universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„How does GDPR effect the work of International Organizations?”

verfasst von / submitted by

Alisa Alia

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2019 / Vienna 2019

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Peter Fischer, Prof.

Table of Contents

List of Abbreviations.

Abbreviation	Name
The Charter	Charter of Fundamental Rights of the EU.
TFEU	Treaty of the Functioning of the EU.
UN	United Nations.
UDNH	Universal Declaration of Human Rights.
ICCPR	Covenant on Civil and Political Rights.
GDPR	General Data Protection Regulation.
IO	International Organization.
EC	European Commission.
Data Subject	A natural person.
WHO	World Health Organization.
INTERPOL	International Crime Police Organization.
UN Global Pulse	United Nations Global Pulse.
SG	UN Secretary General.
OECD	Organization for Economic and Co-operation and Development.
OSCE	Organization for Security and Co-operation in Europe.
UNHCR	United Nation Human Rights Council.
DPO	Data Protection Officer.
EU	European Union.
HQ	Headquarters
The Board	European Data Protection board

"What is at stake is not only the protection of our privacy, but also the protection of our democracies and ensuring the sustainability of our data-driven economies."-

-European Commission.

Introduction.

The protection of a natural person in relation to the processing of personal data is a fundamental human right. Article 8 (1) of the Charter of Fundamental Rights of the European Union ("The Charter") and article 16 (1) of the Treaty of the Functioning of the European Union ("TFEU") provides that everyone has the right to the protection of personal data concerning him or her.[1] United Nations ("UN") has a long history promoting the right to privacy through its Human Rights treaties particularly through article 12 of the Universal Declaration of Human Rights ("UDHR") and article 17 of the Covenant on Civil and Political Rights ("ICCPR")[2].

Ever since the new "General Data Protection Regulation" entered into force in 25th of May 2018, there has been a tremendous interest in this field from everyone because of its broad scope of application and also the way it affects all Union based companies on how they handle "personal data" but also the "spill over effect" that it has on companies that are based outside the Union, but conduct business in the Union or follow to behaviour of the union consumers.

Rapid technological developments and globalization have brought new challenges for the protection of personal data[3]. As a consequence, the scale of the collection and processing of personal data has been significantly increasing. The "General Data Protection Regulation" ("GDPR") has been called by far the "most influential policy instrument" in the data

[1] *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1.

[2] UNCTAD, Data Protection Regulation and International Data Flows: implications for trade and development. (United Nations, 2016).

[3] *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1. Recital 6.

protection sphere[4], because of its broad scope of application and the worldwide impact it has had by far in the business world.

The role of GDPR is indeed well established and it is understandable that it puts the data subject in a "front row seat" when it comes to the way companies handle data, but what happens in cases of International Organizations ("IOs") and the way they handle personal data? Is the GDPR applicable in this case? Can the data subject invoke the same rights towards an IO?

The purpose of this paper is to analyse the relationship between the GDPR and IOs, as well as to analyse whether IOs are bound and should follow the rules as set out in the Regulation.

Chapter 1. What is the meaning of "Personal Data"?

GDPR applies to the processing of **personal data,** wholly or partly by automated means and to the processing other than by automated means of **personal data** which form part of a filing system or are intended to form part of a filing system[5].

But what is understood with "Personal Data"? The European Commission ("EC") has defined personal data as 'any information relating to an identified or identifiable **natural person[6]** ('data subject')[7]'.

So, in this regard it is "safe" to say that personal data consists of different pieces of information which, when collected together, can lead towards the identification of a specific natural person. In order to identify or make a natural personal identifiable, GDPR sets a non-exhaustive list of requirements that include information such as name, identification number,

[4] Collin Bennett and Charles Raab, The Government of Privacy: Policy Instrument in Global Perspective (MIT Press 2006) 93.

[5] *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1, Article 2 para. 1.

[6] *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1, Recital 14 on "Not Applicable to legal person".

[7] *EU Directive 95/46*: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31, Article 4.

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[8]

Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the law.[9]

Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable is no longer considered personal data.[10] For data to be truly anonymized, the anonymization must be irreversible.[11]

A. Data processing by IOs.

The number of IOs has been rapidly increasing in the recent years and it still continues to grow. There are more than 68,000 International non-governmental and Intergovernmental organizations[12] listed (both active and inactive) that are established around the world and the number keeps increasing every day, while the number of those considered to be Intergovernmental Organizations that are subject of public international law is estimated to be around hundreds.[13]

The mandate of IOs touches upon almost every area of human activity,[14] such as in migration; refugee seekers; health; labour; hunger etc. In order for the organization to fulfil this mandate given by its member states, enormous types of data collecting, data processing and data transfer among different entities will have to take place.

For example, the World Health Organization ("WHO") engages in public-private partnerships in the field of international public health cooperation that includes data exchange;[15] the International Criminal Police Organization ("INTERPOL") has a long history

---

[8] Ibid.

[9] "*What is personal data*?", European Commission < https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en#references> accessed 25 November 2018.

[10] Ibid.

[11] Ibid.

[12] Yearbook of International Organizations, *Open Yearbook*, < https://uia.org/ybio/ > accessed 25 November 2018.

[13] J.Klabbers, *An Introduction to International Organization Law* (CUP 3d ed., 2015), at 1 note 2 (Kindle edition), stating that estimates about the number of such IOs vary from 240 to 350; Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 January 2019.

[14] Ibid.

[15] Burci, '*Public/Private Partnerships in the public Health Sector*'.

of exchanging data with the United Nations ("UN");[16] and United Nations Global Pulse ("UN Global Pulse"), an initiative of the UN Secretary-General ("SG") that works with partners in the public and private sectors to harness large-scale data analytics ('Big Data') for the public good.[17] Thus, it has been said that 'institutions like the United Nations, the World Bank or the Organization for Economic and Co-operation and Development ("OECD") function as data hubs and information clearinghouses'[18] that collect and disseminate vast amounts of personal data.[19]

Taking into consideration the abovementioned examples, we can easily get to the conclusion that in the "everyday" work of IOs, a lot of data collecting, and data processing takes place. Therefore, it is crucial to understand the importance of Data Protection Law and strictly follow the rules as set out in the law while performing their tasks in order to fulfil their given mandate.

B. The relationship between Data Protection and IOs.

Data processing is a tool used for years now, that helps businesses to target specific groups of interest, increase productivity as well as profits, better decision-making, lower risks, reduce costs etc. Despite the undoubted benefits, the processing of data also bares risks such as data security breaches, potential misuse of data, collection of data beyond what is necessary, retention of data for unlimited period of time etc. To protect individuals against such risks, data protection laws have emerged throughout the world with the vision of setting clear cuts on what personal data can be collected, how it can be used and the ways to process this data.

Data protection is a concept that is carved in instruments of international human rights law such as the Universal Declaration of Human Rights ("UDHR") of 1948[20] and the International Covenant on Civil and Political Rights ("ICCPR") of 1966,[21] that protects towards a family

[16] INTERPOL website, < https://www.interpol.int/About-INTERPOL/International-partners/United-Nations > accessed 25 November 2018.
[17] "About UN Global Pulse", < https://www.unglobalpulse.org/about-new > accessed 25 November 2018.
[18] Riegner, "*Towards an International Institution Law of Information*" (2015) 50, 51.
[19] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 January 2019.
[20] Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR), Article 12.
[21] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), Article 17.

life, private life, home and correspondence. However, in the abovementioned instruments, data protection is not explicitly mentioned, but it is formulated as a rather vague term that only mentions bits and pieces of what today forms the concept of data protection as such.

The main international treaty dealing specifically with data protection is the Council of Europe Convention for Protection of Individuals with regard to Automatic Processing of Personal Data, dating back in 1981.[22] Later on, in 1988, the UN Human Rights Committee, mentioned in their opinion on CCPR General Comment No.16[23] on Article 17 (Right to Privacy), the term "personal information" which was interpreted in the way that concludes the core principles of data protection law such as lawfulness, legality, and right to correct or eliminate the data.

The document that applies to IOs and Governmental International Organizations is the Un General Assembly ("GA") Guidelines for the Regulation of Computerized Personal Data Files from 1990.[24] In this guideline, among other important things, it is mentioned that it "should apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization"[25]. This explains the binding nature that this guideline has towards IOs meaning that each organization should designate the authority statutorily competent to supervise the observance of these guidelines[26].

In 2007 the UN Secretary General issued a bulletin covering confidential information entrusted to or originating from the UN, and deeming to be sensitive:
'documents whose disclosure is likely to endanger the safety and security of any individual, violate his or her rights or invade his or her privacy.'[27]

[22] Convention for Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108.
[23] HCR, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and protection of Honour and Reputation: < https://www.refworld.org/docid/453883f922.html > accessed 26 November 2018.
[24] Un General Assembly "Guidelines for the Regulation of Computerized Personal Data Files", GA Res. 45/95, 14 December 1990, <https://www.refworld.org/pdfid/3ddcafaac.pdf > accessed on 30 November 2018.
[25] Ibid.
[26] Ibid.
[27] UN Secretary-General's bulletin, 'Information sensitivity, classification and handling'(2007), UN-Doc. ST/SGB/2007/6. < https://hr.un.org/handbook/source/secretary-general%27s-bulletins/date > accessed 27 November 2018.

The UN GA's December 2016 resolution, affirming the right to privacy in the digital age[28] and the appointment in July 2015 of a UN Special Rapporteur on the right to privacy by the Human Rights Council[29] ("UNHCR") demonstrating the interest of the international community in embedding data protection more strongly in the international human rights law.[30]

In the International level there has been very important developments in the sphere of data protection which lead to a rapid growth in data protection legislation at the national and regional level.[31] States saw the need and the importance of having in place these reassurance for data subjects.

Chapter 2. The EU General Data Protection Regulation (GDPR)

A. What is new in the GDPR. [32]

Applies to data processors not just the controllers.	Data processors can be held directly liable if the company is found responsible for a breach. This was limited to data controllers under the EU Directive.
Records of processing activities.	Data controllers must maintain records of their processing activities.

[28]GA Res 71/199, 19 December 2016, < http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199 > accessed 27 November 2018.

[29]United Nations Human Rights Commitee Special repporteur on the right to privacy. < http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx > accessed 27 November 2018.

[30] Over 100 States have now enacted data protection laws. United Nations Conference on Trade and Development (UNCTAD), 'Data protection regulations and international data flows: Implications for Trade and Development', 2016, <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> (last accessed 19 January 2018), at 8.

[31] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 January 2019.

[32]NTT Security, The international impact and opportunity of the General Data Protection Regulation (GDPR) (2017) < https://www.nttsecurity.com/docs/librariesprovider3/resources/global_thought_leadership_gdpr_uea_v4>, accessed 4 February 2019.

Accountability.	Organizations must demonstrate how they comply with GDPR and document what personal identifiable data they have and why.
Data protection impact assessments.	These must be carried out to consider an individual's privacy when and organization is creating or updating a product or service that includes processing likely to result in a high risk to the rights and freedoms of data subjects.
Higher standards of consent.	Consent by data subject must be freely given and based on clear, easily available information about what they are agreeing to. It must be as easy to withdraw consent, as it is to give it.
Enhanced rights for individuals (data subjects' resident and/or citizens in the European Union).	Individuals have the right to be informed, object to processing and be forgotten (through erasure)- as well ad rights regarding access, rectifications on processing, data portability and automated decision making.
Data protection officer ("DPO").	A DPO is not mandatory for all organizations but a senior individual must be made responsible for GDPR compliance.
Breach Notification.	Organizations have the duty to report a breach of personal data within 72 hours and failure to do so may result in a fine.
Level of fines.	GDPR sees a significant increase in fines- up to 4% of global annual turnover.

B. Principles set by the GDPR.

GDPR is an EU Regulation that entered into force on 25th May 2018, it is directly applicable and does not require implementation into national laws. This legislation sets out some general principles in Article 5 (Principles relating to processing of personal data) that can be summarized as follow:

- The principle of "Lawfulness, fairness and transparency" → The processing of personal data is lawful only if it done in accordance with the laws, as laid down in the Union law or the Member State to which the controller is subject, data subject has given consent, pursues a legitimate purpose and is necessary in a democratic society in order to pursue such purposes.
- The principle of "limitation" → Personal data collected for a specific purpose is not further processed in a manner that is incompatible with those purposes. Also, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be done in accordance with Article 89(1) of GDPR.
- The principle of "data minimization" → Personal data is collected for adequate, relevant and limited only to what is necessary in relation to the purposes for which they are processed. Further unnecessary data are not allowed to be collected.
- The principle of "accuracy" → Every reasonable step must be taken to ensure that personal data should be accurate and where necessary, kept up to date. Inaccurate data information ought to be erased or corrected immediately.
- The principle of "storage limitation" → Personal data should not be stored beyond the time necessary and for the purposes for which the personal data are processed; Personal data may be stored for longer periods as long as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR.
- The principle of "integrity and confidentiality" → Personal data should be processed in a manner that ensures appropriate security, including protection against

unauthorized or unlawful processing and against accidental loss, destruction or damage.

- The principle of "accountability" → Controllers are responsible for complying with data protection law and the abovementioned principles while fulfilling their duties. They must promote, implement and safeguard data protection in their processing activities.

Chapter 3. The relationship between IOs and GDPR.

A. The definition of IOs according to the GDPR.

Even though there are many IOs working in numerous fields of life there is no universally accepted definition of what an IO is. However, there are some widely accepted concepts that need to be fulfilled in order for an Organization to be considered as an IO. These criteria can be summarized as the following:

a) An IO is created in the basis of a treaty between the States and should be governed under Public International Law.
b) The members of such organizations are States and possibly other subjects.
c) The organization has its own organs and institutional structure, which is different and separate of those of a State.
d) The organization possesses international legal personality.

All of the abovementioned criteria should be met. If one of the criteria is not fulfilled then, the Organization at stake is not considered as an IO.

GDPR presents a slightly different definition of what an IO is. This definition is only introduced in Article 4 (26) of the GDPR where an IO is defined as "an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries".

Although this definition was only introduced later on, by the Council, and not in the original proposal coming from the European Commission[33] it clearly states all the criteria of what an IO is. There is a huge difference between the four criteria's that an Organization should fulfil in order to be recognized as an IO, and the definition brought by the Council.

a) Firstly, the GDPR does not foresee the criteria that an IO should hold an international legal personality. This is a very important aspect because having legal personality means that the IO possess international rights and obligations in their own name, as opposed to in the name of the member States.
b) Secondly the criteria that an IO should have its own organs and institutional structure which should differ from its member states is also missing in the definition of IO in the GDPR.

Talking these into consideration we can say that the way GDPR defines IO is broader and fits more organizations under this umbrella than the broadly accepted criteria mentioned above. This means that even though an Organization is not governed by International law and does not possess legal personality can still be considered as an IO and therefore should be treated as an IO.

B. The relationship between EU Law and IOs

Since GDPR is part of the EU law, the CJEU in many cases has ruled that EU law must be interpreted, and its scope should be limited, in the light of the relevant rules of international law, including customary international law[34]. Rules of international law are binding on the EU and form part of the European Union's legal order, and the "European Community must respect international law in the exercise of its powers it is therefore required to comply with the rules of customary international law when adopting a regulation.[35]

[33] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General data protection regulation), 25 January 2012, COM(2012) 11 final. < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN > accessed 2 December 2018.
[34] (1992) Case C-286/90
[35] (1998) Case C-162/96

Therefore, even though the applicability of EU law toward an IO cannot be excluded a priori it must be analysed in a case-by-case basis, based on the contents of the EU substantive law itself, this analysis also has to consider the relevant rules of international law. International law, both treaties law and customary international law, widely recognize the privileges and immunities of IOs, and it is therefore likely that EU law, just as national law, would have to be applied in the light of privileges and immunities granted to IOs.[36]

This can be understood as that, normally EU law should be applicable towards IOs and it should not be excluded as an argument, but this isn't always the case. It needs to be determined based on the EU law provisions concerned, and on the basis of the specific provisions that apply to the IOs such as the privileges and immunities that are granted to the specific IO. The same conclusion would be also for the national law. All the provisions would apply unless specific privileges and immunities apply to it.

Thus, determining whether the GDPR applies to IOs should be based on its material and territorial scope, viewed considering any privileges and immunities that an IO may enjoy and the status of international law in the European Union ("EU") legal order.[37]

Since IOs differ in their structure and functions, application of the GDPR will also depend on their individual characteristics.[38] International treaties or customary international law may prevent the application of the GDPR to IOs in many cases, and the GDPR will generally not be enforceable against them, but this is based on the relevant rules of international law and EU law rather than because the GDPR automatically excludes IOs in all cases.[39]

This is a complex issue looking at all the pieces together, where GDPR stands, what is its scope of application and the relevant place is has in EU law and International Law.

---

[36] Baudouin Heuninckx, The law of collaborative defence procurement through international Organisations in the European Union (July 2011)
<https://www.nottingham.ac.uk/pprg/documentsarchive/phdtheses/heuninckxthesiscompletefinal.pdf> accessed 4 February 2018

[37] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019.

[38] ibid

[39] ibid

i. Does GDPR exclude IOs from its scope of application?

Both, Article 2 (Material Scope) and Article 3 (Territorial scope), do not mention IOs directly as subjects of the GDPR but it also does not exclude them explicitly either. The fact that the position of IOs in this Regulation is not well established brings a lot of challenges to companies that want to enter in contracts with IOs and to the Organization itself because it is risky to take one stand when they are not certain if that is the right way "to-go".

There can be several arguments that might be posed both in favour and against and IO being direct subject of the Regulation, and this list is not intended as a non-exhaustive one, but rather posing different perspective and views.

The following arguments exclude the fact that IOs are direct subject of GDPR and therefor they do not need to follow the rules set in this Regulation.

- Article 2 and 3 of GDPR do not mention specifically IO as subjects that need to comply with this Regulation;
- IOs seems to be placed in the same level as third countries. They are treated as subjects to a body of law which is not EU law;
- Throughout the Regulation, legal obligations are not posed to IOs. The only time IO are required to comply with GDPR in under Article 44, which requires that all transfers of personal data should be done in accordance with the GDPR including the case when the IO transfers data to a third country.
- Considering the fact that IOs are excluded from national jurisdiction (as part of their privileges and immunities) they are bound only by their internal rules and regulations, and States are in full agreement with this fact. Therefore it is important if the Organisation has policies in place that put clear guidance on how to protect personal data.

On the other hand, all the above-mentioned arguments have counterarguments that can be summarized as the following:

- It is true that IO are not specifically mentioned as subjects to the GDPR, but Article 2 already sets a list under which cases this Regulation is not applicable. This means that

if the legislator wanted to exclude IOs from the scope of GDPR it should have been easily done in this article.

- Even though IOs and third countries are placed in the same level this does not mean that they have both the same legal status. States have privileges and immunities in place which are governed by the principle of reciprocity, when as for IOs privileges and immunities are granted by the State because of the mandate that an IO has, and not because of the 'reciprocity' principle.
- Even if the only time that GDPR poses obligation to the IOs in under Article 44, as mentioned earlier, IOs closely cooperate with many companies that are subject to the GDPR therefor they need to fulfil all the obligation posed to them by the Regulation. In order for IOs to be able to continue working with these companies, indirectly, they need to have some adequate level of data protection in place. This should be subject for the Commission to determine whether this level of protection is adequate or not.

As has been previously discussed, Article 2 (1) determines the material scope of GDPR. This article underlines that GDPR applies only "to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system"[40].

Article 2 (2) also provides some exceptions from its scope of application but none of them is relevant in the cases of IOs because the GDPR does not apply to law enforcement activities, national security, data processing by EU entities, and purely personal and household activities (activities most of IOs conduct). However, the so-called 'Law Enforcement Data Protection Directive', which covers law enforcement activities, contains several provisions referring to international organizations that are similar to those in the GDPR. Directive (EU) 2016/680[41] 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 by competent authorities for the

[40] Article 2(1) GDPR

[41] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data[42].

Although GDPR does offer a broader definition of "data processing" in Article 4 (2) namely that data processing "means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

When looking at this broad definition, even though IOs don't fall under the exceptions of Article 2(2), almost all of the operations that might be performed by an IO on the data they hold, while fulfilling their mandate, might be the ones explained in this article.

Regarding its territorial scope, GDPR determined Article 3(1) states that it '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'.

Still this is too broad because the main question is that of "what qualifies as an "Establishment"? There is no answer in the Articles of the GDPR, namely Article 4 but Recital 22 tries to bring a kind of definition and states the following:

"Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

Keeping in mind that some IOs have establishments, missions, offices or even headquarters within the Union, this would automatically this IO would qualify as having an establishment within the Union. Under Article 3(2), the GDPR may also apply to processing carried out by data controllers and data processors without an EU establishment when the processing activities are related to 'the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union' or to 'the monitoring of their behaviour as far as their behaviour takes place within the Union'.[43]

[42] ibid

[43] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019.

An important case that should be noted in these situations is the "*Google Spain*" case. *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*[44] → This case took place in the year 2014 and was ruled under the old Data Protection law, Directive 95/46 on the Protection of individuals with regards to the processing of personal data and the freedom of such data. With all the debates that this decision brought it is still considered very relevant in the field of data protection for all the arguments that the CJEU made. Even though this case does not have an IO as part of the proceedings there are some relevant findings by the CJEU that can be used as an argument in the cases of data protection in IOs.

The CJEU found that EU data protection law grants individuals a right to suppress search engine results against a company with an establishment in the EU, even though the servers on which the search engine operated were based in a third country and were operated by the company's parent entity, since the activities of the entities were 'inextricably linked'.[45]

Even thought, as already mentioned, there is not a direct link between the Google Spain case and IOs, the stand that the court takes is very "Data Subject friendly". This way data subject can be potentially subject of the GDPR and might fall under both, territorial and material scope of application. Under the rationale of Google Spain, an IOs establishment in the EU could also be found subject to the GDPR with regard to activities carried out by a non-EU entity of the IO when such activities are found to be inextricably linked with those of the EU establishment.[46]

[44] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (May 13, 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN
[45] Ibid
[46] Ibid para 56.

Also, those IOs or their entities that are not established in the Union, could potentially still fall under the scope of the GDPR in the cases when they interact with Union individuals (not necessary citizens) as described in Article 3(2) of the GDPR.

Chapter 4. Privileges and Immunities of IOs.

IOs might fall within the material scope of the GDPR as set out in article 2, when they engage in the processing of personal data. IOs can also fall under territorial scope of GDPR as set out in article 3, when such processing is carried out in the context of the activities in the Union. Even if data processing by IOs falls within the material and territorial scope of the GDPR, there is still a big loop of what is called "privileges and immunities" that IOs enjoy.

GDPR does not mention in any of its articles the privileges and immunities that an IO has been given by its Member States, in order to fulfil its mandate, and how these privileges and immunities can affect the applicability of GDPR towards IOs. This requires an analysis of what kind of privileges and immunities IOs enjoy and until what extend they go.

A. Domestic Legal personality.

In some cases, IOs enjoy domestic legal personality within the territory of one or more-member states, which is part of their constitution documents. In accordance with Article 104 of Charter of the United Nations[47] ("UN Charter"), the 'Organization shall enjoy in the territory of each of its Member States ("MS") such legal capacity as may be necessary for the exercise of its functions and the fulfilment of its purposes'.

This means that sometimes this domestic legal capacity can be functionally limited in its nature. Sometimes, some constituent treaties speak of 'full' or 'most extensive' legal personalities and add examples of specific capabilities, such as for example article IX section 2 Articles of Agreement of the International Monetary Fund and article VII section 2 of the Agreement of the international Bank of Reconstruction and Development which provide 'The Fund/ Bank shall possess full jurisdictional personality and, in particular, the capacity; (i) to

[47] United Nations, Charter of the United Nations, 24 October 1945, <http://www.un.org/en/charter-united-nations/ > accessed 4 February 2019.

contract, (ii)to acquire and dispose of immovable and movable property; and (iii) to institute legal proceedings.'

From the example above, we can see that these privileges and immunities still remain in that of a functional nature. Domestic legal personality is not such a clear matter in countries which neither member states of a particular IO nor bound to accord domestic legal personality in a host or headquarters agreement.[48] In such cases the domestic courts may be relying in the customary international law or private international law principles through which the domestic legal personality enjoyed by an IO in a member state country might be recognized. In such cases the domestic courts can also seek the help and guidance from foreign court decisions.

B. Privileges and Immunities in the international level.

In the same argument as for the domestic legal capacity, IOs are granted privileges and immunities through numerous constituent's instruments of international law, giving them privileges and immunities that are necessary for them to fulfil their mandate as given by its MS. The privileges and immunities derive from article 105 (1) of the UN Charter which states that 'The organization shall enjoy in the territory of each MS such privileges and immunities as are necessary for the fulfilment of its purposes'.

These provisions are also contained in the constituent treaties of most other organizations that are set up after 1945 like for example, Article 67(a) of WHO Constitution where it is stated that 'The organization shall enjoy in the territory of each MS such privileges and immunities as are necessary for the fulfilment of its objective and for the exercise of its function'.

Immunities comprise a number of exemptions from the powers of a state.[49] In reality, the most important immunity that IOs enjoy is the **exemption from legal process**, the so-called jurisdictional immunity, which usually comes in a "package" with the exemption from the **enforcement measures**. But what does this include? This is quite difficult. This depends on the treaty by treaty basis.

48 The Privileges and Immunities of International Organizations in Domestic Courts, <https://global.oup.com/academic/product/the-privileges-and-immunities-of-international-organizations-in-domestic-courts-9780199679409?cc=at&lang=en&> accessed 4 February 2019.

49 ibid

The main consequent of this immunity is that, even if IOs need to comply with GDPR who will be the authority that will 'make sure' that the IO in stake is indeed fulfilling its obligations towards data protection.

C. Privileges and Immunities in the EU level.

Considering that the GDPR is an instrument of EU law raises questions about whether privileges and immunities granted by the Member States to IOs can be binding with regard to EU law as well. In the case of 'Air Transport Association of America' the court said that

'It should also be pointed out that, by virtue of Article 216(2) TFEU, where international agreements are concluded by the European Union they are binding upon its institutions and, consequently, they prevail over acts of the European Union'.[50]

This conclusion of the Court gives the understanding that international agreements of the EU generally override EU legislation, but in the cases of the agreements that grant privileges and immunities to different IOs that are concluded between the IO and the Member State, the priority that this agreement has over EU legislation prevails over that acts of the EU.

As for a fact, under EU law there is NO international agreement that deals with the privileges and immunities of an IO. EU primary law only mentions in Protocol no.7 on the privileges and immunities of the EU [51] states that:

'The Member State in whose territory the Union has its seat shall accord the customary diplomatic immunities and privileges to missions of third countries accredited to the Union.'

Since the main seat of the EU is situated in Belgium, these privileges and immunities are accorded by Belgium rather than by the EU, as an institution itself. However, this document does not mention any references for the IOs an how such cases should be dealt.

The EU is also not a party to the 1946 Convention on the Privileges and Immunities of the United Nations or the 1947 Convention on the Privileges and Immunities of the Specialized Agencies.[52] However, the details of the relations between the EU and IOs are often very hard

[50] 2011 C-366/10

[51] Protocol No. 7 on the Privileges and Immunities of the European Union, OJ 2010 C 83/266, Article 16; Wouters and Duquet, 'The EU and International Diplomatic Law: New Horizons?', 7 The Hague Journal of Diplomacy (2012) 31, at 33-34.

[52] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019.

to access and sometimes even impossible because as they are set out in form of an exchanges of letters, informal working arrangements, or administrative agreements, which do not necessarily need to be published in the EU Official Journal. What can be easily noticed is that also the agreements signed between Member States and IOs seems not to make reference to the EU law explicitly. For example, the agreement concluded between INTERPOL and France (HQ agreement) [53] and also the agreement between OPEC and Austria[54] do not have any reference to EU law as such.

What seems to be an issue in practice, is the fact that also the CJEU has not issued yet a clear guide on the status of privileges and immunities of IOs with respect to EU law. However, there are several theories under which it could be argued that those privileges and immunities granted to IOs by the Member States should be binding on the EU level as well.[55]

a) The EU is bound by international law, in that when it adopts an act it shall observe international law 'in its entirety, including customary international law, which is binding upon the institutions of the European union'.[56] This commitment is expressed in Article 3(5) of the Treaty of European Union (TEU), which provides that 'the EU shall uphold and promote … the strict observance and the development of international law'. Yet, despite the periodic treaty revision, EU law is still not explicit about the relationship between international law and EU law.[57]

[53] Accord entre l'Organisation Internationale de Police Criminelle—INTERPOL (O.I.P.C.- INTERPOL) et le Gouvernement de la République Française relatif au siège de l'organisation sur le territoire française, 14 April 2008, <https://www.interpol.int/content/download/9747/420416/version/7/file/AccordSiegeRevise2008FR.pdf> (last accessed 1 September 2017), at Article 5.

[54] Agreement between the Republic of Austria and the Organization of the Petroleum Exporting Countries regarding the Headquarters of the Organization of the Petroleum Exporting Countries, 18 February 1974, <http://ilmc.univie.ac.at/uploads/media/HQ_Agreement_OPEC_-_Austria.pdf> (last accessed 1 September 2017), at para. 5(2), stating that 'The service of legal process, including the seizure of private property, shall not take place within the headquarters seat except with the express consent of, and under conditions approved by, the Secretary General', without referring to a particular body of law that is covered by the immunities.

[55] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019.

[56] The Meso Level: Means of Interaction between EU and International Law: Customary International Law as a Source of EU Law: A Two-Way Fertilization Route?
Theodore Konstadinides 14 October 2016 https://academic.oup.com/yel/article-abstract/35/1/513/2549066?redirectedFrom=PDF

[57] ibid

Since the customary international law is binding on the EU, this means that the agreements between Member States and IOs granting privileges and immunities to IOs could be binding. The only condition is that they need to be found to be embodied as customary law. Most likely that this is found to be customary law is an IO that has a universal character such as the UN or its specialized agencies, or IOs like ICRC that have attained the status of customary international law, which was received under the Geneva Convention that mentions that 'who would recognize as binding on the EU agreements entered into by Member States if they are 'generally accepted' conventions of a 'law-making nature' which constitute 'general (customary) international law'. However, as already explained, in many cases the precise scope of an IOs privileges and immunities cannot be derived solely from customary international law.[58]

b) Another argument that can be posed would be in the cases that, specific organizations whose status is widely accepted and recognized under International Law, the agreements granting privileges and immunities to IOs should be binding in the EU level as well. Article 3 (5) of TEU writes that 'Union shall uphold and promote its values …. as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter'.[59] This means that EU should respect and uphold the principles of the Charter, therefore this should apply to the privileges and immunities UN as a whole including the specialized agencies, enjoy in the territory of member state privileges and immunities necessary to fulfil its mandate. Keeping in mind that all EU member states are UN member states as well.

[58] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019.

[59] European Union, Consolidated version of the Treaty on the Functioning of the European Union, 13 December 2007, 2008/C 115/01, <https://www.refworld.org/docid/4b17a07e2.html> accessed 4 February 2019]

c) EU is empowered to conclude agreements and arrangements with third countries and IOs in the field of humanitarian aid as described by article 214 of the TFEU[60] and article 21 of TEU. [61]

d) Article 4 (3) of TEU[62] mentions the principle of sincere cooperation between Member States and EU. The concept of privileges and immunities that Member States grant to IOs can also be interpreted in light of this principle. Failing to recognize the immunities granted bilaterally to IOs by Member States with respect to EU law could create conflicts between international law and EU law, such as if EU law were to apply to an activity for which privileges and immunities had been granted by treaty between an IO and a Member State.[63] The CJEU has also held that '…In view of the customary principle of good faith, which forms part of general international law…' it can be that the rules of GDPR may be interpreted consistently with the privileges and immunities that the Member States have granted to IOs. Not to mention that almost all EU member states have entered into such agreements granting privileges and immunities to IOs.

e) Finally, the CJEU has held that the EU may succeed the Member States with regard to obligations in international agreements they have entered into in certain situations when they have transferred powers to the EU.[64] However, succession is only possible when the EU 'has assumed all the powers exercised by the Member States that fall

---

[60] Article 214 TFEU→ The Union may conclude with third countries and competent international organizations any agreement helping to achieve the objectives referred to in paragraph 1 and in Article 21 of the Treaty on European Union.
<http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments/part-5-external-action-by-the-union/title-3-cooperation-with-third-countries-and-humantarian-aid/chapter-3-humanitarian-aid/502-article-214.html >

[61] Article 21 TEU → The Union shall seek to develop relations and build partnerships with third countries, and international, regional or global organizations which share the principles referred to in the first subparagraph. It shall promote multilateral solutions to common problems, in particular in the framework of the United Nations. < http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-european-union-and-comments/title-5-general-provisions-on-the-unions-external-action-and-specific-provisions/chapter-1-general-provisions-on-the-unions-external-action/101-article-21.html >

[62] Article 4 (3) → . Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.
<http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-european-union-and-comments/title-1-common-provisions/5-article-4.html

[63] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019.

[64] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019.

within the Convention in question', which is not the case with regard to privileges and immunities of IOs.[65]

Chapter 5. Legal compliance and International Data Transfers.

Given the enormous influence that GDPR had over Europe and the world all around it is a key point to discusses through which the GDPR can allow transfer outside the EU. GDPR sets five (5) key elements in order to allow data transfers outside the EU and those can be concluded as;

1. consent,
2. adequacy,
3. standard contractual clauses,
4. binding corporate rules, and
5. codes of conduct.

There are also the additional obligations such as those related to record-keeping, that are required when transfer occurs Article 30(1)(e), (2)(c).

Data subjects should receive full information on where his/her data is being transferred, what is the legal situation in the country the data is being transferred (does the country provide adequate legal protection on personal data), what are the risks that the data subject should bare in case he/she gives the consent that such transfer takes place. It is important to realize that the consent should be freely given, and it should not be imposed.

A. Information about possible transfer of personal data to IOs

The basic requirements for obtaining a valid legal consent are defined in Article 7 and recital 32 of the GDPR. 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement'.[66] The element "free" implies the ability to choose by the data subject if they want to give the consent and they are not forced to do so.

[65] Ibid.
[66] Recital 32 GDPR.

Any element of inappropriate pressure or influence which could affect the outcome of that choice renders the consent invalid.[67]

Data subject should not be put under pressure to give the consent and they should be presented with the opportunity that they can withdraw their consent anytime.

So, from all of the above, data subject should be made aware of all possible transfers that might happen with the personal data and this includes also the cases when the data controller decides to transfer the data to an IO. Article 44 sets out that if 'any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization. All provisions in Chapter V shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined'.

There are several articles in the GDPR that deal with the cases of possible transfer of data from the controller to an IO as set below:

1- Article 13 (1)(f) foresee the cases that the data controller intends to transfer the data subject's personal data to IOs. In every case the data subject should be notified and provided with the relevant information regarding the existence or absence of an adequacy decision by the Commission as set out in article 45 of GDPR, or in the case of transfers referred to in article 46 (transfers subjects to appropriate safeguards) or article 47 (binding corporate rules), or the second subparagraph of article 49 (1) that foresees the cases when personal data can be transfer only if:

   a) the transfer in not repetitive,

   b) concerns only a limited number of data subjects,

[67] Mark Philip, International Data sharing norms: from OECD to the general data protection regulation (GDPR) Published online 1 august 2018; < https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6132662/> accessed 4 February 2018.

c) is 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,

d) the controller has assessed all the circumstances surrounding the data transfer

e) has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

2- Article 14(1)(f)→ where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organization and the existence or absence of an adequacy decision by the Commission as set out in article 45 of GDPR, or in the case where there is not a Commissions decision, reference to the appropriate or suitable safeguards should be made and the means to obtain a copy of them or where they have been made available.[68]

3- Article 28 (3)(a)→ data processors may only transfer personal data to IOs in the based-on document instructions from the data controller, unless they are required to do so by EU or Member State law.[69]

Article 15 (1)(c) foresees that data subject has the right to learn from the data controller if his/her personal data has been disclosed to any IO during anytime and in the cases that the personal has been indeed already disclosed to an IO, data subject, in accordance with article 15 (2), has the right to request the appropriate safeguards that were used for such transfer.

All in all, data subject should always be informed how their data is being used, processed and later on shared in all cases and times. The consent should be given explicitly when the data is foreseen to be shared with an IO, and it should not be forced upon the data subject but should be given freely. Article 7 should be taken into account when asking for the data subject's consent. The data subject shall have the right to withdraw his/her consent at any time[70].

[68] Article 4 of GDPR.
[69] Article 28 (3)(a)
[70] Article 7 GDPR

B. Data Transfer during the everyday work of the IOs.

Taking into consideration the size of some IOs such as UN, Organization for Security and Cooperation in Europe ('OSCE') etc. and the States that they work in (for example a Mission, Presence, Office etc. is established there), sometimes data protection can get "tricky". One perfect example to illustrate this will be the following scenario:[71]

Imagine an IO such as the OSCE, is going to implement a project in the Republic of Tajikistan.[72] According to the European Commission, Tajikistan is not considered as a country that ensures an adequate level of protection on data protection.[73] The OSCE has a Field Mission established in the Republic of Tajikistan namely "OSCE Programme Office in Dushanbe".

Let's suppose that the Programme Director is seated in the Headquarters ("HQ") of the OSCE in Vienna, Austria, and the Programme Office has entered into an agreement with a Union based company to act as the Implementing Partner which is responsible for implementing the project in the Republic of Tajikistan. On a daily basis it is required that information should be exchanged between the Programme Office in Dushanbe, the HQ and the Implementing Partner to track the progress of the project implementation. Theoretically this is as easy as a "button click" in the mouse, but according to the GDPR, this situation requires a lot of settled rules and laws.

The possible things that can "go wrong" in the abovementioned examples are for example:

1. The Implementing Partner, since is a Union based company, needs to comply with GDPR because it falls under the requirement set in Article 3 (Territorial Scope). Since IOs are not mentioned in Article 3 of GDPR it might be safe to say that IOs are not subject to the GDPR one will think. The problem with the statement lies within the following Articles of the GDPR, namely Article 44 where IOs are mentioned as already stated earlier.

[71] This is a fiction scenario.
[72] This case is not real. It is taken only as an example.
[73] European Commission; Adequacy of the protection of personal data in non-EU countries < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en> accessed 4 February 2019

2. Transferring data between the HQ and the Programme Office in Dushanbe is subject to the GDPR as such. Since the Republic of Tajikistan is considered as not having adequate protection in place the possibility to transfer the data immediately will be of a risk therefore it will require exceptional basic to be allowed to transfer this data.

An IO, even if it has several Offices in different parts of the world, they all are part of one

Organization, meaning that all the Offices fall under the same rules, regulations and policies. If and IO has policies in place that protect personal data, normally, it should not be a problem to transfer information form one Office to another if this information stays within the Organization. The different Offices should be perceived as one big Organization.

i. Data Transfer in the humanitarian sector.

The issue of personal data transfers becomes even more sensitive in the cases of humanitarian actions. IOs in order to fulfil their mandate will need to collect and process an enormous amount of personal data. The sensitivity of the data collected by IOs engaged in the humanitarian sector is very delicate, therefore IOs should be very careful when engaging in such activities.

When in this case, it is of a general belief that the GDPR tends to make it easier for IOs engaging in the humanitarian sector to process personal data based on legal bases such as for example in the basis of "public interest" or because processing such data will be in the vital interests of data subjects concerned or another natural person. Recital 46 explains that 'some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters'.

In the cases when processing of personal data, based on the vital interest of another natural person takes place, should only be performed in the cases where the processing cannot be manifestly based on another legal basis, and no other cases. This Recital does not explicitly refer to IOs, but, in many cases IOs will carry out these kinds of transfers in the situations to which applies for the reasons that are already mentioned above.

The GDPR continues with Recital 112 where it states that 'any transfer to an international humanitarian organization of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject'.

As already mentioned, even though these recitals and articles are not directly linked, or specifically mentioning IOs, parallels can be drawn, and these provisions might be applicable in such situations as well.

C. The Adequacy decision.

As was mentioned several times throughout the document, the GDPR only poses legal obligations towards IOs under Chapter V, more specifically the obligations mentioned in article 44. In order for personal data to be transferred to an IO, the Commission should be responsible in deciding whether or not the IO in question ensures an adequate level of protection of personal data. If the IO is found to have an adequate level of protection in place, such a transfer of personal data shall not require any specific authorization but can be transferred immediately without further complications.

But the question rises that what are the criteria's that the Commission uses in order to determine if a specific IO has or has not an adequate level of protection in place?

In accordance with article 45 paragraph 2, when assessing the level of protection that an IO should have in place, the Commission should measure the following criteria's:

a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defines, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to an IO which are compiled within that IO, case-law, 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;[74]

b) the existence and effective functioning of one or more independent supervisory authorities to which an IO is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States;[75] and

c) the international commitments the IO concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.[76]

After the Commission having assessed the adequacy of the level of protection that the specific IO has in place, may decide, by means of implementing act that the Organisation ensures an adequate level of protection within the meaning of article 45 paragraph 2. The implementing act, is the act that Commission issues that provides a mechanism for a periodic review. This means that the IO should pass the assessment of the level of protection at least every four years, and it is not in a one-time basis. This periodic assessment shall take into account all relevant developments in the IO, meaning reviews of their data protection policies, relevant developments in regard to cases that might have been filed during this period.

The implementing act shall be very specific in regard to its territorial and sectoral application and, where applicable, it needs to specifically identify the supervisory authority or authorities.[77] The Commission shall monitor developments in the IO on an ongoing basis and should assess if any recent development might affect the assessment that the Commission gave to this IO as having adequate level of protection.

In the cases that the Commission finds that the IO does not fulfil the elements as set by article 45 paragraph 2 and no longer ensures and adequate level of protection, the Commission can repeal, amend or suspend the decision of granting the IO the implementing acts without retro-active effect consequent to this the transfer of the personal data should be prohibited.

74 Article 45 2 (a) GDPR
75 Article 45 2 (b) GDPR
[76] Article 45 2 (c) GDPR
77 Article 2 paragraph 2 point (b) GDPR

In cases that the IO fulfils the requirements of having appropriate safeguards and derogation from specific situations, the transfer of personal data might take place in consultation with the Commission. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorized by a supervisory authority.[78] Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country.[79]

In the absence of an adequacy decision or of appropriate safeguards, GDPR has set a strict corpse of rules under which a transfer of personal data to an IO might take place. The conditions are as follows:

a) the data subject should have consented explicitly to the proposed transfer, and the other party should have informed the data subject of all the possible risks of such transfers because of the lack of an adequacy decision from the Commission and appropriate safeguards in place;
b) the cases when such transfer is necessary for carrying out a contract signed between the data subject and the controller or the implementation of pre-contractual measures taken only in the cases when the data subject has requested it.
c) Such transfer is necessary to conclude or perform a contract concluded in the interest of the data subject. Such contract should be between the controller and another natural or legal person;
d) the transfer is important for reasons of public interest and such interest shall be recognized in the Union law or in the law of the Member State to which the controller is subject.
e) the transfer of personal data is necessary for the establishment, exercise or defence of legal claims in the court of law;

78 Recital 108 GDPR
79 ibid

f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, only in the cases where the data subject is physically or legally incapable of giving explicit consent;

g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case;[80]

h) In the cases that none of the above criteria in fulfilled, the transfer might take place only if the transfer is not repetitive, it concerns only a limited number of data subjects. What should also be considered is that this transfer is 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, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The data subject should also be notified for this transfer.

Chapter 6. Enforcement of the GDPR

There are two different concepts that need to be distinguished from one another when it comes to the enforcement and the application of the GDPR.

- "application of the GDPR" is explained as the binding nature of the regulation toward IOs. In simple words meaning that the IO should comply or not with the GDPR.
- "enforcement of the GDPR" one should understand the authority which is responsible for the monitoring of how the IO is committing to these rules and how it is "putting those into practice".

GDPR has already created the "Supervisory authority" which according to the regulation "shall be competent for the performance of the tasks assigned to and the exercise

80 Article 49 GDPR.

of the powers conferred on it in accordance with this Regulation on the territory of its own Member State'.[81]

The Supervisory authority is responsible to monitor and enforce the application of the GDPR and fulfil all the tasks as described in article 57 of the Regulation. It is decided that also individuals will have the right to a judicial remedy against data controllers and data processors, which means that they can sue directly and enforce their rights in the court of law.

As already discussed above, the problem lies within the "Privileges and Immunities" that IOs enjoy in the national jurisdiction. One of them is the "immunities against legal process" which is a fairly common immunity that IOs enjoy across different countries. This is a very important remedy that IO have that gives them the "freedom" in their everyday work, but when it comes to the protection of personal data and enforcement of the law, it gets tricky.

Because of the privileges and immunities, even in the cases that it is found that GDPR applies to the IO, then enforcement by a National Supervisory Authority or court would not be possible because the IO enjoys privileges and immunities within the territory of the specific state.

EU law such as the GDPR becomes part of the legal order of the Member States, and immunities granted on a national level should also apply under the GDPR when a Supervisory Authority or National court conducts enforcement action against the IO.[82] Since most enforcement of the GDPR will be carried out at the national level, this means that in practice, IOs will be protected against it by the immunities they enjoy,[83] and the decision cannot be enforced in this level.

Article 68 of the GDPR deals with the European Data Protection board ("The board") and the responsibilities that the Board has. The Board, as represented by its Chair, is established as a body of the EU and enjoys legal personality.[84] According to the GDPR, the decision of the board has a binding nature and can be challenged in the Court under the procedures set out in the TFEU.[85]

---

[81] Article 55 GDPR

[82] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 4 February 2019.

83 ibid

84 Article 68 (1) GDPR

85 Article 263 TFEU Recital 143 GDPR

The GDPR sets out the 'consistency mechanism' concept which ensures the consistent application of the GDPR throughout the Union. The consistency mechanism should be respected in the cases where there is an undergoing dispute between Supervisory Authorities.[86]

Also, in the cases when there is an urgent need to act to protect the rights and freedoms of data subjects as set out in article 66 of the GDPR, for example when 'in exceptional circumstances', a data protection authority (Supervisory Authority) believes it is urgent and necessary to protect individual rights (Article 60(11)); or the cases when a data protection authority fails to grant mutual assistance (Article 61(8)); and lastly when a data protection authority does not comply with a decision issued by the lead data protection authority (Article 62(7)), should the consistency mechanism be respected.

In the cases when the Board has to issue legally binding decisions that address to national data protection authority it is considered to be the lead supervisory authority as set out in article 56 of GDPR, as well as to all other data protection authorities concerned.

All the final decisions coming from the data protection authorities have to be adjusted to the decision of the Board without delay in accordance with article 65 (6) of the GDPR. There is a two-step process put in place, under which:

1- Firstly, the Board will first issue its decision,
2- Secondly the national data protection authorities are supposed to 'convert it' into national law by adopting their own decisions consistent with that of the Board.

The situations when and IO is involved is a little different. An enforcement action towards an IO is more likely to be taken by a national data protection authority, which means in a national level, any enforcement based on a decision by the EDPB would also be foreclosed by the jurisdictional immunities that an IO enjoys under Member State law.[87]

Last but not lease, IOs may come under "informal" type of pressure to adopt EU data protection standards, which can happen when EU law makes access to resources or benefits conditional on compliance with the its policy requirements (which may be referred to as

86 Article 65/1 GDPR

87 Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019

'conditionality' or 'soft enforcement').[88] This kind of informal pressure has led many commercial actors and global companies to adapting their internal company rules in compliance with the EU data protection laws. Another big actor that has been pressured to comply with the GDPR is the data exporters, that have had to change and adopt their data privacy policy to comply with the standards set out in the GDPR by the EU. In some cases, there has been requirements from them towards IO that receive data from the EU to implement suitable safeguards in order for a transfer of data to take place.

Chapter 7. Legal conflicts

Flows of personal data to and from countries outside the Union and international organizations are necessary for the expansion of international trade and international cooperation[89]. As already mentioned throughout this document, there are some potential legal conflicts that might rise that are clearly demonstrated in Article 44 GDPR. The reason why this legal conflict stands is because, article 44 in itself, addresses the data controllers and data processors that carry out international data transfers and does not address IO tas such.

Article 44 requires that "any transfer of personal data which are undergoing processing or are intended for processing after transfer to an IO shall take place only if the conditions laid down in the GDPRR are complied with by the controller and processor, including for onward transfers of personal data from the third country or an IO to another IO"[90].

Possible legal conflicts that could arise under article 44 of the GDPR, might be the following:

1- IO no. 1 which is established in the EU transfers personal data to IO no. 2 in a third country, or to another party in a third country.
2- IO no. 2 in a third country that has received personal data from IO no. 1 then transfers the data to another party (aside from an IO) outside the EU.

[88] ibid
[89] Recital 101 GDPR
[90] Article 44 GDPR

3- IO no. 2 in a third country that has received personal data from IO no. 1 then transfers the data to IO no. 3 outside the EU.[91]

These uncertainties make the work of the IO very hard and sometimes unpredictable.

It is generally believed that the transfer of data between IOs is to be governed by the provisions set out in the UN Charter ("The Charter") when we consider the UN or the Specialized Agencies, and all the treaties, international customary law or the organizations internal rules for all the other IOs.

On the other hand, article 44 of the GDPR sets out a clear rule when it comes to data transfers in the abovementioned scenarios that such transfer of data can only take place if the controller or processor fully comply with the rules and conditions set out in the GDPR because the level of protection of the data subject ensured in the Union should not be undermined in any circumstances.

But how can these rules apply in the situations mentioned above?

1. In the first situation, under the GDPR, data transfers are supposed to be carried out only under its terms, although IO no. 1 may contend that the GDPR should not apply to it in lights of its privileges and immunities.[92]
2. In situation 2, the conflict seems even more acute, because the data have left the territory of the EU and are now being processed by a party that is subject to law other than that of the EU.[93]
3. And in situation 3, if IO no. 2 or IO no. 3 enjoy privileges and immunities then there may be a clash between EU data protection law on the one hand and public international law on the other hand.[94]

What needs to be taken into consideration is the fact that the concept of the personal data protection is a fundamental human right[95] as set out in the EU legal system. As a fundamental

91 Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 4 February 2019.
92 ibid
93 ibid
94 ibid
95 Article 8 of the Charter of the fundamental rights of the European Union.

right, it shall have the same legal value as the Treaties[96] so it shall enjoy the status of primary law.

As was mentioned already, IOs are granted privileges and immunities by the states in the form of an international agreement, and in this moment the conflict arises. Thus, this might be resolved with the reasoning that since the international agreement overrides with that of a fundamental right, the fundamental right, specifically, the right to personal data protection, will be placed higher in the hierarchy as it is part of primary law. This gives the picture that the GDPR could potentially be seen as overriding rules of international law granting privileges and immunities to IOs if such rules were regarded as violating the fundamental right to data protection.[97]

EU law is still part of international law and there is a strong commitment in principle of the EU to international law at international level, as expressed in the dictum or the Court that the EU 'must respect international law in the exercise of its powers.'[98] There are aspects in which general international law stands less strongly in the relationship. They all concern the internal application of international law within the EU legal order and relate to direct effect, the hierarchy of international law and the possibility to derogate from EU law to honour international treaty obligations.[99]

Considering that there might be circumstances where EU law overrides International Law in the cases where the two clash, should be limited only to the situations where the core principles of data protection are at stake. Article 29 Working Party (the group of data protection authorities that is the predecessor to the EDPB) has also referred to a set of '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'.[100]

---

[96] Article 6 (1) TEU

[97] Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ < https://ssrn.com/abstract=3050675 > accessed 30 December 2019.

[98] Racke (n 15), para 55; Poulsen (n 15), para 9 f; C-405/92 Etablissements Armand Mondiet SA v Armement Islais SARL [1993] ECR I-6133, paras 13-15; Intertanko (n 23), para 51; Kadi I (n 1), para. 291 f; (n 15), para 101.

[99] Katja S. Ziegler The Relationship between EU Law and International Law (2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2373296 > Accessed 4 February 2019

[100] Article 29 GDPR

The commitment of the United Nations to human rights stems from the Organization's founding Charter.[101] Since personal data protection is set out as a fundamental right,[102] many UN organizations have already created some sort of "data protection policies" that set out rules and conditions under which the Organization can collect, retain, analyse and transfer the personal data.

For example, United Nations High Commissioner for Refugees ("UNHCR") has defined "data protection as part and parcel of refugee protection".[103] UNHCR claims that they are a "very data intensive organization. That means many UNHCR staff and colleagues and partner organizations need to process a lot of information on individual refugees, asylum-seekers, internally displaced persons, and other people whom we protect and assist – so-called personal data – in our daily work".[104]

It is normal practice that IOs enter into different types of contracts with companies and vendors to carry out, for example, maintenance work or any other jobs. In the cases where the company is located within the Union, or falls under the GDPR scope, it has to make sure that all the clauses in the regulation are fulfilled and the contract is in full compliance with the regulation.

To achieve this, the IO should reassure the vendors that it has policies in place that protect personal data and that there is no risk for the data in the cases that it will be transferred from the vendor to the IO. Since this is yet in the first steps of development, some IOs have presented certain clauses in their contracts where they state that both parties shall ensure that the personal data of the data subject is protected as set out in the internal rules and regulations of the IO at stake.

Some IOs, for example the OECD, have created strict policies, focusing in the following points:

---

[101] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), <https://www.refworld.org/docid/3ae6b3712c.html> accessed 4 February 2019

[102] European Commission, Data protection in the EU, <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en> accessed 4 February 2019

[103] UNHCR, Data protection is part and parcel of refugee protection, <https://www.unhcr.org/blogs/data-protection-part-parcel-refugee-protection/> accessed 4 February 2019

[104] Ibid

- The **volume of personal data** being collected, used and stored[105];
- The **range of analytics** involving personal data, providing insights into individual and group trends, movements, interests, and activities[106];
- The **value** of the societal and economic benefits enabled by new technologies and responsible uses of personal data[107];
- The extent of **threats** to privacy[108];
- The **number and variety of actors** capable of either putting privacy at risk or protecting privacy[109];
- The **frequency and complexity** of interactions involving personal data that individuals are expected to understand and negotiate;[110]
- The **global availability** of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows[111].

According to the GDPR, once an IO assures an adequate level a protection of the personal data, such transfers shall not require any specific authorization. Meaning that transfers can take place without further complications.

Conclusion

The international community has a duty to uphold and defend the fundamental human rights.[112] Data protection law emerged from the fundamental right to privacy, recognized in the Universal Declaration of Human Rights, other international and regional human rights instruments and national constitutions.[113]

---

[105] OECD, Data protection principles for the 21st century (2014) <https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf> accessed 4 February 2019

[106] ibid

[107] ibid

[108] ibid

[109] ibid

[110] The OECD privacy framework (2013) <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 4 February 2019

[111] ibid

[112] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), <https://www.refworld.org/docid/3ae6b3712c.html> accessed 4 February 2019

[113] UNHCR, Data protection is part and parcel of refugee protection, <https://www.unhcr.org/blogs/data-protection-part-parcel-refugee-protection/> accessed 4 February 2019

Personal Data is becoming more and more valuable[114] in the nowadays reality. The purpose of personal data protection isn't to just protect a person's data, but to protect the fundamental rights and the freedoms of persons that are related to that data.[115] Because of the increased importance of personal data, IOs play an important role in becoming "role models" in setting out standards for everyone to follow.

Some of the IOs have a complex structure, meaning that they have several HQ in many countries, including in the Union territory and outside. The cooperation and communication between the structures is essential for their work. With the GDPR entering into force, there have been many questions raising regarding the effects that the regulation has in this everyday work between the structures.

Even though there has been no update from the Commission in regard to whether GDPR applies to IOs and if they should comply with the regulation, knowing that processing of data is core for some IOs to fulfil their mandate,[116] data protection policies should be put in place and fundamental human rights should be safeguarded and respected in all aspects of their work. Reducing the possibility of data misuse and increasing the trust among the public should be in the centre of an IOs work.

The discussion if GDPR applies toward IOs is not that clear since the main aim of the Regulation is to impose rules and obligations towards the establishments in the Union, or not established in the Union but the processing of personal data is that of the Union's data subject, as set out in article 3, and not to impose rules and obligations against IO as such.

Normally, the conversation of GDPR posing legal obligations towards IOs should not be this complicated because of the 'special' nature IOs have. This only comes to life when most of the IOs enter into different contracts with companies and vendors, especially the ones that must comply with the regulation. As already mentioned, IO are bound by their own rules and regulations, and since this is the governing 'law', IOs should consider creating policies that are transparent enough, explaining what types of data is being collected, what is the purpose, how long is it retained etc.

[114] Three reasons why we need strict data protection regulations, (2018) <https://www.njordlaw.com/three-reasons-need-strict-data-protection-regulations/ > accessed 4 February 2019.
[115] ibid
[116] For ex. UNHCR, UNICEF etc.

Since GDPR is setting a new standard for data protection, and this standard is being followed by many other countries outside the Union, it is essential that their policies are driven by the GDPR rules, but IO do not necessarily need to comply with GDPR as such. Taking into consideration the complex nature of an IO, meaning the status that they have in each country with all the privileges and immunities that are granted to them by their member States to fulfil their mandate, and specifically when IOs are excluded from national jurisdiction, it will be hard for the regulation to apply.

Since in most of the cases IOs are excluded from national jurisdiction a data subject whose rights might have been violated, do not have the possibility to initiate a legal process in front of a national court.[117] IOs are bound to respect human rights law, and the right to a fair trial[118] is as much of a fundamental right as the right to data protection is, which makes the fact of having policies in place to protect the data subjects in such cases even more important and provide them with a platform to pursue a claim if their rights are violated. If these rights are violated, this can lead to denial of fundamental rights of the data subject in question. Because this risk is too high to bear from the IO, they should already have in place an alternative so that the data subject is not denied from exercising these rights.

All in all, as complex as this topic can be, it is important to understand that an IO even if it has several Offices, Missions and/or HQ in different locations, the internal rules, regulations and policies apply everywhere the same. IO should be seen as one no matter where it is located and when we pose the question 'Does GDPR apply to IOs' we have to see the IO as one with all its locations.

This matter should be seen and discussed keeping in mind that IOs work in different parts of the world (depending on the nature and the purpose of the organization) and not necessarily only in Europe. Therefore, before answering the question if GDPR applies toward IOs an analysis should be made on what the nature of GDPR is, what is the territorial scope, and what is the purpose of the Regulation. After having answered these questions, we should

[117]August Reinisch, The Immunity of International Organizations and the Jurisdiction of their Administrative Tribunals (2008) <https://deicl.univie.ac.at/fileadmin/user_upload/i_deicl/VR/VR_Personal/Reinisch/Publikationen/TheImmunityIOs_2008.pdf > accessed 4 February 2019.

[118]Article 6, Right to a fair trial, (2018) <https://www.equalityhumanrights.com/en/human-rights-act/article-6-right-fair-trial > accessed 4 February 2019.

go ahead and analyse the impact it would have if GDPR applies toward an IO and imposes legal obligations to it.

In this moment the 'to go' solution might be that IOs put together policies and rules that are clear, transparent and that respect fundamental human rights. It is important to notice that most of the IOs are only[119] bound by their internal rules and policies, therefor the way their rules are shaped is crucial for ensuring protection and respect of fundamental human rights. The wave that GDPR brought should be a 'wake up' call for everyone and not only for the subjects of the GDPR, to realize the current reality and the value that personal data has, and to find a way of moving forward.

Personal data is intimately linked to autonomy and human dignity, and the principle that everyone should be valued and respected[120]. For this principle to guide the development of today's information society[121], data protection must be rigorously applied by all the parties involved in collecting, processing, or retaining personal data.

[119] Emphasis added

[120] European Commission, Ethics and Data Protection (2018) <http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf> accessed 4 February 2019

[121] Ibid.

Bibliography

1- *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1.

2- UNCTAD, Data Protection Regulation and International Data Flows: implications for trade and development. (United Nations, 2016).

3- Collin Bennett and Charles Raab, The Government of Privacy: Policy Instrument in Global Perspective (MIT Press 2006) 93.

4- *EU Directive 95/46*: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31, Article 4.

5- "*What is personal data*?", European Commission <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en#references> accessed 25 November 2018.

6- Yearbook of International Organizations, *Open Yearbook*, <https://uia.org/ybio/> accessed 25 November 2018.

7- J.Klabbers, *An Introduction to International Organization Law* (CUP 3d ed., 2015), at 1 note 2 (Kindle edition), stating that estimates about the number of such IOs vary from 240 to 350; Christoper Kuner, International Organization and the EU General Data Protection Regulation (February 1,2018). University of Cambridge Faculty of Law Research Paper Nr. 20/2018/ <https://ssrn.com/abstract=3050675 > accessed 30 January 2019.

8- Burci, '*Public/Private Partnerships in the public Health Sector*'.

9- INTERPOL website, <https://www.interpol.int/About-INTERPOL/International-partners/United-Nations> accessed 25 November 2018.

10- "About UN Global Pulse", <https://www.unglobalpulse.org/about-new> accessed 25 November 2018.

11- Riegner, "*Towards an International Institution Law of Information*" (2015) 50, 51.

12- Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR), Article 12.

13- International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), Article 17.
14- Convention for Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108.
15- HCR, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and protection of Honour and Reputation: <https://www.refworld.org/docid/453883f922.html> accessed 26 November 2018.
16- Un General Assembly "Guidelines for the Regulation of Computerized Personal Data Files", GA Res. 45/95, 14 December 1990, <https://www.refworld.org/pdfid/3ddcafaac.pdf > accessed on 30 November 2018.
17- UN Secretary-General's bulletin, 'Information sensitivity, classification and handling'(2007), UN-Doc. ST/SGB/2007/6. <https://hr.un.org/handbook/source/secretary-general%27s-bulletins/date> accessed 27 November 2018.
18- GA Res 71/199, 19 December 2016, <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199> accessed 27 November 2018.
19- United Nations Human Rights Committee Special rapporteur on the right to privacy. <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx> accessed 27 November 2018.
20- Over 100 States have now enacted data protection laws. United Nations Conference on Trade and Development (UNCTAD), 'Data protection regulations and international data flows: Implications for Trade and Development', 2016, <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> (last accessed 19 January 2018), at 8.
21- NTT Security, The international impact and opportunity of the General Data Protection Regulation (GDPR) (2017) <https://www.nttsecurity.com/docs/librariesprovider3/resources/global_thought_leadership_gdpr_uea_v4>, accessed 4 February 2019.
22- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General data protection regulation), 25 January 2012, COM(2012) 11 final. <https://eur-

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN> accessed 2 December 2018.

23- (1992) Case C-286/90

24- (1998) Case C-162/96

25- Baudouin Heuninckx, The law of collaborative defence procurement through international Organisations in the European Union (July 2011)

26- <https://www.nottingham.ac.uk/pprg/documentsarchive/phdtheses/heuninckxthesiscompletefinal.pdf> accessed 4 February 2018

27- Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

28- Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (May 13, 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

29- United Nations, Charter of the United Nations, 24 October 1945, http://www.un.org/en/charter-united-nations/

30- The Privileges and Immunities of International Organizations in Domestic Courts, <https://global.oup.com/academic/product/the-privileges-and-immunities-of-international-organizations-in-domestic-courts-9780199679409?cc=at&lang=en&> accessed 4 February 2019.

31- 2011 C-366/10

32- Protocol No. 7 on the Privileges and Immunities of the European Union, OJ 2010 C 83/266, Article 16; Wouters and Duquet, 'The EU and International Diplomatic Law: New Horizons?', 7 The Hague Journal of Diplomacy (2012) 31, at 33-34.

33- Accord entre l'Organisation Internationale de Police Criminelle—INTERPOL (O.I.P.C.-INTERPOL) et le Gouvernement de la République Française relatif au siège de l'organisation sur le territoire française, 14 April 2008, <https://www.interpol.int/content/download/9747/420416/version/7/file/AccordSiegeRevise2 008FR.pdf> (last accessed 1 September 2017), at Article 5.

34- Agreement between the Republic of Austria and the Organization of the Petroleum Exporting Countries regarding the Headquarters of the Organization of the Petroleum Exporting Countries, 18 February 1974, <http://ilmc.univie.ac.at/uploads/media/HQ_Agreement_OPEC_-_Austria.pdf> (last accessed 1 September 2017), at para. 5(2), stating that 'The service of legal process, including the seizure of private property, shall not take place within the headquarters seat except with the express consent of, and under conditions approved by, the Secretary General', without referring to a particular body of law that is covered by the immunities.

35- The Meso Level: Means of Interaction between EU and International Law: Customary International Law as a Source of EU Law: A Two-Way Fertilization Route.

36- Theodore Konstadinides 14 October 2016 https://academic.oup.com/yel/article-abstract/35/1/513/2549066?redirectedFrom=PDF

37- European Union, Consolidated version of the Treaty on the Functioning of the European Union, 13 December 2007, 2008/C 115/01, available at: https://www.refworld.org/docid/4b17a07e2.html [accessed 4 February 2019 < http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments/part-5-external-action-by-the-union/title-3-cooperation-with-third-countries-and-humantarian-aid/chapter-3-humanitarian-aid/502-article-214.html >

38- Mark Philip, International Data sharing norms: from OECD to the general data protection regulation (GDPR) Published online 1 august 2018; < https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6132662/ > accessed 4 February 2018.

39- European Commission; Adequacy of the protection of personal data in non-EU countries <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en> accessed 4 February 2019

40- Racke (n 15), para 55; Poulsen (n 15), para 9 f; C-405/92 Etablissements Armand Mondiet SA v Armement Islais SARL [1993] ECR I-6133, paras 13-15; Intertanko (n 23), para 51; Kadi I (n 1), para. 291 f; (n 15), para 101.

41- Katja S. Ziegler The Relationship between EU Law and International Law (2013) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2373296 > Accessed 4 February 2019

Annex 1

Abstract

The right to data protection is enshrined in the EU Charter of Fundamental Rights and the Treaty on the Functioning of the European Union, which give effect to individuals' right to privacy by providing them with control over the way information about them is collected and used[122]. Personal Data is very valuable and therefor setting clear regulations in place to protect such data is essential. The General Data Protection Regulation entered into force on May 25,2018 setting out a huge scope of application covering the whole Union area but only. The impact that had was all over the world. The discussion begins when analyzing if this Regulation applies towards International Organizations, only because of the special 'status' that these Organizations hold in the International environment.

Das Datenschutzrecht ist in der EU-Charta der Grundrechte und im Vertrag über die Arbeitsweise der Europäischen Union verankert, die schützen das Recht des Einzelnen und die Privatsphäre.Sie geben der Einzelne das Recht auf Privatsphäre, indem sie die Art und Weise kontrollieren, wie Informationen über sie gesammelt und verwendet werden.Persönliche Daten sind sehr wertvoll, und daher sind klare Regelungen zum Schutz dieser Daten erforderlich. Die Datenschutz-Grundverordnung trat am 25. Mai 2008 in Kraft und umfasste einen großen Anwendungsbereich, auf das gesamte Gebiet der Union. Die Auswirkungen waren auf der ganzen Welt. Die Diskussion beginnt mit der Analyse, ob diese Verordnung für internationale Organisationen gilt, nur aufgrund des besonderen" Status "dieser Organisationen im internationalen Umfeld haben.

[122] Article 8, EU Charter of Fundamental Rights.