ct. Justice, Jan. 10, 2019). The Court gave its judgment in the case on Sept. 24, 2019. Case C-507/17, Google LLC v. CNIL, ECLI:EU:C:2019:772 (Eur. Ct. Justice, Sept. 24, 2019).

[12] *See* Opinion 1/15, ECLI:EU:C:2017:592 (Eur. Ct. Justice, July 26, 2017); Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Eur. Ct. Justice, Oct. 6, 2015).

[13] *See* Joined Cases C-402/05 P and C-415/05 P, Kadi, ECLI:EU:C:2008:461, para. 285 (Eur. Ct. Justice, Sept. 3, 2008).

or frameworks for occasional diplomacy by states)[14] undermine the argument that the GDPR was intended to exclude all IOs per se.

Privileges and Immunities of IOs and the GDPR

The privileges and immunities of IOs are not mentioned in the EU constitutional treaties (aside from those of the EU itself and certain of its entities), and the EU is not a party to the 1946 Convention covering the privileges and immunities of the UN[15] and the 1947 Convention covering those of its specialized agencies.[16] Privileges and immunities of IOs outside the UN system derive most frequently from bilateral agreements between IOs and states, and determining their application to the GDPR is complicated by the fact that in such cases privileges and immunities are granted by the member states and not by the EU. (Privileges and immunities of IOs deriving from national legislation or from customary international law will not be discussed here.) The GDPR does not mention the privileges and immunities of IOs, and not all member states have granted them to all IOs.

This situation makes it necessary to rely on general EU law when attempting to clarify the status of the privileges and immunities of IOs in light of the GDPR. For instance, an argument can be made that EU law (including the GDPR) should not undermine the application of privileges and immunities granted to IOs by the member states, based on the duty of sincere cooperation between the EU and the member states under Article 4(3) of the Treaty on European Union.[17] Failure of EU law to respect privileges and immunities in such cases could create conflicts between international law and EU law, such as if a member state were obliged to apply EU law to an activity by an IO for which it had granted privileges and immunities under a bilateral treaty. The duty of sincere cooperation requires that such conflicts be avoided as much as possible, and the CJEU has held that EU law must be interpreted in light of rules of international law binding on the member states, such as the principle of good faith.[18] This could arguably include a duty to interpret the GDPR consistently with the privileges and immunities that the member states have granted to IOs.

The CJEU, which is the ultimate arbiter of EU law, has yet to opine on these issues. However, it may do so in the future in a case that was referred to it in July 2019 and which involves, among others, the question of whether an IO such as INTERPOL provides an adequate level of data protection based on the standards of EU law.[19]

Hard and Soft Enforcement of the GDPR

Given this murky legal situation, it is not surprising that there is considerable uncertainty about the extent to which IOs should implement the GDPR. However, the situation becomes clearer when one turns from application of the GDPR to its enforcement.

With regard to "hard enforcement," i.e., legal enforcement based on an order by a data protection authority (DPA) or a court, IOs typically enjoy immunities against legal process. EU law becomes part of the legal order of the member states, and immunities granted on a national level should also apply when a DPA or national court

[14] *See* Jan Klabbers, An Introduction to International Organizations Law 11 (2015) (Kindle ed.).

[15] Convention on the Privileges and Immunities of the United Nations, Feb. 13, 1946, 1 UNTS 15, UN Doc. ST/LEG/SER.B/10 (1959), at 184 *et seq.*

[16] Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations of 1947, 33 UNTS 261.

[17] Consolidated Version of the Treaty on European Union, 2012 O.J. (C 326) 1 (Oct. 26, 2012).

[18] Case C-308/06 Intertanko, ECLI:EU:C:2008:312, para. 52 (Eur. Ct. of Justice, June 3, 2008).

[19] Case C-505/19 WS v. Federal Republic of Germany (pending).

attempts to carry out enforcement action under the GDPR. Since legal enforcement under the GDPR is conducted at the national level, this means that IOs will generally be protected against it by the immunities they enjoy.

However, there is also what can be referred to as "soft enforcement," meaning informal pressure that actors in the public and private sectors can exert against IOs to force them to adopt the standards of the GDPR. This may involve, for example, an EU agency requiring an IO to comply with the GDPR as a condition for receiving funding; or a company that provides services to an IO demanding that it accept a clause in the services agreement stating that it complies with the GDPR. Soft enforcement can be more difficult for IOs to resist than is hard enforcement, since there is usually no way to mitigate the former's effects short of refusing to deal with the actor making the demands. IOs are understandably concerned that succumbing to such pressure could be construed as a waiver of their privileges and immunities.

Data Transfers to IOs

Certain provisions of the GDPR provide a legal basis for the transfer of personal data to IOs in some cases. For example, under Article 46(3)(b), appropriate safeguards for data transfers to IOs may be provided by "provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights." On February 12, 2019, the European Data Protection Board (EDPB) issued an opinion on a draft administrative arrangement for the transfer of personal data between European Economic Area (EEA) financial supervisory authorities and those outside the EEA, and found that the arrangement could provide appropriate safeguards for the transfer of personal data under the GDPR.[20] Such arrangements could potentially be adapted to serve as a legal basis for data transfers to IOs as well.

Other provisions of the GDPR contain legal bases that member states could use for data transfers to IOs in the humanitarian sector. Thus, Recital 112 states that data transfers to international humanitarian organizations of the personal data of an individual who is physically or legally incapable of giving consent may be found necessary for an important reason of public interest or because it is in the vital interest of the data subject when this is necessary to accomplish a task under the Geneva Conventions or to comply with international humanitarian law in armed conflicts. This could provide a legal basis under Article 49(1)(d) or Article 49(1)(f) of the GDPR for data transfers to certain IOs, such as the ICRC.

Conclusion

IOs need to process ever-increasing amounts of personal data in order to fulfil the functions assigned to them, and data protection facilitates this by reducing the possibility of data misuse and building trust among the individuals and organizations that they deal with. Data protection also represents a normative standard anchored in human rights law that increases the accountability of IOs. They should thus implement data protection regardless of whether the GDPR applies to them in a legal sense.

The global impact of the GDPR and the fact that many of its principles have influenced data protection laws around the world mean that it can serve IOs as a source of inspiration and international best practices. Implementing data protection can also help IOs prevent the erosion of their privileges and immunities by demonstrating that they have put in place alternate mechanisms to protect personal data even when the law may not apply to them directly.

[20] European Data Protection Board, *Opinion 4/2019 on the Draft Administrative Arrangement for the Transfer of Personal Data Between European Economic Area ("EEA") Financial Supervisory Authorities and Non-EEA Financial Supervisory Authorities* (Feb. 12, 2019).

Beyond the practical issues that arise under the GDPR, its impact on IOs shows that there is a lack of clarity surrounding the interaction between EU law and public international law, and illustrates the tension between the traditional functionalist approach to the governance of IOs and the modern trend towards greater accountability.[21] From the perspective of public international law, scholars, states, and courts have paid insufficient attention to what law applies to the operation of IOs, and how the law of a regional organization like the EU can impact their privileges and immunities. In most cases the privileges and immunities of IOs are based on international agreements between states and IOs, but international law does not address the impact on privileges and immunities of the law of a supranational organization (i.e., the EU) of which the states granting them are members.

The example of the GDPR also exposes contradictions in the way that EU law deals with IOs. Since EU law becomes part of member state law, applying EU law to IOs when they have been granted privileges and immunities by the member states is bound to create tension between EU law and international law. In enacting the GDPR, the EU legislator failed to clarify its application to IOs, which creates legal uncertainty for IOs, the individuals whose personal data they process, and regulators who are charged with enforcing data protection law.

In this situation, dialogue and bridge-building between the EU and IOs is essential. Such discussions are ongoing between various IOs and the Legal Service of the European Commission, and IOs have also met regularly among themselves to discuss data protection issues.[22] The EU institutions and IOs could also discuss the possibility of adapting data transfer mechanisms under the GDPR to cover the special case of IOs. In November 2019, the EDPB issued a paper stating that "the application of the GDPR is without prejudice to the provisions of international law," including the privileges and immunities of IOs,[23] but this seems to be little more than a statement of the obvious (i.e., that the GDPR may not be enforced when an IO enjoys privileges and immunities).

The European Commission should also confirm publicly its informal position that the GDPR does not apply to IOs (aside from its rules on data transfers from the EU) and indicate the legal reasoning that underlies it. The Commission's invocation of the privileges and immunities of IOs as a way to dismiss concerns about application of the GDPR without further explanation is unconvincing, particularly in light of the well-established position in diplomatic law that privileges and immunities act as a procedural bar to enforcement of the law rather than to preclude legal liability.[24] Even if not legally binding, guidance by the EDPB and the Commission could help provide IOs with arguments to resist the effects of the various forms of soft enforcement to which they may be subject.

Data processing has attained substantial significance in the work of IOs. The GDPR is influential around the world, and it is inevitable that questions about its application to IOs have arisen. These questions are not dealt with in the GDPR itself, nor does EU law or public international law provide easy answers to them. It is therefore essential that IOs, data protection authorities, and EU institutions enter into an open dialogue to discuss how IOs can implement data protection in their operations while safeguarding their privileges and immunities.

[21] *See* Jan Klabbers, *The EJIL Forward: The Transformation of International Organizations Law*, 26 EJIL 9 (2015).

[22] *See, e.g.*, Wojciech Wiewiórowski, *International Organisations Demonstrate Dedication to Data Protection*, Eur. Data Prot. Supervisor (July 17, 2018).

[23] Eur. Data Prot. Bd., *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) Version 2.0*, at 23 (Nov. 12, 2019).

[24] *See* Eileen Denza, Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations 257–59 (2016) (Kindle edition).