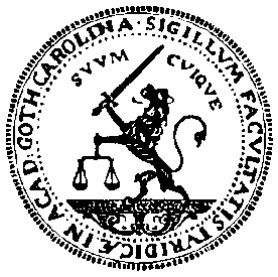


FACULTY OF LAW
Lund University

Nicolás Bahm

The Interplay of EU Data Protection Roles within Groups of Undertakings

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Eduardo Gill-Pedro

Term: Spring 2022

Summary

The GDPR is the EU's latest instalment in the attempt to establish a harmonised data protection regime across the Union, something that started over 25 years ago with the Data Protection Directive. And although a milestone in European legislation for placing the respect for fundamental rights of individuals above the interests of powerful economic groups, it still has left some aspects not fully regulated.

From the perspective of a group of undertakings operating across several Member States and processing personal data, the imposition of responsibilities introduced at EU level has presented new challenges for their business operations and the need to take considerable measures to ensure compliance.

This work finds that, in the context of groups of undertakings operating in the EU, the regime introduced by the GDPR may conflict with classic company law structures and the principle of separate legal personality, making it hard to identify which entity is finally responsible for compliance in relation to the processing activities. Considering also that these activities take place across several Member States, this may not only determine which national authority should enforce the regulatory compliance, but also hinder the possibilities of the data subjects when executing their rights. In this context, the lack of clear rules at EU level opens several interpretational possibilities in relation to which entity within a group is finally responsible for the data protection obligations.

This thesis attempts to understand which entity within a group of undertakings may be ultimately responsible for complying with the EU data protection legislation, while also identifying and analysing potential contradictions and conflicts between the responsibilities allocated by the GDPR and existing concepts of company law.

Table of Contents

List of abbreviations

CFR	EU Charter of Fundamental Rights [2016] OJ C 202/02
CJEU	Court of Justice of the European Union (covering the actual composition and pre-Lisbon composition known as the European Court of Justice – ECJ)
CNIL	Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority)
DPA	Data Protection Authority
DPD	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31
EC	European Commission
EDPB	European Data Protection Board
EU	European Union
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council 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) [2016] OJ L 119/59
OECD	Organisation for Economic Co-operation and Development
ROPA	Record of Processing Activities
SME	Small and Medium-sized Enterprises
TEU	The Treaty on European Union
TFEU	Treaty on the Functioning of the European Union (Consolidated version 2016) OJ C 202/47
US	United States of America
WP29	Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. Introduction

1.1 Background

1.1.1 Data Protection in the EU

The General Data Protection Regulation (hereinafter, the 'GDPR')[1] is the latest instalment in the European Union's ('EU') attempt to harmonise the personal data protection legislation which had started back in 1995 with the Data Protection Directive ('DPD').[2] It is considered a milestone in European legislation with an impact both internally and abroad, and praised for placing the respect for fundamental rights of individuals above the interests of powerful economic groups.

Nonetheless, any harmonisation process is an intricate task where actors involved need to make compromises. Although the GDPR introduced substantive rules which regulate personal data protection across the Union and had direct effect, some procedural elements were left on the hands of Member States with the collaboration of national data protection authorities ('DPAs'). Some of these elements may be subject to different interpretations, thus hindering the intended harmonisation.

Personal data protection also faces other inherent challenges. While its legislation contains elements of public law which impose obligations to organisations to protect the interests of the individuals whose personal data is being processed, it also sets ground rules for private parties to regulate their relations. As an example, while perhaps making the entity responsible subject to enforcement in its own Member State could be considered efficient, it could hinder the rights of individuals from other Member States whose data had been processed. But before any enforcement, it is vital to determine who is responsible for these EU Data Protection obligations.

1.1.2 Business Groups and EU Data Protection

Businesses were one of the most affected by the GDPR. In fear of the hefty fining regime, companies had to adhere with the newly introduced framework which included robust consent requirements, privacy by default and design, and mandatory breach notifications, among other obligations.[3] For groups of undertakings operating across the EU, these new responsibilities

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council 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) [2016] OJ L 119/59 (hereinafter, the 'GDPR').
[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (hereinafter, the 'DPD').
[3] Ilse Heine, '3 Years Later: An Analysis of GDPR Enforcement' (*Center for Strategic & International Studies - CSIS Blog*, 13 September 2021) <https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement> accessed 17 March 2022.

in relation to personal data presented challenges that affected their operations both within the Union and abroad.

The GDPR chose the 'data controller' as main responsible for complying with a specific processing operation. This role is meant to be analysed using a functional approach based on the processing operations and independently from 'labels' coming from other areas of law. This means that an entity can be a controller for certain processing activities for which it is ultimately responsible, while also a 'data processor' when handling different personal data on behalf of another controller. An example of this could be a Cloud service provider, who would be considered a controller for the personal data it holds from its own employees, while also a data processor for the personal data it stores for its clients.

Aside from this role coexistence, the sharing of personal data and other synergies is relevant in the context of a group of undertakings accustomed to collaborating and complementing their activities. Whenever personal data is disclosed, EU Data Protection rules apply, and its roles may not always fit with typical corporate law structures. EU Data Protection Law may even assign joint responsibility (as 'joint controllers') for undertakings jointly influencing a processing activity despite any contractual arrangements describing the opposite.

With processing activities occurring across several Member States, different national DPAs –each of them with its own interpretation– may intervene. This also presents a difficulty for data subjects whose data is processed by a company in another Member State where enforcement rules, although similar, may differ.

For groups of undertakings, the lack of clear rules at EU level opens several interpretational possibilities as to which entity within the group is responsible for GDPR obligations. Hopefully, this work will provide clarity on these complex scenarios or at least expose the necessity for further clarification.

1.2 Purpose and Research Questions

As described above, the lack of sharply defined rules at EU level or guidelines from the European Data Protection Board ('EDPB') allows multiple interpretations of the legislation, based on the interest to protect data subjects under each jurisdiction.

The ultimate purpose of this paper is to understand who is responsible to comply with the GDPR in the context of a group of undertakings. To achieve this, it will be vital to first identify which entities within a group may classify as data controllers, before analysing their relations from the perspective of EU Data Protection Law.

Therefore, my research questions are the following:

1) Who has the ultimate responsibility for compliance under GDPR in the context of a group of undertakings?
   a) Which entities could be identified as data controllers under GDPR within a group of undertakings?
   b) How do the roles of the GDPR interplay in the relations between entities in the context of a group of undertakings?
2) Are there contradictions or conflicts between how GDPR allocates responsibilities and the concepts of branches and subsidiaries under company law?

The compliance responsibility should be understood not only as following the principles related to the processing of personal data, but also acting on the GDPR imposed obligations in relation to data subjects' rights, data protection by design and by default, record-keeping, the performance of impact assessments, and others.

1.3 Methodology and Material

To answer the questions proposed, the main legal method that will be implemented for my research and reasoning will be the legal dogmatic. This method is frequently employed for the identification and interpretation of the positive law, including legal rules, principles, and case law, in a systematic order.

Because this work deals with EU Law, some extra methodology implications are bound to it. This requires understanding the co-actorship between national and EU institutions, plus being able to look beyond the categories of national law to construct legal arguments deriving from a multi-layered legal system where the Court of Justice of the European Union ('CJEU') is committed to preserve a uniform application across the EU.[4]

To that purpose, an introductory chapter will present how EU Data Protection Law and specifically the topic of my thesis fit in the EU's integration process as a necessary means to a bigger goal. Consequently, this paper will contain several remarks on how EU Data Protection Law contributes to ensuring a proper functioning of the internal market and how this can be tarnished by different interpretations of the law.

To maintain a scientific attitude, I intend to analyse the concepts presented by the legislation while also methodologically presenting different scenarios between entities of a group from a practical perspective, remaining open to its potential outcomes.

In relation to the material, during the brief introduction of EU Data Protection Law, primary sources such as the Treaty on the European Union ('TEU'), the Treaty on the Functioning of

[4] Anthony Arnull, *The European Union and its Court of Justice* (2nd edn, OUP 2006), p. 659.

the European Union ('TFEU') and the EU Charter of Fundamental Rights ('CFR') will be of utmost importance to understand its role within the EU's internal market.

To cover EU Data Protection Law from which this thesis wishes to explore its deficiencies, other key sources will include directives and regulations, specifically the GDPR and its predecessor, the DPD. Both will be crucial to understand and clarify the scope of the concepts there presented and the legislators' intentions.

This work will also include secondary sources such as guidelines and opinions from other EU institutions, as well as supplementary sources and case law from the CJEU. I also want to specify the relevance of the EDPB's 'Guidelines 07/2020 on the concept of controller and processors in the GDPR which, despite the terminology employed, provide a structured analysis which contributed to make this work possible.[5]

Finally, being the GDPR also relatively recent legislation, this thesis will also cite some working documents, books, journals, and blogs where relevant.

When interpreting the materials, I will use a teleological approach, considering both the literal meaning as well as the contextual elements, the intended objectives, their hierarchy and, due to the constant change and updates in technology and the use of data, their present-time relevance.

1.4 Delimitations

As previously indicated, this thesis attempts to understand how EU Data Protection Law contributes to the functioning of the EU's legal system as a supranational integration process, and implications that may arise from unclear rules. This means that several topics will be addressed up to the extent that they illustrate either the intricate system that regulates data protection within the EU or that are vital to elaborate the research questions proposed.

Although some comments will be made in relation to GDPR's scope of application and how it affects individuals, this paper will mainly address issues concerning the functioning of the internal market from the perspective of businesses. Mind that for groups of undertakings operating internationally, foreign data protection legislation may apply in addition to GDPR.

Considerations of the previous paragraph apply also to national and EU company law, whose rules and principles will be developed to the necessary extent as to illustrate their potential overlap with EU Data Protection Law.

[5] EDPB, 'Guidelines 07/2020 on the concept of controller and processor in the GDPR' Version 2.0 adopted on 07 July 2021 (hereinafter, 'the Controller Guidelines').

Finally, although this work highlights the complications of having multiple entities of a group "in charge" of processing operations in connection to data subjects' rights, this thesis attempts to understand the previous step of who should be the subject of that enforcement, and not how it be performed.

1.5 Outline

The following chapter aims to provide an overview about EU Data Protection Law, briefly describing its origins, relevant legislation, and its main actors, to understand how this complex subject affects the internal market as a whole and the need for clear rules.

Chapter 3 will present the concept of 'group of undertakings' introduced by the GDPR but also define several legal terminologies that will be used throughout this thesis, to allow a clear and structured analysis.

Chapter 4 will be focused on analysing the EU Data Protection roles in detail, mainly to understand who can be considered 'data controller'. It will also cover the notions of data processor, third party, recipients, and joint controllers, which may apply to other entities within a group in relation to the controller.

Chapter 5, which will be the most substantive part of my research, will examine scenarios in which undertakings may be related under the rules of company law and apply the concepts of EU Data Protection Law based on their processing operations. This is with the intention not only to determine who should be the data controller, but also to clarify the roles of the remaining entities of a group.

Finally, for my conclusions on Chapter 6, I intend to summarize how the current EU Data Protection Law framework regulates groups of undertakings and the challenges involved, as well as some suggestions or ideas of what could be done to align interpretations and provide legal certainty.

2. Data Protection in the EU's Internal Market

2.1 Data in the Internal Market

The creation of an internal market comprising 'an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured'[6] and the strengthening of relations among European countries and their people were among the main purposes of the European Economic Community ('EEC'), which remained a fundamental part of the EU embodied in the TEU and TFEU.[7]

With technological development and interconnectedness influencing how business is conducted around the world, ensuring the free movement of data is key to better achieve the four freedoms in the internal market.[8] This was not an easy task for the EU that, as the most complex integration process created through Law, intervened at EU-level to provide transparency for economic operators and ensure enforceability to individuals, while dealing with tensions from the very own Member States.[9]

For companies operating across the EU, problems involving data may not be easily labelled as either national or international. With data handled by entities in different countries, enterprises need to navigate through each jurisdiction's rules to ensure the success of their operations.[10] Consequently, a law that went beyond the Member States' boundaries was needed to ensure the protection of the 'data subjects'.[11]

2.2 EU Data Protection Law

EU Data Protection Law, which concerns the protection of personal data and individual privacy, is the most familiar part of European Data Law. The term 'data protection' is easily misinterpreted in three ways because: **a)** despite its name, it does not protect data but individuals; **b)** it does not protect all data but only personal data; and **c)** it does not regulate data as understood in information theory, but information (data with meaning).[12] With these comments in mind, whenever referring to 'data protection' throughout this paper it will mean the protection of personal data.

---

[6] Article 26(2) TFEU.
[7] Article 3(3) TEU and Article 4(2)(a) TFEU.
[8] Recital (13) GDPR.
[9] Paul Craig and Gráinne de Burca, *EU Law: Text, Cases, and Materials* (6th edn, OUP 2015), pp. 1-2.
[10] Thomas Streinz, 'The Evolution of European Data Law' in Paul Craig and Gráinne de Búrca (eds) *The Evolution of EU Law* (3rd edn, OUP 2021), also available <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762971> accessed 11 March 2022, pp. 31-32.
[11] An identified or identifiable natural person whose personal data is being collected, according to Article 2(a) GDPR.
[12] Streinz (n 10) 3.

But qualifying data protection is not easy. EU Data Protection Law is a result of both national and international legislation recognizing the protection of personal data and privacy. Despite connecting criteria traditionally relating to a geographical location, this may be extremely hard to determine when it takes place in a global computerised network.[13] Although EU Data Protection Law having the theoretical legal authority and having set up the main rules, occasional fissures in the practice may lead to variations across the EU, particularly when the legal concepts involved were initially developed at a domestic level and then incorporated onto EU-level instruments.[14]

EU Data Protection Law also presents provisions of both public and private nature that make regulation even more complex. While ensuring compliance and enforcement by the relevant authorities falls mainly under the sphere of public law, EU Data Protection Law also regulates relations between private parties, which seem more characteristic of private law.[15] For enforcement in these cross-border scenarios, the choice of law and jurisdiction is far from straightforward. The scope of public authority will only reach within its own territory unless an agreement exists with the other states.

These elements make EU Data Protection law belong to many different areas of law to which different criterions may be assigned, so the right balancing may be the key to EU Data Protection legislation's success.

2.3 The Evolution of EU Data Protection Law

2.3.1 The Origins of EU Data Protection Law

Data Protection is a relatively recent area of EU Law, which previously existed at a domestic level. In response to technological advances, several countries began to legislate data protection issues from 1960 onwards, developing concepts that became part of the European data protection acquis.[16] After the German state of Hesse, often credited for the world's first data protection law,[17] several then and future Member States followed with their own legislations in the 1970s.[18] With the need for international coordination growing, organisations such as the Organisation for Economic Co-operation and Development ('OECD') and the Council of Europe filled the void. While the OECD issued guidelines on protection of privacy and transborder flow of data based on the fair information principles developed in the

[13] Jon Bing, 'Data Protection, Jurisdiction and the choice of law' (1999) Privacy Law & Policy Reporter <http://www.austlii.edu.au/au/journals/PrivLawPRpr/1999/65.html> accessed 11 March 2022.
[14] Streinz (n 10) 6.
[15] Bing (n 13).
[16] Streinz (n 10) 6.
[17] Hesssisches Datenschultzgesetz [1970] GVBl I 625.
[18] Sweden (1973), Germany (1977), Austria, Denmark, and France (1978) and Luxemburg (1979).

United States of America ('US'),[19] the Council of Europe adopted the world's first data protection treaty.[20] Together with domestic law antecedents, these constituted the basis that later influenced EU Data Protection Law.[21]

It was not until 1990 that the European Commission ('EC'), after the Member States' demand for Europe-wide action, proposed a directive to engineer harmonisation based on Article 114 TFEU. Because of the nature and functions of EU law and its capacity to cut across boundaries of different fields of law on different levels, this seemed like the best solution.[22] The result was the DPD.

2.3.2 The Data Protection Directive

The DPD was a result of complex struggle where Member States pushed for their own interests while also attempting to preserve concepts elaborated under national laws, such as the one of 'data controller'.[23] The DPD's objectives were **(a)** integrating the data protection frameworks created by the Member States and other supranational data protection legislation to ensure a smooth use of data in the internal market, and **(b)** placing on Member States the duty to protect the EU citizens' fundamental rights and freedoms, in particular the right of privacy and respect to the processing of personal data.[24]

2.3.2.1 Harmonisation of EU Data Protection Law

To achieve the first, the DPD required Member States to apply this harmonised data protection regime when the controller was established in its territory or used any equipment situated in it.[25]

Although the first DPD proposal considered the country-of-origin principle to avoid situations where data subjects may find themselves lacking protection or that the same processing operation could be governed by the laws of more than one country, the legislators inclined for the territoriality principle, connecting the data processing activity to the territory of the EU.[26] Article 4(1)(a) DPD indicated that EU Data Protection Law applied "when the processing is carried out in the context of the activities of an establishment of the controller on

[19] OECD, 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' [1980] www.oecd.org <https://perma.cc/9CRF-4NPW> accessed 12 March 2022.
[20] CETS No. 108 [Convention 108] for the Protection of Individuals with regard to Automatic Processing of Personal Data <https://rm.coe.int/1680078b37> accessed 12 March 2022.
[21] Streinz (n 10) 6.
[22] Rob Van Gestel & others, 'Methodology in the New Legal World' (2012) Working Paper, EUI LAW <https://cadmus.eui.eu/handle/1814/22016> accessed 8 March 2022, p. 15.
[23] As part of the negotiations, it eliminated the distinction between public and private sector data processing on which German data protection law relied upon. Streinz (n 10) 8-9.
[24] Article 1 DPD.
[25] Article 4(1) DPD.
[26] Lokke Moerel, 'Back to basics: when does EU data protection law apply?' (2011) International Data Privacy Law, Issue 2011, Vol. 1., No. 2, Oxford University Press, pp. 95-96.

the territory of the Member State". This meant that controllers might have both 'relevant' and 'non-relevant' establishments in connection to the specific processing activities.[27]

When controllers were established in several Member States, necessary measures were required "to ensure that each of these establishments complies with the obligations laid down by the national law".[28] So for groups of undertakings across the EU, they would need to comply with national obligations from any processing activity performed in the context of one of its establishments. If the same operation involved two establishments in different Member States, national provisions of both countries would apply. In summary, the DPD allowed cumulative laws.

2.3.2.2 The Extraterritoriality Principle

For protecting the fundamental rights of individuals, the DPD ensured that data protection law applied even when personal data from European subjects was processed outside the EU.[29] If the activities were carried out in the context of their establishment within the EU, Article 4(1)(a) would apply. But to prevent situations where the controller had no establishment in the EU, Article 4(1)(c) also included situations where controllers used equipment situated on the territory of a Member State (unless used for transit only).

Another interesting feature of the DPD was that the nationality of the data subjects was of no relevance and might have applied to non-EU nationals' personal data if it had been processed in the context of the activities of an EU establishment.

2.3.3 Post DPD

Despite its intentions, the DPD left many aspects to be implemented by Member States and interpreted by national DPAs, which did not always have the same approach to these legal problems. For example, if a foreign controller created a secondary establishment within the EU and its parent company used equipment in the EU without the secondary establishment being involved, it could avoid the application of both 4(1)(a) and (c) DPD. Here, some DPAs would apply (c) even though the controller had an establishment within the EU, by considering a branch or subsidiary as 'equipment' (another undefined term by the DPD).[30]

On a different note, some Member States understood that data protection laws would only apply when the controllers were established in their territory. This incorrect interpretation of the

[27] Diana Sancho, 'The concept of establishment and data protection law: rethinking establishment' (2017) European Law Review 2014 42(2), Sweet & Maxwell, p. 494.
[28] Article 4(1) DPD.
[29] Streinz (n 10) 32.
[30] Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) International Data Privacy Law, Issue 2011, Vol. 1, No. 1, Oxford University Press, p. 35-36.

DPD narrowed the scope of application considerably.[31] Even on its SWIFT Opinion, the Working Party on the Protection of Individuals regarding the Processing of Personal Data ('WP29') indicated that the data protection law from the controllers' Member State should be applied to the processing by establishments of such controllers in other Member States, side lining local data protection laws.[32]

It should be remembered that the DPD was created when the internet had just begun to transform global communications and commerce, without full knowledge of what this would entail for data protection and privacy.[33] In consequence, the EU enacted complementing directives, such as the E-Privacy Directive, to prevent electronic communications and the internet outdating the DPD.[34]

2.3.4 Privacy as a Fundamental Right

Despite being mentioned in Article 1 DPD, it was not until the EU's CFR was developed that the matter of privacy as a fundamental right took prominence. The CFR was so influential that it started shaping EU Law even before formally becoming part of the EU's primary law with the Lisbon Treaty in 2009, and since then has been prominent in almost every major data protection case, going as far as the CJEU invalidating secondary EU Law for violating the rights to data protection and privacy.[35] The right to the protection of personal data was even recognised in the TFEU.[36]

The CFR acknowledged the need to protect the rights for respect for private and family life and the protection of personal data. It even provided conditions for how personal data should be lawfully processed, recognising the rights of access and rectification, and imposing that these rules should be enforced by an independent authority.[37] Later came the 'right to be forgotten' that the CJEU recognized in *Google Spain*, where it also emphatically declared that economic interests do not override data subjects' fundamental rights.[38] The CFR changed a scenario where fundamental rights had only played secondary roles when Member States needed to justify measures that hindered the proper functioning of the internal market. While

[31] Moerel, 'Back to basics: when does EU data protection law apply?' (n 26) 94.
[32] WP29, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' WP128 adopted on 22 November 2006 (hereinafter, the 'SWIFT Opinion') para 2.2.
[33] Streinz (n 10) 10.
[34] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201/37.
[35] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert v Land Hessen* [2010] EU:C:2010:662; Streinz (n 10) 15.
[36] Article 16 TFEU.
[37] Articles 7 and 8 CFR.
[38] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317.

the objectives of the internal market had initially dominated, now fundamental rights have been emphasised on EU Data Protection Law.[39]

2.3.5 The GDPR

The continuous technological advance over the last decades changed accessibility to information, leading to unprecedented global interconnectedness and the way in which enterprises conduct business, with data becoming a valuable resource to make right business decisions.[40] Personal data became an essential component of informational capital and a key competitive advantage that, placed in the production process, would allow manufacturers to create products in high volume and reduced costs, adapting to the customer's unique needs.[41] On the other hand, easy accessibility may have negative consequences by allowing the creation of profiles based on information obtained from individuals, with no control over where that information may end up.

But data also has a capacity to transmit social and relational meaning that, if put to good use, could benefit individuals other than the data subjects.[42] This has not gone unnoticed by the EU, which expressed the importance of the free flow of data to better achieve the four freedoms in the internal market, and became part of the EU's digital strategy by enhancing the digital transformation of businesses.[43]

In this context, with an aged DPD, a reformed EU competence for data protection law explicitly recognising the need for fundamental rights protection in this domain and the irruption of new technologies, the GDPR carried forward the legacy of the DPD while injecting new concepts and ideas into EU Data Protection Law, reforming its institutional structure, and even codifying some of the CJEU's most recent case law.[44]

One of the main novelties was the codification of the CJEU's 'extraterritorial application' approach from *Google Spain*, establishing a connection with the EU.[45] This means that aside from the companies established in the EU, foreign companies offering goods or services to

[39] Orla Lynskey, *The Foundation of EU Data Protection Law* (OUP 2015) p. 75.
[40] Kiran Bhageshpur, 'Data is the New Oil - - And That's a Good Thing' (*Forbes' Technology Council Blog*, 15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=160380007304> accessed 19 March 2022.
[41] Salomé Viljoen, 'A Relational Theory of Data Governance' (2021) Yale Law Journal, Vol. 131 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3727562> accessed 11 March 2022 (forthcoming) p. 3, 12; Brad Peters, 'The Age of Big Data' (*Forbes' Blog*, 12 July 2012) <https://www.forbes.com/sites/bradpeters/2012/07/12/the-age-of-big-data/?sh=7b6d85a44f66> accessed 19 March 2022.
[42] Viljoen (n 41) 9.
[43] Article 1(2) DPD and Article 1(1) GDPR; See European Commission ('EC'), '2030 Digital Compass: the European way for the Digital Decade' COM (2021) 118 final <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118> accessed 06 May 2022.
[44] Streinz (n 10) 11-12.
[45] *Google Spain* (n 38).

people within the EU or monitoring their behaviour are subject to the regulation.[46] Same as with the DPD, the GDPR's scope also comprehends data of non-EU persons by mentioning that it will apply to data subjects who are "in the Union" when processed in the context of an establishment of a company located in the EU, no matter where the processing takes place.[47]

Another relevant note was the sanctions regime, which caught the attention of every business located in the EU or offering services to people in it. Inspired by EU Competition Law, it replaced the DPD's system where Member States were in charge of issuing sanctions by setting up new parameters for determining fines in case of non-compliance.[48] Combined with other responsibilities such as keeping records of processing activities (ROPA) and ensuring 'data protection by design and by default', the fear of businessmen grew considerably.[49]

Finally, in the context of a group of undertakings, the GDPR has another curious particularity. Because of its extraterritoriality principle, the Regulation would also protect the personal data and privacy of data subjects from group entities outside the EU whenever their data was considered as "processed in the context of an establishment within the EU". For multinational undertakings headquartered in the EU and using central HR systems for staff administration, the data in question may be processed in the EU.[50] And although the GDPR does not care for the place of processing, foreign legislation may still include it as a point of connection for applying their own rules, which would finally result in a cumulative application of both EU and non-EU data protection legislations.

Another hiccup is that from the perspective of the data subjects (employees of undertakings of the same group outside the EU), although in theory having their rights protected by the GDPR, the practical application may not be straightforward if they need to lodge a complaint with DPAs located in the EU. Unfortunately, these issues related to foreign legislations and jurisdictions escape the scope of my paper and will not be further developed.

Without diminishing the importance of the GDPR, I will now proceed to introduce the players in the EU Data Protection Law scenario.

2.4 The Institutionalisation of EU Data Protection Law

Data Protection in the EU is a complex integration process which was initially regulated by Member States and policed by national DPAs. With the legislation's integration, a parallel

[46] Article 3 GDPR.
[47] David Froud, 'GDPR: It's not just about EU citizens, or residents' (*Froud on Fraud Blog*, 2018) <www.davidfroud.com/gdpr-not-just-eu-citizens-or-residents/> accessed 11 March 2022; Article 3(1) and recitals (2), (14) and (22) GDPR.
[48] Streinz (n 10) 12.
[49] Articles 25(1), 25(2) and 30(1) GDPR.
[50] See chapter 5.

process took place where the authorities regulating the protection of personal data had to find their place in a broader scenario.

2.4.1 National Data Protection Authorities

Despite many countries established their own DPAs in the 1970s, circumstances differed from one country to another. National data protection laws in some had established a legacy of unusually powerful and independent DPAs which confronted the national governments' data processing activities. This influenced the drafters of the DPD, which decreed that each Member State required at least one supervisory authority which could act with complete independence.[51]

These authorities were entrusted to act with complete independence with investigation and intervention powers, but also to engage in legal proceedings where national provisions violated the DPD.[52] In brief, they were the ones tasked with monitoring the implementation of EU Law, although interpretation was still in the hands of the CJEU.

Nonetheless, because of the many disparities between DPAs such as enforcement priorities or uneven capacities, the uniformity of EU Data Protection Law was threatened.[53] And although the EU promoted the GDPR to business stakeholders with the promise that only one data protection authority would be responsible for them ("one stop shop"), the complex reality resulted in Member States preventing undue centralization by entrusting the EDPB with binding power only in some isolated circumstances.[54]

Although enforcement escapes the scope of my work, it is important to understand that, despite some clarifications by the CJEU in relation to the national DPAs powers and sovereignty after the GDPR, their roles and scope are still under scrutiny, generating tensions at EU level.[55] In a domain where so many multi-jurisdictional elements are involved, the need for coordination is vital for its success.

2.4.2 Supranational Coordination Structures

The same Article 29 DPD that entrusted implementation to the DPAs created the WP29, an advisory structure composed by representatives from each Member States' DPAs and the

[51] Streinz (n 10) 18. Article 28(1) DPD.
[52] Article 28 DPD.
[53] Streinz (n 10) 19.
[54] See Paolo Balboni and others, 'Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation' (2014) Computer Law & Security Review 30 <https://www.sciencedirect.com/science/article/abs/pii/S0267364914000934> accessed 23 May 2022, p. 398.
[55] See Case C-645/19 *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit (*Belgium Data Protection Authority*)* [2021] ECLI:EU:C:2021:483; See also Conseil d'Etat, Judgement of 19 June 2020, No. 430810 (*Société Google LLC*) upholding fine after Deliberation no. SAN-2019-001 of 21 January 2019 by the *Commission National de l'Informatique et des libertés* ('CNIL') <https://www.cnil.fr/sites/default/files/atoms/files/council-of-state-decision-google-2020-06-19_en_0.pdf> accessed 19 May 2022 (English translation).

EU institutions. Among its tasks, it was delegated with the examination of national measures to achieve uniform application between Member States, advising the EC on the level of protection of third countries, providing opinions and recommendations, etc.[56]

It was the WP29 that, through guidelines and recommendations, interpreted the EU Data Protection regime until the GDPR entered into force. This includes the 'Guidelines for identifying a controller or processor's lead supervisory authority' adopted after the GDPR's sanction and attempted to coordinate the activities of DPAs when there was a cross-border processing operation.[57] Following these, a 'concerned' DPA could act to ensure that the lead DPA model does take measures that could hinder the rights of individuals under their jurisdiction.[58] Although enforcement by the DPAs escapes my thesis, these guidelines will help when analysing processing operations of groups of undertakings.

With the GDPR, the EDPB was created to succeed the WP29 and delegated to ensure consistent application of the Regulation in line with Article 70 GDPR.[59]

2.4.3 Jurisdictional authority

Although the DPAs and the EDPB have defined roles in relation to interpreting, implementing, and enforcing the GDPR, it is worth remembering that EU Data Protection Law also contains elements which regulate relations between organisations and private individuals, and will be subject to local jurisdictional authorities.

For undertakings processing personal data from subjects across several Member States, they may be liable for their non-compliance in several jurisdictions. For a data subject, the possibility to make a civil claim in its own jurisdiction would avoid costs and other practical difficulties that could arise if having to sue a controller in the Member State of its main establishment.

As mentioned in 1.4, enforcement is a broader topic which escapes the scope of my thesis and will not be further developed.[60] Nonetheless, it is important to highlight that in the context of EU Data Protection Law and with multiple players intervening for its enforcement, the need for clear rules is of utmost importance.

[56] Article 30 DPD.
[57] WP29, 'Guidelines of identifying a controller or processor's lead supervisory authority' WP244 rev.01 adopted on 13 December 2016 as last revised and adopted on 5 April 2017 (hereinafter, the "Lead Supervisory Authority Guidelines"); Cross-border processing is defined in Article 4(23) GDPR.
[58] Lead Supervisory Authority Guidelines (n 57) 9. See also Article 56(2) and (5) GDPR.
[59] Article 68 GDPR.
[60] For the topic of enforcement, applicable law and jurisdiction, see Bing (n 13).

3. Groups of undertakings

To facilitate further analysis, this chapter will present the legal terminologies and concepts introduced by the GDPR and EU Law relevant for groups of undertakings which will be used throughout this work.

Article 4 presents the list of the definitions contained in the GDPR. Because of this early introduction of the terms ‘data controller’ and ‘data processor’ that we will cover in chapter 4, it strategically assigns all responsibilities on these roles without further need to explain what they entail. Nonetheless, when it needs to refer to subjects as an interrelated collective, it opted for the terms ‘group of undertakings’ and ‘group of enterprises’. The first is even included in the list of definitions, which explains that a group of undertakings is a controlling undertaking and its controlled undertakings, but without indicating what an undertaking means individually.[61]

Thanks to the recitals, we know that this ‘control’ is related to the idea of a dominant influence of one undertaking over the others by virtue of ownership, financial participation, etc. and not strictly in relation to the ‘data controller’ of a specific processing activity. It also explains that an undertaking which controls the processing of personal data in affiliated undertakings to it should be regarded, together with those, as a group of undertakings.[62] Because it does not particularly mention that the controlling undertaking needs to be the one which controls the processing of personal data, it is interpreted that any of the controlled undertakings can be the one controlling the data processing per se. In summary, within a group of undertakings there is a relationship of control related to dominant influence, which is not necessarily connected to the control of personal data.

Because this thesis focuses on the relations within groups of undertakings, it is important to define first what an undertaking is. But before reaching that point, some previous steps are required. Although the WP29 and EDPB have created guidelines in relation to the concepts introduced by the GDPR, unfortunately they used terms such as ‘company’, which is avoided by the GDPR, or ‘entity’, which may be open for debate. Without a set of strict definitions used by the EDPB, I must analyse these considering the existing legislation and in their specific context. Therefore, I propose starting from the most elementary and make my way to the collective ‘group of undertakings’.

3.1 Entity, Persons, and Legal Persons

[61] Article 4(19) GDPR.
[62] Recital (37) GDPR.

One of the terms preferred by the EDPB's guidelines is the concept of 'entity'. Its different interpretations make it a controversial term, which may comprise human persons according to some,[63] but not according to others.[64] This might be one of the reasons why the GDPR legislators practically avoided its use, but when referring to binding corporate rules in relation to whoever should oversee compliance.[65]

Almost a century ago and citing Michoud, Dewey explained that, for the legal science, the notion of person signifies "a subject of rights-duties, a being capable of having the subjective rights properly belonging to him".[66] It is then important to understand that, for the law, there are two kinds of entities or persons which can be subject to rights and duties: human and non-human. To avoid complications, I will use the terms 'legal person' or 'juridical person' to refer to non-human entities, and 'individuals' or 'natural person' to human entities/persons.[67] Be aware that the EDPB, aside from using 'entity', also uses 'legal person' and 'legal entity' (which might cause a confusion because according to our paragraph above, human persons can also be entities subject to the law), so I will examine how each is used in the specific context. Because both natural and legal persons can be deemed data controllers according to the GDPR, there is no need to further scrutinize the concepts at this stage.

3.2 Companies and Basic Corporate Forms

As you might have realised, I avoided using the term 'company' or 'companies' when referring to the groups of undertakings, unless referring to rules of company (or corporate) law. There is no doubt that companies or corporations are included within the category of 'juridical persons', as well as in the broader concepts of 'undertaking' and 'enterprise'. The inclination for the term 'undertaking' has been a constant in EU Law, which in the case of the GDPR contributed to avoid misinterpretations based on the different national rules that regulate companies and corporations in every Member State.[68]

Company law in Europe is a much broader topic which escapes the scope and intended extension of my thesis. My goal in this work is not to cover the specific rules that regulate company law either by the Member States or even at EU level, but to focus on the notions of branches and subsidiaries which are expressly mentioned in the GDPR and have significant relevance when understanding relations between entities within groups of undertakings.

---

[63] "Entity", Legal Information Institute, Cornell Law School <https://www.law.cornell.edu/wex/entity> accessed 24 March 2022.
[64] "Entity", The People's Law Dictionary, Edition 2 <https://legal-dictionary.thefreedictionary.com/Entity> accessed 24 March 2022.
[65] Article 47 (h) and (j) GDPR.
[66] Léon Michoud, 'La Notion de Personnalité Morale' (1899) 11 Revue du Droit Public, 1, at 8 cited by John Dewey, 'The Historic Background of Corporate Legal Personality' (1926) Yale Law Journal Vol. XXXV No. 6, p. 659.
[67] In line with the definitions in Article 4 GDPR, which distinguish natural and legal persons.
[68] Besides, the fact that the EU has 24 official languages does not make this interpretation any easier.

When it comes to 'corporate groups' or 'groups of companies', it is understood as a collection of holding and subsidiary companies that function as a single economic entity through a common source of control.[69] Despite this, no jurisdiction recognises this group of entities as endowed with legal personality.[70] These groups are composed by several companies which, as a general rule, are separate legal entities from its shareholders, whose liability is limited to the value of their shares and cannot be required to perform the company's obligations, and from one another.

This principle of 'separate legal personality' is fundamental to understand that although the shareholders may have shares (and control) over several different companies, these are independent, and their responsibilities should in principle be limited to them.[71] Nonetheless, this concept is not absolute, and the boundaries of company law can be surpassed by 'lifting the corporate veil' and extending the rights and liabilities of corporations to its shareholders.[72]

Because one of my objectives is to analyse any contradictions between the regime imposed by the GDPR and the rules of company law, I will implement the terminology of 'company' to refer exclusively to legal persons within the context of company law. Also, both the notions of 'company' and 'group of companies' (used by the EDPB) should be interpreted as comprised within the broader notions of 'undertaking' and 'group of undertakings' that I will address under 3.3.

3.2.1 Establishment according to EU Law

Because 'establishment' is the point of connection to apply GDPR, it is fundamental to understand its meaning according to EU Law.

The 'freedom of establishment' enshrined in the TFEU entails that legal persons have the right to set up either primary or secondary establishments such as subsidiaries, branches, and agencies across the EU.[73] Article 54 TFEU explains that companies or firms (constituted under civil or commercial law) having a registered office, central administration, or principal place of business within the EU shall be treated as natural persons who are nationals of those Member States without any discriminations. It also comprises a "right for a secondary establishment", if a legal person is already established somewhere in the EU.[74] But although this freedom

[69] See Javier Perez Font, 'Group of Companies and International Jurisdiction over Individual Contracts of Employment' in *Cuadernos de Derecho Transnacional* (Vol.13 Issue 2, UC3M 2021), pp. 863-869 (in Spanish).
[70] Peter Böckli and others, 'A proposal for reforming group law in the European Union – Comparative observations on the way forward' (*European Company Law Experts – ECLE Website*, October 2016) <https://europeancompanylawexperts.wordpress.com/publications/reforming-group-law-in-the-eu/#_ftn23> accessed 22 May 2022.
[71] ibid.
[72] *Google Spain* (n 38).
[73] Article 49 TFEU.
[74] Case 205/84 *Commission of the European Communities v Federal Republic of Germany (Insurance Services)* [1986] EU:C:1986:463.

allows moving the registered office or central management and control within the EU, this is not an unconditional right as they may be subject to national company law.[75]

Establishment is not defined by the GDPR, but its recitals indicated that it implied "the effective and real exercise of activity trough stable arrangements", clarifying as well that the legal form of that establishment (either a branch or subsidiary with legal personality) was not a determining factor.[76] The "stable arrangements" are in line with the CJEU's rulings which require a "stable and continuous basis", "regularity, periodicity or continuity", and the actual pursuit of an economic activity in another Member State for an indefinite period.[77] In *Somafer*, the CJEU also explained that, although an extension of a parent body, the concept of branch includes management and is materially equipped to negotiate business with third parties, which recognise the link with the parent body.[78]

From a literal interpretation, the use of "an establishment" in Article 3(1) GDPR seems to indicate one establishment among several, making any of these establishments, either primary or secondary, a point of connection for the application of the GDPR.[79] The DPD's recitals explicitly indicated that when a single controller was established on several Member States, particularly by means of subsidiaries, it should ensure that each establishment fulfilled the applicable obligations as to avoid circumventing data protection rules,[80] which created a decentralisation that allowed data subjects to maintain their rights within the laws of a country they were familiar with.[81] The fact that foreign controllers, although having their main establishments abroad, were required to comply with the DPD when the processing is performed in the context of their establishments in the EU seemed to support this concept.

3.2.2 Establishment in the GDPR: Branches and Subsidiaries

But although "the processing of personal data in the context of the activities of an establishment of a controller or processor" is the point of connection, there is no indication in the GDPR suggesting that establishments could be either independent controllers or

[75] See Case 81/87 *The Queen v H.M. Treasury and Commissioners of Inland Revenue, ex parte Daily Mail and General Trust plc.* [1988] EU:C1988:456; Case C-208/00 *Überseering BV v Nordic construction Company Baumanagement FmbH (NCC)* [2002] EU:C:2002:632; Case C-378/10 *VALE Építési kft.* [2012] EU:C:2012:440.
[76] Recital (22) GDPR.
[77] Case C-55/94 *Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano* [1995] EU:C:1995:411, paras 25 and 27; Case C-221/89 *The Queen v Secretary of State of Transport, ex parte Factortame Ltd and Others* [1991] EU:C:1991:320, para 20.
[78] Case 33/78 *Somafer SA v Saar-Ferngas AG* [1978] EU:C:1978:205, para 12.
[79] Moerel, 'Back to basics: when does EU data protection law apply?' (n 26) 95.
[80] Recital (19) DPD.
[81] Ulrich Dammann and Spiros Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft, Baden Baden 1997) 127-8 cited by Moerel, 'Back to basics: when does EU data protection law apply?' (n 26) 97.

processors within a group of undertakings.[82] Nonetheless, the EDPB refers to the possibility of an establishment acting as either controller or processor.[83]

Because the GDPR explicitly indicates that both subsidiaries and branches can be considered establishments for the purposes of EU Data Protection Law,[84] the EDPB's choice of the word 'establishment' suggests that both subsidiaries and branches could be deemed independent data controllers from their principals under GDPR. This is strengthened by expressly indicating in its 'Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on International Transfers as per Chapter V of the GDPR' (hereinafter, the 'International Transfer Guidelines') that entities within a same corporate group may be separate controllers or processors for EU Data Protection Law.[85]

It is worth observing that, while a subsidiary is a company controlled (in company law terms) by another 'holding' company but subject to the laws of the Member State where it is incorporated, a branch is an establishment set up by the 'parent' company to perform the same business operations at a different location, subject to direction, control, and laws of the parent body.[86] In consequence, a branch is owned completely by its parent organisation that, because it has no separate legal standing and cannot benefit from the limited liability that subsidiaries have, cannot isolate the risks involved in a venture.[87] While there should not be any issues with applying the concept of data controller to a subsidiary with independent legal standing, its attribution to a branch is troublesome considering that it is a 'separate body' within the same legal person. Here the notion of 'separate legal personality' is challenged, without GDPR nor the EDPB providing guidance on how to navigate this matter. According to Moerel, some DPAs believed branch offices could qualify as controllers even before the GDPR.[88]

In short, the EDPB's use of the word establishment allows two different interpretations:

---

[82] Recital (124) GDPR explains that when processing occurs in the context of activities of a single establishment that could affect data subjects in more than one Member State, the supervisory authority of the main establishment or for the single establishment of the controller should act as lead authority. Although the possibility of having the DPA from the single establishment processing data fits the idea of an establishment being an independent controller, the GDPR avoids making express references to an undertaking having multiple controllers.

[83] Controller Guidelines (n 5) para 17.

[84] Recital (19) DPD and recital (22) GDPR.

[85] EDPB, 'Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR' adopted on 18 November 2021 (hereinafter, the 'International Transfer Guidelines') para 16.

[86] See Case 139/80 *Blanckaert & Willems PVBA v Luise Trost* [1981] EU:C:1981:70, para 9.

[87] Kartsten Engsig Sørensen, 'Branches of Companies in the EU: Balancing the Eleventh Company Law Directive, National Company Law and the Right of Establishment' [2013] Nordic & European Company Law Working Paper No. 10-37 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2264091> accessed 27 March 2022, p. 5.

[88] Fonteijn-Bijnsdorp, ''Art. 4 Wbp revisited': enkele opmerkingen inzake de toepasslijkheid van de Wet bescherming persoonsgegevens' (2008) 6/2008 Computerrecht, p. 289, cited by Moerel, 'Back to basics: when does EU data protection law apply?' (n 26) 99. See also Gerrit-Jan Zwenne and Chris Erents, 'De reikwijdte Wbp:enige opmerkingen over artikel 4, eerste lid, Wbp' (2009) Privacy & Informatie 2009/2, English translation available from Zwenne's Blog <https://zwenneblog.weblog.leidenuniv.nl/files/2009/10/GJZ-CER-ScopeofDDPATranslationOct09.pdf> accessed 18 April 2022.

1) ‘Establishment’ is to be used exclusively as a point of connection for the application of the GDPR and there is no express indication that an establishment could be a data controller (and the EDPB should have avoided using the term).
2) The term ‘establishment’ was consciously chosen by the EDPB in line with Recital (22) GDPR, therefore allowing branches to be data controllers when handling personal data independently from their parent companies.

Inclined to agree with the latter, the following chapters will analyse all the circumstances to determine if this scenario is possible according to the legislation, and what could be the foreseeable consequences of this interpretation. [89] To avoid any confusion in further analysis, a branch may be referred to as an ‘entity’ within a company but should be understood as part of the same ‘legal person’, unless stating the opposite.

3.3 ‘Undertaking’ and ‘Group of undertakings’

In the field of EU competition law, the concept of ‘undertaking’ covers any entity engaged in an economic activity, regardless of its legal status and the way in which it is financed.[90] The use of this approach consequently captures individuals, trade associations, partnerships, companies, public authorities, etc. It may also encompass several legal or natural persons, resulting in the principle of separate legal personality giving way in the area of competition law to the economic concept of undertaking.

Ezrachi explains that the concept refers to a “single economic entity”, which may affect how competition law is applied to groups of companies because **a)** it may exclude agreements between separate legal entities and view them as internal allocation of functions within a single economic unit, and **b)** it may link separate legal entities by viewing them as a single undertaking, making them all responsible for the actions of one of them.[91]

Did EU legislators intend for the term ‘undertaking’ in the GDPR to be interpreted as the one defined by EU Competition Law? Under the latter, the notion of an undertaking as a single economic unit has a palpable benefit to help identify the association of undertakings and potential evasion of competition law rules.[92] In the context of EU Data Protection Law where the roles are based depending on specific processing operations,[93] using the same notion as in EU Competition Law does not seem fitting. While EU Competition Law aims to identify a

[89] On 28/02/22 I contacted the EDPB asking for guidance on the matter, receiving a reply on 15/03/22 where they explained that they could not advise students on research topics and referred to their institutional website.
[90] Case C-222/04 *Ministero dell’Economia e delle Finanze v. Cassa di Risparmio di Firenze SpA and Others* [2006] EU:C:2006:8, para 107.
[91] Ariel Ezrachi, ‘The Concept of Undertaking’ in *EU Competition Law: An Analytical Guide to the Leading Cases* (Hart 2014) p. 2.
[92] Case C-309/99 *J. C. J. Wouters and Others v Algemene Raad van de Nederlandse Orde van Advocaten* [2001] Opinion of AG Léger EU:C:2001:390, para 62.
[93] Will be analyzed in further detail under section 4.1.

single, converging will by several participants that form an undertaking, EU Data Protection Law attempts to find the specific entity responsible for determining the purposes and means of a processing activity.

The GDPR also explains that when administrative fines are imposed on an undertaking, the term should be understood in accordance with Articles 101 and 102 TFEU for those purposes.[94] This shows that the term of 'undertaking' under the GDPR is not always the same as the one in EU Competition Law.

In general, the GDPR avoids using 'undertaking' unless referring to a 'group of undertakings', and mainly to explain the relation between undertakings under the same control sphere. Despite defining 'group of undertakings', it is barely mentioned in the GDPR nor introduces specific rules in regards how these should deal with their internal relations, which seem to remain the same as with any other undertaking not part of the group. The recitals indicate that controllers that are part of a group of undertakings may have a legitimate interest to transmit personal data within the group for internal administrative purposes, but with no clear indication that their responsibilities should be waived to do so. In fact, it directly follows by explaining that when transferring data within the group to an undertaking in a third country, the general principles for the transfer of personal data remain unaffected.[95]

Moreover, the GDPR legislators delegated to the Member States the task of providing more specific rules in relation to transfers of data within a group of undertakings in the context of employment.[96] Aside from leaving the door open to multiple interpretations, this attribution seems to indicate a notion of undertaking slightly more similar to a legal person under civil law who can be attributed legal obligations (such as being an employer).

Despite their differences, both EU Competition law and EU Data Protection Law apply the notion of "piercing" through entities with separate personality under company law to identify a "single economic entity" for the former or, as I will address shortly under chapter 4 for the latter, to attribute responsibilities for the processing of personal data.

3.4 Enterprise

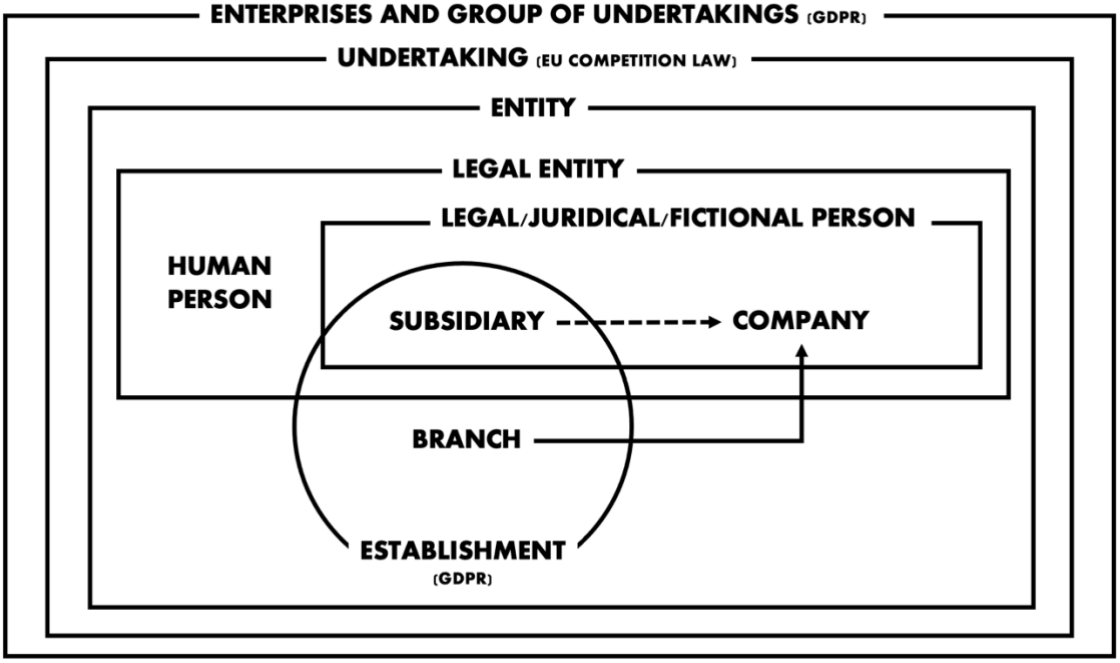
The GDPR also defines "enterprise" as a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.[97] And although the terms 'group of undertakings' and 'group of enterprises' generally go together throughout the GDPR, the use of independent terminology

[94] Recital (150) GDPR.
[95] Recital (48) GDPR.
[96] Article 88 GDPR.
[97] Article 4(18) GDPR.

implies that they are not the same.[98] While both undertakings and enterprises seem to be connected to the engagement of an economic activity and its legal form is not relevant, 'enterprises' seems to cover both natural and legal persons while 'undertaking' seems more aligned with the notion of 'company' from company law, due to the mention of dominant influence due to ownership or financial participation.[99]

Because this thesis attempts to identify responsibilities within a collective of undertakings, 'group of undertakings' should be understood as potentially including both individuals and legal persons, including all internal organisational structures of the legal persons involved. To address these internal organisational structures within legal persons independently, I will use the terms 'entity' or 'entities', regardless of their classifications under the rules of company law.

To help the reader while navigating these multiple legal concepts, the following graphic illustrates how each of the concepts discussed throughout this chapter fits within the others.[100]



With some understanding of what a 'group of undertakings' entails and how it may be organised internally according to company law, it is time to dive deeper into the roles introduced by EU Data Protection Law.

[98] See Recital (110), Articles 4(20), 47 and 88 GDPR as examples.
[99] Recital (37) GDPR.
[100] Please note that some of these differ from the ones used by the EDPB in its guidelines.

4. The roles under EU Data Protection Law

As seen throughout chapter 2, the intervention of players both on a national and supranational level in EU Data Protection Law may allow different interpretations whenever rules are not consistent, making it hard to navigate for entities established in several Member States and hindering the proper functioning of the internal market.

It is now time to submerge into the core of data protection law and introduce the main roles from the GDPR. In brief, this Chapter will place specific emphasis on the concept of data controller, but also attempt to understand other relevant roles that may be attributed by EU Data Protection Law and may help untangle the complex web of relations between undertakings of the same group. Before analysing each of the elements required to make a controller, I would like to preliminary point out that the GDPR deems data controllers those who determine purposes and means of a processing activity, while data processors are those who process personal data on behalf of a data controller.[101] I will further develop these two below.

4.1 The Functional and Autonomous Concepts

Before addressing the specific roles, it is important to present the notions of *functional* and *autonomous*, which are applied to the concepts of data controllers and data processors and will be discussed throughout this chapter.

The notion of *functional* is aimed to allocate responsibilities and legal status according to EU Data Protection Law based on the actual roles of the parties. This means that an actor will only be a controller or processor based on its actual activities in relation to the processing activity rather than a mere private designation from the parties or the nature of the entity who does the processing.[102] Consider *Google Spain*, where the CJEU used a broad approach and explained that Google operated as an economic whole irrespective of the technical separation of corporate forms and the location of the processing.[103] When interpreting these roles, excessive formalism would make it easy to circumvent the provisions, so it may be necessary to "rely upon a more factual than formal analysis".[104]

Therefore, an entity can be a controller for certain processing activities for which it is ultimately responsible, while also being a 'data processor' when processing data on behalf of other controllers. As mentioned in the introduction, a good example could be an undertaking

[101] Article 4(7) and (8) GDPR.
[102] Controller Guidelines (n 5) paras 12 and 26.
[103] *Google Spain* (n 38).
[104] Case C-25/17 *Proceedings brought by Tietosoujavaltuutettu* [2018] EU:C:2018:57, Opinion of AG Mengozzi, para 68.

providing Cloud services, who would probably be controller for the personal data it processes from its own employees, but at the same time data processor for the personal data it stores for its clients.

Unfortunately, the notion of *autonomous* is not that clear. The EDPB indicates that although external legal sources can help identify the controller, it should be mainly interpreted according to EU Data Protection Law and not prejudiced by concepts in other fields of law, with which it may sometimes collide or overlap.[105] To some extent, this explanation contradicts the previous opinion by the WP29, which explained that it was important to stay as close as possible to the practices established both in the public and private sector by other areas of law.[106]

4.2 The Data Controller

The concept of data controller is crucial to understand who should comply with the GDPR for processing personal data. It will not only be a point of reference for the public authorities but also required to show transparency to the data subjects, making them aware of who is processing their data, for which purposes, and to whom they should turn to when needed.

The GDPR maintains the definition from Article 2 DPD, explaining that it is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[107] In short, it is a body that decides the key elements of the processing activity: why and how.

Being a data controller is not a merely formal criterion that the parties can appoint at the own will, but a consequence of the factual circumstances that an entity decided to process personal data for its own purposes. This means that the entity has the responsibilities entailed even without any formal appointment or, even when existing, if it does not reflect the reality by entrusting the role to a body that is not in the position to "determine" the conditions of the processing.[108]

For a clear analysis, I will proceed to separate this definition into five blocks as performed by the EDPB.[109] These are the following:

- Natural or legal person, public authority, agency, or other body.
- Determines.
- Alone or jointly with others.
- The purposes and means.

[105] Controller Guidelines (n 5) para 13.
[106] WP29, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP169 adopted on 16 February 2010 (hereinafter, the "Opinion on concepts of controller and processor"), p. 15.
[107] Article 4(7) GDPR.
[108] Opinion on concepts of controller and processor (n 106) 15.
[109] Controller Guidelines (n 5) para 16.

- Of the processing of personal data.

4.2.1 Controller as a Subject

As the GDPR definition enumerates, natural persons, legal persons, public authorities, agencies, or bodies can be deemed as data controllers. Because my purpose is to understand this role in the context of a group of undertakings, I will concentrate mainly on legal persons, but natural persons may also be controllers in their own rights. This means that there is no requirement for a proper "organisation", and it applies as long as data is being processed and falls under the scope of the GDPR.[110]

The EDPB mentions that certain existing roles and professional expertise which imply a degree of responsibility may help identify the controller. It even uses the example of a law firm indicating that, when using personal data provided by a client to be represented in a dispute, because of its significant degree of independence to decide what information and how to use it, it may be regarded as controller.[111] Although the guidelines use the term 'law firm', which seems to imply some degree of organisation, the processing activity would be very similar for independent professionals (lawyer, accountant, etc) who as natural persons can also be data controllers.

The EDPB indicates that, in principle, there is no limitation as to the type of entity that may assume the role of a controller but, in practice, it is usually the organisation as such. Although it may also be an individual or group of individuals, in the context of an organisation it does make more sense considering the organisation as the data controller, and not a particular individual such as the CEO, a determined employee or board member. When a department or area of an organisation has some operational responsibility for ensuring compliance for a particular processing activity, it does not mean that such department is the data controller instead of the organisations as a whole. Any processing of personal data that takes place within the realm of activities of an organisation may be presumed to take place under that organisation's control.[112]

When it comes to groups of undertakings (or "company groups", the terminology used by the EDPB), the challenge is understanding where their establishments fit. As mentioned in 3.2.2, both branches and subsidiaries may be either data controller or data processors in relation to their parent (in the case of branches) or holding companies (for subsidiaries).[113] But in paragraphs 76-77, while explaining the concept of data processor, the EDPB explains that

[110] In line with Article 2(2)(c) GDPR, processing of personal data by a natural person for purely personal or household activities does not fall within the scope of the regulation.
[111] Controller Guidelines (n 5) para 27.
[112] ibid 17-19.
[113] ibid 17.

only separate entities can process data on behalf of the controller. It clarifies that within a group of companies, one company can be a processor to another company acting as controller because both companies are separate entities, before closing by saying that within a company, a department cannot be a processor to another department within the same entity.[114]

The fact that the EDPB has not properly defined the concepts it used for the guidelines nor relied on the ones from the GDPR does not make this analysis any easier. While the use of 'establishment' in paragraph 17 seems to include branches, the term 'company' in 76-77 seems not even to consider the possibility (either on purpose or by omission). If by 'separate entity' and 'external organisation' in paragraph 77 the EDPB means separate legal person, it would be contradicting its own paragraph 17 and recital (22) GDPR by excluding branches from the definition of establishment. So, after interpreting these two paragraphs and the GDPR altogether, it would seem that a branch could be considered as an 'external organisation' and a 'separate entity' for paragraph 77, thus possible data controller or processor.

4.2.2 "Determines"

The second element to establish the role of a data controller is determination. This element refers to the influence that the controller has over the processing activity, by virtue of an exercise of decision-making power. It might be worth mentioning that this influence relates to the particular processing activity, and not over the whole undertaking in terms of control from company law.[115] So, the entity that makes the ultimate decision about some certain key elements of the processing activity will be the data controller.[116]

According to the EDPB, this controllership may be defined by the law or stem from the analysis of the facts and circumstances of the case. To do so, one must observe the processing activity and answer the questions of 'why' the processing takes place, and 'who' decided that it should take place for the determined purpose. Based on the functionality discussed in 4.1, some presumptions may be applied to guide the process: the "determining body" can be identified by reference to certain legal and/or factual circumstances from which "influence" may be normally inferred, unless other elements indicate otherwise.[117]

In relation to the first, the GDPR explains that "where the purposes and means of the processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided by the Union or Member State law".[118] So, in principle,

[114] ibid 77.
[115] Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, OUP 2007) p. 117-18, cited by Moerel, 'Back to basics: when does EU data protection law apply?' (n 26) 99.
[116] Controller Guidelines (n 5) para 20.
[117] ibid 20-21.
[118] Article 4(7) GDPR.

where a controller has been specifically identified by law there should be no doubt about who is acting as data controller. In spite that, two issues make this assessment harder than one might expect.

The first is that commonly the law imposes tasks or duties on individuals or entities to collect and process data without formally "appointing" them as data controllers.[119] As a consequence, the link between the task/duty and being a data controller is conditional to the purposes and means being determined by the law. As an example, if the law of a Member State required a legal person to process an employee's social security number and explained that this is for the purposes of paying the correspondent contributions (which is a legal obligation), the legal person could be inferred as the data controller for such processing activity (the collection of the employee's social security number). So, when the law imposes a duty on an individual or entity and the purposes of the task are specified by the law, there should be no doubt on who the data controller is. But if besides its security number this legal person also collected its employee's home address without the law having specifically given a purpose for it, this assumption would not be so straightforward even when the relationship between employer-employee were the same. This also helps illustrate how complex a processing activity can be, and how it could be at the same time composed by several "micro" processing activities.

The second problem is that, even when done by the legislator, the law might have not always assigned an entity with genuine capacity to exercise the role of data controller.[120] Without getting too far ahead of myself and continuing with the example above, a holding company may own a subsidiary who only employs the personnel (in the sense of being responsible for the legal relationship employer-employee) but where all processing operations are still being determined by the holding company, therefore circumventing EU Data Protection legislation. In this scenario, identifying controllership over the processing operation might require the intervention of the authorities to determine which company is the "real" data controller by using the functional notion from *Google Spain.*[121] This is one of the cases where 'control' (or influence) in terms of company law may prevail over the control on a specific processing operation set by EU Data Protection Law.

This leads us to the other possibility, where the processing activity stems from the factual elements and circumstances of the case. The EDPB explains that when control stems from factual influence, all relevant circumstances must be considered to assess which entity has determinative influence.[122] In practice, some processing operations can be considered as

[119] Controller Guidelines (n 5) para 24.
[120] ibid 23.
[121] *Google Spain* (n 38).
[122] Controller Guidelines (n 5) para 25.

naturally attached to the roles or activities of an entity based on general legal provisions or established practices in different areas (civil law, commercial law, labour law, etc.), which may imply responsibilities from a data protection perspective, and thus help identify the data controller. Among its examples, it specifically mentions an employer in relation to processing personal data about its employees.[123] But as discussed above when introducing the autonomous concept, the same EDPB had indicated that although external legal sources could help identify a controller, this should not be prejudiced by other concepts in other fields of law, with which it may sometimes collide or overlap.[124]

In short, making an easy attribution such as "employer equals controller" would create a scenario where EU Data Protection Law may be easily circumvented by a simple company group setup. So, although the EDPB indicates that when entities interact with employees, they would generally be the ones determining purposes and means, these are not decisive, and the use of the word 'generally' implies that it might not always be the case. Even when a contract may contain an explicit statement as to who is identified as data controller, it is not possible to either become controller or escape the obligations when the factual circumstances prove so.[125] Navigating this issue within a group of undertakings will be the core of chapter 5.

Still related to determination, the EDPB clarifies that even when a data processor offers services which are preliminary standardised in a specific way, the fact that the controller will be presented with a detailed description of the services and make the final decision to actively approve is what makes it indeed the data controller. The processor will be limited in its tasks and cannot change any of the essential elements of a processing operation without the controller's approval.[126]

4.2.3 The Concept of Joint Controllers

The GDPR recognizes that purposes and means can be determined by several different entities for the same processing, each of them subject to data protection provisions.[127] Although the notion already existed in Article 2(d) DPD, Article 26(1) GDPR presents an organised allocation of duties by indicating that the controllers involved shall determine their responsibilities in a transparent manner and provide the data subjects clear information about their rights and how to enforce them.

This arrangement –whose legal form is not specified by the GDPR– is supposed to be the result of converging decisions complementing each other and necessary for the processing to

[123] ibid 27.
[124] See Section 4.1 above.
[125] Controller Guidelines (n 5) para 27-28.
[126] ibid 30.
[127] ibid 31.

take place as to have a tangible impact on the determination of purposes and means of processing. This means whether the processing would not be possible without both parties' participation, in the sense that the processing by each party is inseparable or inextricably linked.[128]

Article 26(1) GDPR presupposes that the actors involved are willing to take the responsibilities involved, assign sufficient resources, and implement the necessary measures to comply. To avoid situations where the responsibilities may be circumvented, part (2) imposes the duty of ensuring that the arrangement of joint controllership reflects the respective roles, and part (3) allows the data subjects to exercise their rights in respect to any of the controllers involved. In essence, the regulatory idea behind the article is avoiding the risk of an "accountability vacuum" when multiple players take part in determining and structuring the processing operations but are not willing to take responsibility for it.[129]

Although the EDPB explains that the assessment of joint controllership should be carried out on a factual analysis of the actual influence,[130] the problem still resides on the fact the arrangement requires the will of the actors involved and its communication to the competent DPA. Without doubting the DPA's enforcement power, it seems improbable that they would analyse and verify the relations between entities as potential joint controllers, unless these had already circumvented the legislation. In the meantime, the parties will probably allocate their responsibilities according to how they interpret the specific scenarios, which may still not reflect the reality.

An interesting note in relation to groups of undertakings is that, according to the EDPB, the use of a common data processing system, shared database or common infrastructure will not always lead to joint controllership if the processing is separable and could be performed by one party without the other's intervention, and each entity independently determines its own purposes.[131] If all entities in the group shared a database where each entity could enter data of its own subjects and decide independently on the access, retention periods, correction and deletion, and could not access or use the other entities' data, they would all be separate controllers (but the parent company, which seems to be data processor). This proves that, to assess the real situation within a group of entities, the level of scrutiny must be highly detailed.

4.2.4 Purpose and Means

[128] Controller Guidelines (n 5) paras 50 and 55.
[129] Christian Kurtz and others, 'Accountability of platform providers for unlawful personal data processing in their ecosystems-A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR' (2022) Journal of Responsible Technology Volume 9, April 2022, ScienceDirect - Elsevier <https://www.sciencedirect.com/science/article/pii/S2666659621000111> accessed 14 March 2022.
[130] Controller Guidelines (n 5) para 52.
[131] ibid 68 and 71.

"Purpose and means" refers to being the object of the controller's influence. While purpose refers to the anticipated outcome intended, means refers to how that result will be obtained. When only one entity determines purposes and means and entrusts another entity with the execution of the processing operations under detailed instructions, the situation is straightforward and there should not be any doubts as to who is the processor and who is the controller.[132] In relation to purpose, this was already discussed under 4.2.2, when answering to 'why' the processing occurs.

When it comes to means, there is an important distinction to make: essential or non-essential. The EDPB explains that essential means are those closely linked to the purpose and scope of the processing: which types of data are being processed, for how long they will be stored, from what category of data subjects, to whom they will be transferred, etc. Because of these close links to the purpose, they can only be selected by the controller. On the contrary, non-essential means are other practical aspects related to the implementation, such as what types of hardware and software should be used, which security measures should be implemented, etc., and can be left to the data processor without any alteration in their roles.[133]

4.2.5 Of the Processing of Personal Data

Although obvious, the four other elements covered above should be in relation to the processing of personal data. The processing of personal data is defined in the GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data", and also gives examples such as collection, recording, storage, consultation, use, disclosure, destruction, etc.[134] The distinction between operation or set of operations is not minor in the practice, because a controller could either be linked to a set of operations on a 'macro' level, or to deconstructed 'micro' processing operations.[135]

Imagine that, for the purposes of acquiring new talents, a company performs recruitment activities to evaluate candidates for a position. This recruitment should be considered as a complex processing activity on a 'macro' level which, on a micro-level, is composed of multiple processing operations such as collecting data from candidate's job applications, structuring the data to make comparisons, recording short video presentations from the candidates, storing their CVs, sharing them with the relevant manager, etc. Because the GDPR does not give any specific instructions about the level of meticulousness required by the controllers, this analysis is left to the interpretation of the controllers and any guidelines provided by the DPAs.

[132] ibid 33 and 38.
[133] ibid 40.
[134] Article 4(2) GDPR.
[135] Controller Guidelines (n 5) para 44.

When dismembering “macro” operations, this could result in multiple purposes or even controllers. For example, a multinational company from Member State A hires an employee for its recently opened subsidiary in Member State B. Most of the personal data required from the employee is based on requirements to comply with local Member State B legislation, but the parent company also asks the employee to provide its gender to be used for a group-wide study to promote equal gender opportunities. While most of the types of data were collected by the subsidiary to comply with local law and probably using ‘legal obligation’ as a legal basis, ‘gender’ was collected either with the employee’s consent or based on a legitimate interest and might have even been determined by the parent company instead of the subsidiary (which is the employer). Thus, considering the collection of personal data from an employee during the onboarding as a single “macro” processing activity may overlook the fact that the ‘gender’ data is collected for other purposes and will be shared with the holding company.

The lack of clarifications at EU-level leaves allows the very own undertakings to perform this scrutiny in the degree they deem necessary, unless the DPAs had provided country-specific rules. A good practice is that the more complex the processing is, the more detailed the ROPA should be. Although several entities’ approach is based on the software programs used, the French *Commission National de l’Informatique et des Libertés* (‘CNIL’) recommends identifying processing activities “by its end”, which requires a higher level of detail.[136] Once again, diverse interpretations in Member States may attempt against uniform application of EU Law.

Before diving deeper into this, I will briefly comment on two more GDPR roles which will be key to understanding chapter 5.

4.3 The Data Processor

Data processors are a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.[137] This requires a separate entity or external organisation, and the fact that the data is being processed on behalf of the controller’s behalf and under its specific instructions.[138] As seen under 4.2.1, an establishment can be a processor to another establishment acting as a controller, both being separate entities. Also mentioned under 4.2.4, the data processor may determine non-essential means in relation to the processing operations they perform, as long as they are following the instructions provided by data controllers in relation to essential means.

[136] CNIL, ‘Record of processing activities’ (*GDPR Toolkit*, 19 August 2019) <https://www.cnil.fr/en/record-processing-activities> accessed 24 April 2022.
[137] Article 4(8) GDPR.
[138] Controller Guidelines (n 5) para 76.

An interesting note is that according to the CJEU's case law, it is not necessary for the controller to have access to the data being processed by one of its data processors to qualify as data controller.[139]

4.4 Third Parties and Data Recipients

The final concepts are the ones of third party and data recipients. The GDPR does not regulate obligations and responsibilities for these two, which are used as relative concepts which describe a relation with a controller or processor.[140]

Article 4(10) GDPR defines 'third party' as a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the controller or processor's direct authority, are authorised to process data. The EDPB explains that "persons who are authorised to process personal data under the direct authority of the controller or processor" is generally understood as persons that belong to the "legal entity" of the controller or the processor.[141] In short, it refers to someone who is not the data subject, controller, processor, or employee of these last two.

In the context of a group of undertakings, once again we rely on the EDPB's interpretation of the terms used. Recalling my observation under 4.2.1, the term 'separate entity' used by the EDPB did not refer to a legal person in strict terms but an entity within a company in line with the concept of establishment, such as a branch. The fact that on this occasion the EDPB chooses to add the term 'legal' before 'entity' presents a new question: does 'legal entity' in this case include or exclude branches? Considering a branch as a third party is problematic because they are technically still part of the same legal entity under company law and the employees receiving the personal data from the controller or processor would also be employees of the same legal person, so they should be excluded according to my paragraph above. The other possible lecture is that the EDPB considered that, within a group of undertakings, a branch would also qualify as a (separate) 'legal entity' and therefore could be a third party. But this leap might not even be necessary.

The EDPB explains that when receiving personal data from a controller or processor, a third party will then be considered a controller in its own right for the processing that it carries out for its own purposes. It even says that in a "company group" (the term chosen), a "company" other than the controller or processor would be a third party, even when it belongs to the same group.[142] If we followed my reasoning under 3.2.2 where branches could be deemed data

[139] Case C-210/16 *Wirtschaftsakademie* [2018] EU:C:2018:388, para 38.
[140] Controller Guidelines (n 5) para 85.
[141] ibid 88.
[142] ibid 89.

controllers, even if branches could not be considered “third parties” they would be recipients of the personal data anyway, and required to comply with the GDPR for their processing activities.

Article 4(9) GDPR defines recipients as a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not.[143] Because recipients do not need to necessarily be third parties, it includes independent controllers, joint controllers, or processors to whom data is transferred or disclosed.[144] For groups of undertakings, it is important to stress that entities in all possible interactions would be recipients according to the GDPR, while they might also be third parties (independent data controllers), joint controllers or data processors when they process such data.

[143] Although it also excludes public authorities acting in accordance with Union or Member State law.
[144] WP29, ‘Guidelines on transparency under Regulation 2016/679’ WP260 rev.01 adopted on 29 November 2017 as last revised and adopted on 11 April 2018, page 37.

5. Applying the Roles within a Group of Undertakings

Finally, we have arrived at the most exciting part of this work. After navigating through the notions of groups of undertakings in EU Data Protection Law and some basic concepts of company law, it is now time to see how these apply and interplay within the entities that compose a group of undertakings.

Groups of undertakings may be composed by multiple legal entities, either natural or legal persons, who could be deemed data controllers but, for legal persons, also their internal 'entities' could also be deemed independent controllers. My analysis will attempt to illustrate the situation of branches and subsidiaries within these corporate organisations, and how they should navigate the EU Data Protection Law obligations. Hopefully, its results will help identify the scenarios where branches and subsidiaries may be data controllers within a group of undertakings, and how their interactions involving personal data conditionate their roles.

Undertakings process and share several types of data within their groups, which may vary according to different business models, but it is hard to find an undertaking which does not process data from their own employees. Employee data is attractive not only for the special considerations in the GDPR that delegate faculties to Member States to further regulate processing in the context of employment and groups of undertakings,[145] but also because national law may require specific uses for it based on obligations under employment and tax law, setting them at the core of their activities. Despite this, I will be open-minded to investigate other types of personal data that may flow from one entity to another within a group of undertakings during my analysis.

5.1 Groups of Undertakings Using Personal Data at EU Level

Whenever an undertaking operating locally wishes to expand, one of its first steps may be setting up an establishment in another Member State which may take the form of a branch or a subsidiary. This choice will determine whether the establishment will be part of the same legal person or not, and in principle also determine which entity will have responsibility to comply with local obligations under employment and tax law. And although easily overlooked, along with these lie the personal data protection obligations.

Once the establishments are up and running, undertakings generally share synergies which may entail the disclosure of personal data to different entities of the group tasked with specific projects (which may be the main office, but not necessarily). Groups may structure

[145] Article 88 GDPR.

their data processing operations in various ways: centralize or keep sensitive data in each establishment, limit the other establishments' access to databases, maintain data inside or outside the EEA, etc. The level of autonomy and possibility to determine purposes and means will determine who is the controller in each case, based on a case-by-case evaluation. Thus, controllers may have establishments across the EU following their instructions,[146] but also entities of the groups may qualify as separate controllers.[147]

I will proceed by methodologically analysing complex "group set-ups" including branches and subsidiaries. For each case, I will first analyse the entities as subjects of EU Data Protection Law (4.2.1), the capacity to determine purpose (4.2.2) and essential and non-essential means (4.2.4) to establish if these can be deemed controllers, how these entities relate to one another other and potential consequences. After being covered under 4.2.5, the level of scrutiny in each scenario will not be further discussed, but the potential joint controllership scenarios (4.2.3) will be addressed while discussing relations between these entities.

To help the reader, I will begin with the very basic scenarios of a single undertaking and two independent undertakings, to set up the stage properly and illustrate the different possible relations.

5.2 Single Undertaking

Imagine we have a single undertaking which collects and processes personal data without any other undertaking's intervention and stores it without any intention of disclosure other than what is required by the law. In line with 4.2.1 and based on the focus of my work, this undertaking may be an individual, a business or even a company, depending on the company law structures attached to it by the law (if any). For any processing activity in the context of its business (from employees, users, customers, suppliers, etc.), there would be no doubt as to who is "in charge" as a subject of EU Data Protection Law.

As a potential employer, this undertaking may collect several personal data connected to legal obligations imposed to it for that relation as well as other legitimate interests it pursues. But either imposed by the law or its own will, it should be clear who has the power to determine the processing operations. Being the only undertaking linked to these, it is also straightforward to see that it will be the one choosing both essential and non-essential means.

Because this undertaking checks the elements contained in the definition of a data controller, it may unquestionably be deemed as such.

[146] Recital (19) DPD.
[147] International Transfer Guidelines (n 85) 16.

5.3 Two Independent Undertakings

When two independent organisations with their own business goals, structures, etc., are involved in the same processing activity, the way in which they interact may result in the allocation of different roles under EU Data Protection Law. For each case, it will be important to consider the degree of independence, the way personal data is processed and the control over the content of the data.

5.3.1 The Controller – Processor Relation

This relation requires two key elements: separate legal entities and the processing being performed by the processor on the controllers' behalf.[148]

Imagine that Undertaking A decides to get an IT platform where new hires can be onboarded without its HR Department's intervention. They reach out to Undertaking B, an independent company who sells this kind of service, and agree on its implementation. In the practice, Undertaking A's new employees will complete their personal data on a platform provided by Undertaking B, who will store it and place it at Undertaking A's behest. Data will be handled by both undertakings, but in a different capacity.

The EDPB explains that the "processing done on the controller's behalf" also requires that it is being done for the controller's benefit and under its direct authority or control by recalling the concept of "delegation", reflected in our example.[149] Following the elements of 4.2, although both undertakings as legal persons may be deemed controllers, the fact that the processing is done by Undertaking B as a delegation and for the benefit of Undertaking A indicates that Undertaking A has main control and power to "determine" the processing operation. Ideally, Undertakings A and B would celebrate a data processing agreement prior to any processing activities where they would define their roles, essential and non-essential means.

In summary, when the relation entails an undertaking doing something on another undertaking's behalf and under its direction, we will be in the presence of a controller-processor relationship. In our example, Undertaking A would be the controller and Undertaking B the processor.

5.3.2 The Controller to Third Party Scenario

Another interaction is where a data controller transfers or discloses data to a third party who will later process that same personal data for other purposes. With two different undertakings involved, it might be relevant to check their involvement.

[148] Controller Guidelines (n 5) para 76.
[149] ibid 79-80.

A useful example could be a travel company which provides services for other businesses. Undertaking A enters into an agreement with Undertaking B, who handles bookings for Undertaking A's employees whenever they need to travel in the course of their activities. Although Company A may share the required data from its own employees and determine purposes similar to what we have seen in 5.3.1, in this case Undertaking B processes the personal data in the context of its own services, such as booking airline tickets, hotel reservations, etc. Undertaking B will also independently determine the categories of data required and how long these will be retained.

Because of the degree of independence and the fact that it will process personal data for its own purposes, this scenario is different from the controller-processor relation. Here, each undertaking will exercise control over the purposes and the way it is being processed and be responsible to comply with its obligations as controller. Without getting too involved with data transfers yet, it might be relevant for both these undertakings to have a data transfer agreement to ensure that the data disclosed will be properly safeguarded. Depending on the frequency of data flows between them, the scale or the inclusion of sensitive personal data, their approach may vary.

5.3.3 The Joint Controllers Scenario

When purposes and means are determined by more than one actor, these may be joint controllers and both subject to the applicable provisions.[150] As seen under 4.2.3, this may result from an agreement between the controllers where their responsibilities are clearly determined and explained to the data subjects, or due to the factual elements of the case.

An example to imagine joint controllership could be an agreement between Undertaking A, which provides services as an airline, and Undertaking B, a luxury hotel chain. Both undertakings, although being separate legal persons, decide to sell a specific package where customers can register and get a discount for choosing the services of both undertakings together. Both undertakings will have access to the data collected from customers and will use it independently to perform their own separate activities. Both have an influence on the early stages of the processing where they collect the information so both should be deemed data controllers for such data collection. To avoid confusion, the GDPR requires them to clarify these responsibilities in a transparent manner so that data subjects can easily enforce their rights.[151]

[150] ibid 31.
[151] Article 26(1) GDPR.

If after the collection any of these undertakings were to further process the personal data for other purposes without the other undertaking's involvement, it should be considered an independent controller as seen in 5.2.

An important takeaway from section 5.3 is that we have only discussed situations where independent undertakings which have a 'horizontal' relation participate in the same processing activity. Within a group of undertakings, these relations may be both horizontal and vertical, as we will see in the following sections.

5.4 Subsidiaries and their Relation to Holding Companies

We have finally reached the stage where we will discuss the situation of 'establishments' according to EU Data Protection Law. Recalling 3.2.2, subsidiaries are considered different legal persons under company law which, based on the principle of 'separate legal personality', could be attributed legal obligations without affecting their holding companies.

At first glance, if a subsidiary –an independent legal person within a group of undertakings– processes personal data without the intervention of any other entity within the group, it is not hard to see why it could be considered an 'undertaking' as well as an independent controller in line with 5.2. Here, any breach of EU Data Protection Law could be attributed, in principle, only to the subsidiary. But although the reasoning of 'one legal person equals one data controller' may seem straightforward, special considerations arise in the context of a 'group of undertakings'.

As seen under chapter 3, the concept of 'group of undertakings' is related to the idea of 'control' as dominant influence, aligned with basic notions of company law.[152] When looking into subsidiaries which relate to each other on a horizontal level within a group, this dominant influence does not seem to interfere in their relation (unless the holding company intervenes), therefore allowing the scenarios mentioned under 5.3: controller-third parties, controller-processors or even joint controllers, based on the factual circumstances. Due to the lack of specific rules for groups of undertakings, any data disclosures are in principle regulated by the GDPR in the same way as two independent undertakings.[153]

But the keynote here is the vertical relation between a subsidiary and a holding company. The dominant influence resulting from their relation may not only allow data to flow between these two entities but, on a group structure, may also influence –and potentially help circumvent– data flows between subsidiaries on a horizontal level. For example, Subsidiary A may have an agreement with its holding company which then becomes data controller for the

[152] See Recital (37) GDPR.
[153] Recital (48) GDPR.

data received and decides to share it with Subsidiary B, resulting in data being triangulated to subsidiaries through the holding company. This section will concentrate on this vertical relation between subsidiaries and their holding companies.

5.4.1 Can they be Data Controllers?

5.4.1.1 Holding Company and Subsidiary as Potential Controllers

Being separate legal persons with legal capacity to contract obligations, both can be subjects of EU Data Protection obligations.

The position of the holding company as data controller, not only for its own activities but also on behalf of its establishments, is reflected on the GDPR which, by saying "the processing of personal data in the context of the activities of an establishment of a controller or processor", indicates that controllers may have their own "sub-entities" in the form of establishments.[154]

On the other hand, the possibility of a subsidiary as controller derives from the GDPR's recitals and is further developed by the EDPB's guidelines.[155]

5.4.1.2 Power to "Determine"

The ability to assert determination may be one of the most complex issues in a group structure because, as previously shown, determination refers to a specific processing activity.[156] The question is how that determination may be influenced by a general 'control' by the holding company.

As exemplified in 4.2.5, a holding company may require information from employees of its subsidiaries across the world to perform a study in relation to female representation in the workplace to ensure equal opportunities. Even though subsidiaries may already hold that data from its employees, it is evident that the holding company is the one processing the data for such study and it surely obtained it from the subsidiary based on its controlling influence over it.

5.4.1.2.1 Employer as Data Controller

Unless stated otherwise, the initial personal data collection from employees seems to be related to the specific legal person who hires them. To be lawful, it should be based on any legal basis from Article 6 GDPR. If such collection was minimal and based on the completion of legal obligations (c) or in order to fulfil a contract with the employee (b) it would be relatively straightforward, but if the employer relied on the employees' consent (a) or legitimate interests

[154] See Recital (124) GDPR.
[155] Controller Guidelines (n 5) para 17 and recital (22) GDPR.
[156] See 4.2.2.

(d), extra work may be required.[157] So far, it is clear to see that the employer may well be the data controller, which would be the most common scenario. But depending on the factual circumstances in each case, the employer on the papers may not be the factual data controller and it would be required to 'pierce through the corporate veil' using an approach similar to *Google Spain* to identify the real data controller (and perhaps also real employer).[158]

A holding company from Member State A may have initiated activities and decided to collect data from employees during onboarding according to the laws of such Member State. If the exact same processing activity were to be replicated for a subsidiary of the group operating on Member State B where legal requirements were different, the legality from some sets of data collected may require other precautions from the controller. Here we can also see how the different levels of scrutiny over a processing activity may produce different analytical results.[159]

5.4.1.3 Determination of Purposes and Essential Means

Without doubt, any of these legal persons can determine the purposes as well as essential and non-essential means. As discussed under 4.2.4, how the latter are structured will help identify the corresponding role for the entity within the group, as we will see in the following sub section.

5.4.2 Data Processing Relations Between Subsidiaries and Holding Companies

These sections will address the scenarios from 5.3 when directly applied to the subsidiary-holding company relation.

5.4.2.1 Data Controller – Data Processor

In this bilateral relation, there are two potential results: where the subsidiary is the data controller and the holding company the processor, or vice versa. Within a group of undertakings and both entities being separate legal persons, a data processing agreement may be crucial to regulate this relation, which may even be part of a broader inter group agreement or even binding corporate rules approved by the corresponding DPA.

According to the WP29, the establishment of an undertaking with overall control (in company law terms) should be presumed as the decision-making centre related to the processing of personal data, except where decisions are taken by other establishments.[160] The

[157] Article 6 GDPR.
[158] *Google Spain* (n 38).
[159] See 4.2.5.
[160] Lead Supervisory Authority Guidelines (n 57) 7.

WP29 also underlined that controllership was a consequence of the factual circumstance than an entity choosing to process personal data for its own purposes.[161]

A holding company may decide to use one of its subsidiaries as a data processor, for example for the latter to store data of all their clients worldwide. Here the holding company is providing the instructions and clearly acting as a data controller.

But the type of data involved in the operation may be decisive: if instead the holding company was asking its subsidiary to store personal data of all group employees worldwide, the subsidiary would certainly remain processor in relation to personal data from the other group entities, but not so clear in relation to data of its own employees which may have been initially collected to comply with other legal obligations.[162] Can the subsidiary still be considered processor for the data of its own employees? If it is based on legal obligations, I would not think so. Is the holding company the one determining the processing based on its influence under company law? In this case we might be closer to a joint controllership, soon to be covered in 5.4.2.2.

The opposite scenario would be when a subsidiary, as controller of personal data, decides to have that data processed by the holding company, which for example hosts a central database. The EDPB indicated that the mere fact that data is stored in a database administered by the holding company does not necessarily mean that the holding company is a controller because subsidiaries may well decide independently on the access, retention periods, correction, and deletion, making the parent company a mere processor of such data. But if the holding company required processing some of that data for any other internal purposes, it would be hard to say that it is merely a data processor.[163]

The use of employee data again presents an interesting note: the subsidiary would not be able to escape being a controller for data of its own employees in the system but, in practice, the principal may be the one determining the purposes and essential means and perhaps even exceeding the data required merely for concluding an employment agreement. This could also lead to the principal being primarily responsible for the data in the central database, while the subsidiaries would be jointly responsible only for the parts of the central data system that concerns their employee's data.[164]

Another element to consider is that, imagining a group of undertakings where every subsidiary followed the instructions of its holding company in different jurisdictions may raise some suspicions as to which entity in the group actually has the influence to determine the

[161] Opinion on concepts of controller and processor (n 106) 8.
[162] In line with the definition of data controller in Article 4(7) GDPR.
[163] Controller Guidelines (n 5) para 71. See also International Transfer Guidelines (n 85) 16.
[164] Moerel, 'Back to basics: when does EU data protection law apply?' (n 26) 107.

processing operations, and where the 'control' from company law may be exerting some influence on the individual controllership on the specific processing activities of its entities.

In summary, the use of common processing systems in groups of undertakings may indicate any of the scenarios seen under 5.3 depending on the factual situations,[165] and if the authorities understood that it was in the context of the activity of an EU establishment, GDPR would apply.[166] The key for a controller-processor relation are clear instructions in relation to purposes and essential means included in the corresponding data processing agreement.

5.4.2.2 Joint Controllers

The EDPB expressly recognizes the possibility for "companies which are part of a group" (or groups of undertakings) to be joint controllers, given the right factual circumstances.[167]

In line with 4.2.3, if both entities are involved in a processing operation and their wills are inseparable or inextricably linked, they should be deemed joint controllers. On the contrary, if the processing can be separable or could be performed by one party without the other's intervention and each entity independently determined its own purposes, they may simply be independent controllers.[168]

In a vertical relation within a group of undertakings, the factual situations of the case will be the ones that determine the roles from the GDPR. Once again, the shared database between subsidiaries and holding companies may or may not entail joint controllership. Data from the subsidiary's employees will undoubtedly be controlled by the subsidiary as an employer, but joint controllership may arise if the holding company influenced the processing activity by taking substantial decisions about the purposes and means involved.[169]

The level of scrutiny on the processing activity per se (as seen in 4.2.5) may show different results: if the subsidiary claims to collect data based on legal tax or employment obligations but also processes some extra types of data based on instructions provided by the holding company, a detailed ROPA may help separate the micro-level processing operations and deem the holding company as a processor or even an independent controller. On the contrary, a macro-level perspective may indicate joint controllership of the personal data. The CJEU explained that when multiple operators are involved in the operation at different stages of that

[165] Controller Guidelines (n 5) para 68 and 71.
[166] Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (n 30) 30.
[167] Controller Guidelines (n 5) para 71.
[168] ibid 68 and 71.
[169] See 5.4.2.1.

processing, each of them must be assessed, opening to the possibility that they will only be joint controllers for those stages they determine together, and separate for the rest.[170]

One thing is clear: the subsidiary, as an employer, cannot escape responsibility as a controller from data of its own employees based on a legal obligation, up to the point where data is transferred to another entity (third party) which will act as an independent controller, the scenario that will be covered on the following sub section.

5.4.2.3 Data Controller to Third Party

The last possibility is that a holding company or subsidiary should be considered independent data controllers after one of the entities disclosed personal data to one another. While joint controllership required converging decisions, this disclosure/transfer implies that the first entity already had the personal data and decided to share it with its counterpart based on one of the legal bases from the GDPR.[171] This decision to share the data is made by the first entity, although the conditions for potential uses by the third party should probably be part of a data transfer agreement (which may lead to contractual responsibilities). Within a group, these disclosures between entities (intra-group disclosures) may constitute a transfer of personal data according to the EDPB.[172] Once the transfer is concluded, each controller would be responsible for their own obligations based on the principle of separate legal personality, and to the extent of their own personas. As commented in 3.2, if any of these entities had acted like a "shell" to circumvent data protection obligations, 'piercing of the corporate veil' should help indicate who the real controller is, leading to a potential extension of the legal obligations.

The EDPB exemplifies that when subsidiaries process personal data of their respective employees for administration purposes but then share this data with their parent company (at its request) for group wide statistics, the parent company should be considered as a third party regardless of the fact that companies are part of the same group.[173] The collection of the data by the subsidiary prior to the disclosure with the holding company would be a determinant factor, but if the holding company had influenced the types of data to be collected by the subsidiary this would become less clear.

Another factor in this scenario might be the periodicity and scale of the data sharing. While 'one-offs', small-scaled and low-risk disclosures may seem straightforward, systemic sharing on a large scale implies a closer relation and need for further scrutiny.

---

[170] According to the Controller Guidelines (n 5) para 58, although not providing the explicit case where this was decided.
[171] Article 6 GDPR.
[172] International Transfer Guidelines (n 85) 16.
[173] Controller Guidelines (n 5) para 89.

A final observation is that when subsidiaries are located outside the EU, any of the three relations from 5.3 would be very similar, although further requirements should be in place to ensure the safe disclosure of personal data to third countries.[174]

5.5 Branches and their Relationship with Parent Companies

Although similar to subsidiaries and holding companies, the distinctive element for branches is that they belong to the same legal person as their own parent company and should be seen as entities within it, although having a higher degree of independence than departments or areas within a company.[175] In the internal market, branches are key for EU-based companies to expand their operations to other Member States.

Returning to our dilemma under 3.2.2, branches can be establishments and thus data controllers, despite being mere extensions of the same legal person/undertaking.

Although assigning responsibilities to an entity independent enough to conduct business – despite having a link to the parent company– makes sense from the EU Data Protection Law perspective to ensure that entities which effectively determine the processing of personal data are compliant, the fact that both entities are technically the same legal person leaves more questions than solutions. Some of these will be addressed under 5.5.2 because they are key to understanding the relations between entities within a single legal person, something I will attempt in 5.5.3.

My proposal for this subchapter is the following: first, assess branches and parent companies as potential data controllers based on the controller definition as previously done for subsidiaries; second, to analyse the conflicts of having coexistent data controllers within the same legal person; and third, to see the relations from 5.3 between entities from the same legal person in detail.

5.5.1 Can they be Data Controllers?

5.5.1.1 Parent Company and Branch as Data Controllers

For the parent company, there should be no doubt that, as a legal person, it may be deemed data controller for the processing activities under its sphere of action according to my analysis under 4.2.1 and 5.2.

[174] In line with Articles 45 and 46 GDPR.
[175] See 4.2.1.

When it comes to branches, the use of the word 'establishment' by the EDPB allows them to be independent data controllers from their parent companies despite not having legal personality.[176]

5.5.1.2 Power to "Determine"

For determination over a specific processing activity, we must observe the factual situations to identify if the operations are influenced by the control from the parent company. As previously discussed, controllership may stem from the law or factual situations of the case.

For example, in relation to an employee working in a branch, it may not even be possible to determine which specific entity is the employer, being branch and parent company the same legal person (despite being assigned to a specific branch). Specific local requirements may require branches to collect data from the employees working in them and the degree of autonomy in these decisions may effectively make them data controllers. Depending on how their operations had been structured, personal data might be stored by the branch itself or even the parent company as part of a shared database.

Based on a real example, an Italian branch is required to collect health data from its employees based on national health and safety obligations imposed on employers. Its parent company based in Denmark does not collect any personal data from its employees located in that Member State because it is not a legal requirement and decides not to intervene in the processing of such sensitive data, leaving it in the hands of the Italian branch. Following *Somafer*, branches have management and are materially equipped to negotiate business with third parties so that others, although acknowledging the legal link with the parent body, can transact business with the branch as an extension of the parent body.[177] In this scenario, it would seem clear that the branch is the one actually handling the personal data required to comply with the obligations, even the liabilities for non-compliance may extend to the parent company.

The initial data collection might also be relevant when branch and parent company are not located in the same Member State. Although under the sphere of the same legal person, if an employee is providing data to the branch in its home country, it should be clear that the data will be disclosed to the parent company in another Member State (or perhaps even outside the EU), but this will be discussed under 5.5.2.5.

As seen for subsidiaries, if undertakings attempted to collect the least data possible from its subjects (employers) based on legal and contractual obligations but have a standard form

[176] Controller Guidelines (n 5) para 17. See also 3.2.2.
[177] *Somafer SA* (n 78) 12.

applied to all its branches in different Member States, the level of influence would seem to be greater from the parent company rather than each branch.

Despite the distinction between entities within the same legal person is problematic, it seems that both parent company and branch may have capacity to determine certain processing obligations independently.

5.5.1.3 Determination of Purposes and Essential Means

The independent capacity to negotiate business and existence of management give branches an autonomy that could allow them to choose purposes and means of a processing activity.[178] The internal structure of an undertaking (or group) will provide the factual circumstances necessary to identify the level of dependency between a branch and a parent company, as will be covered under 5.5.3.

5.5.2 The Coexistence of Data Controllers within a Single Legal Person

Led to believe that, under the right circumstances, branches may be independent data controllers, I will enunciate some of the legal problems that may arise from the coexistence of independent controllers within a single legal person to provide some context before moving onto the potential relations these may have.

5.5.2.1 'Group of Undertakings' vs Internal Undertaking Organisation

With 3.3 in consideration, it might be worth pointing out that while the concept of 'group of undertakings' seems perfectly fitting for a group structure which encompasses several legal persons, it might not be the same for a branch-structured organisation which comprehends one single legal person. If a legal person/company which initially operated business in one Member State decided to open branches in eight other Member States, we might be in the presence of an eight-armed structure which may organisationally look similar to a group of undertakings composed by several subsidiaries, but where everything happens within the "internal" realm of a single legal person.

Can this scenario also be comprehended by the concept 'group of undertakings'? Using the concept of undertaking from EU Competition Law,[179] every branch could be considered an independent undertaking because it is an entity engaged in an economic activity regardless of its legal status. But as Ezrachi explains in the context of EU Competition Law, the application of a "single economic entity" to groups of companies may collide with the "internal allocation

[178] ibid.
[179] *Ministero dell'Economia e delle Finanze v. Cassa di Risparmio di Firenze SpA and Others* (n 90) 107.

of functions" within a single economic unit.[180] I am inclined to believe that because branches can be independent data controllers, their relations should not be considered merely "internal allocation of functions" but proper relations between undertakings subject to the rules of EU Data Protection Law.

5.5.2.2 A Single Legal Person Composed by Several Entities

Assigning a data controller role to a branch means the attribution of obligations to specific entities within the same legal person, which collides the whole concept of independent legal personality from company law. This is not only a theoretical challenge, but also one with several practical implications. Each branch autonomous enough to be a controller for data processing should fully comply with GDPR, making it extremely complex and resource demanding. For potential "transfers" or data disclosures, these independent controllers may well be at both ends of a relation, being the same legal person.

5.5.2.3 A Single Legal Person in Multiple Jurisdictions

A (parent) company which opens branches across several Member States is in fact a single legal person existent in multiple jurisdictions. With the GDPR regulating the free movement of data within the Union, there is a presumption that data is protected while being within the interal market. However, this might not be the case when the single legal person has a presence outside the EU, something I will address in 5.5.2.6.

5.5.2.4 Compliance Obligations for Every Entity

To what extent should each of these entities, as independent data controllers, comply with the obligations imposed by the GDPR? Should every branch have its own independent ROPA?[181] Should it produce its very own impact assessments?[182] Should it keep a log of every data disclosure made to any other branch part of the same group of undertakings?

The GDPR includes a derogation for organisations or enterprises with less that 250 employees in relation to record-keeping to alleviate some of these responsibilities for small and medium-sized enterprises.[183] Nonetheless, it does not apply if the processing is likely to result in a risk to the rights and freedoms of the data subjects, is "not occasional" or includes special categories of personal data or criminal convictions and offences.[184] Within a group of undertakings, while the risky processing may be contained when processing is kept within the

[180] Ezrachi (n 91) 2.
[181] Article 30(1) GDPR.
[182] Article 35 GDPR.
[183] Recital (13) and Article 30(5) GDPR.
[184] Articles 9 and 10 GDPR.

EU and the processing of special categories of personal data can be avoided when using a data minimisation approach, it would still be hard to qualify data flows between entities as "occasional". Besides, the choice of words "enterprise" or "organisation" does not clarify if this refers to a data controller, an establishment, or an entity.

This derogation based on the number of employees presents another interesting discussion: should the number of employees be the determining factor to derogate GDPR obligations? A branch may only have a few employees but process data from millions of users in the region where it conducts business. Perhaps the number of processing operations or their potential risks to the data subjects would be a better parameter to determine the level of compliance required.

Because aside from Article 30(5) the GDPR and the EDPB do not address the level of compliance required by branches, I am inclined to believe that when acting as an independent controller, their obligations should not be waived only because they occur within the same legal person. A data subject may want to understand why its personal data is being processed in another Member State after having entered a relation with a branch on its own, and thus compliance with record-keeping obligations might still be relevant, even if only to provide transparency to the data subjects. This is not a minor topic considering the impact these obligations may have on businesses opening "sufficiently independent" branches able to determine processing operations without the parent company's intervention.

5.5.2.5 Data Flows within a Single Legal Person

Having branches as independent data controllers presents another question: can entities within the same legal person "transfer" data to each other as data controllers? The GDPR introduces the concept of 'cross-border processing' which includes the processing of personal data in the context of activities of establishments in more than one Member State by a controller or processor established in more than one Member State.[185] Although not a "transfer", this concept helps understand and regulate the data flow for establishments within the EU and key in the context of the EU's internal market.[186]

But even this 'cross-border' processing not being a transfer does not entail that compliance with the GDPR should be waived for relations between different controllers which belong to the same legal person or in the context of groups of undertakings. Although the requirements are stricter for data leaving the EEA, if an entity receiving the personal data intends to process

[185] Article 4(23)(a) GDPR.
[186] See recitals (3), (6), (53) and (170) GDPR.

it for its own purposes within the EEA, it will need to comply with record-keeping obligations, observing the legal basis, data minimisation principles, etc.

While the existence of data processing or data transfer agreements may help regulate the relations between subsidiaries,[187] this is less clear for branches where personal data flow towards another Member State but remain within the sphere of the same legal person. The EPDB explains that if the sender and recipient are not different controller/processors, the disclosure of data should not be regarded as a transfer under Chapter V of the GDPR – since data is processed within the same controller/processor.[188] Having established that branches may be independent data controllers/processors, a literal interpretation means that they may be able to "transfer" data to one another. But considering that we are discussing a scenario within the realms of a single legal person and geographically within the EU, this "transfer" seems more in line with the concept of cross-border processing mentioned above.

Can a branch have an agreement to share or to process data on behalf of its parent company or another branch? There should not be a problem for independent controllers but would seem like a futile effort within the sphere of a single legal person. Although internal guidelines and handbooks may help regulate these flows within a branch-structured business, these documents may not be binding.

5.5.2.6 Data Flows Abroad within a Single Legal Person

Although almost overreaching the scope of this thesis, is it hard not to notice the consequences of having a branch outside the EEA involved in the processing activities of an EU-based undertaking. Here, personal data may be geographically leaving the EU although remaining within the same legal person.

The GDPR recognises the legitimate interest to transmit data within a group but explains that when data is transferred to a third country, the general principles of data transfers should apply.[189] Once again, the notion of "transfer" is doubtful when happening within the same legal person.

The EDPB provides an example where an EU-based company's employee travels to a third country for a meeting and during its stay remotely accesses personal data from the company's databases. It explains that this remote access does not qualify as a data transfer because the employee is not a separate controller but a mere employee and thus an integral part of the controller.[190] The rationale behind this seems to be that because the access in a

[187] Article 28 GDPR.
[188] International Transfer Guidelines (n 85) 15.
[189] Recital (48) GDPR.
[190] International Transfer Guidelines (n 85) 14.

third country is occasional, a stringent regulation is not required. But when an EU-based company opens a branch outside the EU and decides to process data from EU data subjects there, it is not an occasional activity according to the GDPR.[191]

Based on the *Bodil Lindqvist* case, the EDPB established a three cumulative criteria to assess if a movement of data could qualify as a transfer: a controller or processor is subject to the GDPR for the processing, the "exporter" makes the data available to the "importer", and the importer is in a third country.[192] The three of them would seem to be applicable in the case of a branch located outside the EU. But despite having two entities which could fit the roles of exporter and importer, can we still refer to it as a "transfer" when there is only on legal person involved? If EU Data Protection Law did not intervene, the GDPR could be easily circumvented by establishing a branch outside the EEA.

The EDPB provides a transfer example using a subsidiary but does not specify if the same scenario applies to branches. It also recognises that although certain data flows may not qualify as a strict "transfer" in accordance with Chapter V GDPR, such processing may still be associated with risks due to conflicting national laws or government access in third countries, as well as difficulties to enforce and obtain redress against entities outside the EU. It continues by saying that the controller is accountable for its processing activities regardless of where they take place and must comply with the GDPR, specifically articles 24, 32, 33, 35 and 48.[193] This is in line with its recommendations regarding the CJEU's ruling in *Schrems II*, that "the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes".[194]

In summary, having a branch abroad is a complex issue from the EU Data Protection Law perspective where even this "non-transfer" of data might require complying with the GDPR in a stricter manner that any other branch within, which resembles the situation of a subsidiary but without the possibility to sign any agreements between "parties" involved.

5.5.2.7 Enforcement

Because branches lack their own independent legal standing, their responsibilities are shared with the parent company, being the sole legal person responsible for the consequences that non-compliance by any of its branches –whether in another Member State or abroad– may bring. In a scenario where the parent is fully compliant with GDPR in its establishment, but the

[191] Recital (22) GDPR.
[192] International Transfer Guidelines (n 85) 7; Case C-101/01 *Bodil Lindqvist* [2003] EU:C:2003:596.
[193] International Transfer Guidelines (n 85) 16-17.
[194] EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' Version 2.0 adopted on 18 June 2021; Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* [2020] EU:C:2020:559.

branch is not, there is still only one responsible to pay the fines for the branches' non-compliance. But the fact that the branch may not "pay" does not mean that it is not capable of determining processing activities by itself. There is no indication by the GDPR that an entity should have its own independent legal standing to be deemed data controller, despite the peculiarity of assigning an obligation to only part of a legal person.

5.5.3 Data Processing Operations Between Branches and Parent Companies

When deemed independent data controllers, branches may, in principle, take part in any of the three relations from 5.3. The difference here is that between branches and their parent companies, data flows never leave the sphere of the same legal person.[195]

Another relevant factor is the level in which they relate to each other. While we concentrated mainly in vertical relations between subsidiaries and holding companies because horizontally these separate legal persons had the same rules as independent undertakings, branches require looking into both levels because they take place within the spectrum of the same legal person. The following sections will analyse both the vertical relations between a branch and a parent company and the horizontal relations between branches part of the same legal person.

5.5.3.1 Data Controller – Data Processor

Considering sufficiently autonomous branches as independent entities within a legal person, nothing prevents them from having a controller-processor relation when one acts on behalf of its counterpart and under clear instructions, as seen under 5.4.2.1.

Does it make sense identifying a controller and a processor within the same legal person? Even when the legal person finally responsible is the same and the potential celebration of a data processing agreement by the same entity on both ends seems impractical, the clear allocation of roles may be fundamental for data subjects to understand where their data was handled and enforce their rights if required.

As to the different levels this relationship may have, we have mentioned the possibility of both a vertical and horizontal relation.

For the first, it would not be hard to imagine a parent company which hosts a central database from employees in all its branches.[196] As long as the instructions, purposes and essential means are determined by the branches, the parent company would remain as a mere processor on their behalf.[197] This would only work as long as the parent company did not

[195] See 5.5.2.5.
[196] Similar to 5.4.2.1 for subsidiaries.
[197] Controller Guidelines (n 5) para 71 and International Transfer Guidelines (n 86) 16.

impose their branches any specific requirements that could condition their processing operations nor decided to use the data collected by them for any other purposes.

It is also possible having a reverse scenario, where a parent company (even one headquartered in a third country) had branches within the EEA and decided to have all the personal data stored in a database hosted by one of its EEA branches to avoid any unnecessary oversharing and minimise data flows. With clearly provided instructions by the parent company, this would still be the data controller and the branch the data processor. This might not be the same when employee data is involved, where it might be hard for a branch to claim merely being a processor for the data from workers operating in its branch.

As for the horizontal-level scenario between branches, imagining a controller-processor relation without any intervention of the parent company would be seen as very unrealistic. Imagine a parent company in Member State A has branches in Member States B and C. If certain processing operations were performed by the branch in Member State B in relation to personal data from data subjects located in Member State C, it would be very hard to sustain that the parent company had not been involved in this decision to determine where the processing operations should take place. The lack of legal separation between entities portrays a scenario where 'control' in terms of company law seems to prevail. Because we are referring to entities within the same legal person and the relation may be guided by internal rules, informing the data subjects in questions that their data is being processed in another Member State (B in our example) would be a step towards the transparency requirements by the GDPR.[198]

5.5.3.2 Joint Controllers

As with subsidiaries, entities using the same database or infrastructure to store personal data does not necessarily entail a joint controller relation if the processing is separable or could have been performed by any of the parties involved without the others' intervention.[199] Following 4.2.3, joint controllership between branches would be possible only if both were involved in the processing and each had decisive influence on whether and how it should take place. But this scenario is confusing given that each entity would be an independent controller but part of the same legal person, and that decisions may be taken by individuals in the parent company.

On a vertical level, although a branch and parent company may have internal rules as to whether and how the processing operation should take place, the idea of joint controllership still feels void knowing that there is only one legal person involved. No matter how detailed the

[198] Article 13 GDPR.
[199] Controller Guidelines (n 5) para 68 and 71.

level of scrutiny is on a processing operation, the fact that all these decisions come from within the sphere of the same legal person may make identifying the determining entity almost impossible, and the legal person responsible for any breaches to the GDPR would still remain unchanged.

Knowing that the parent company may have decisive influence on the branches' actions, perhaps indicating only the parent company as data controller would provide data subjects clear reference to enforce their rights. Nonetheless, the existence of the joint controllers would cause no extra harm, allowing them to exercise their rights against any of them.[200]

5.5.3.3 Data Controller to Third Party

As discussed throughout this paper, the EDPB explains that when receiving personal data from a controller or processor, a third party will then be considered an independent controller for the processing that it carries out for its own purposes. As mentioned earlier, it is a common practice to share some data with parent companies for group-wide statistics, where the parent company should be considered as a third party regardless of being part of the same group.[201]

Even with no actual 'transfer', any entity within the group would be turned into an independent from the moment it started processing such data for other purposes (even if it is merely storage, unless it had been instructed to do so as a processor as seen under 5.5.3.1), and thus required to comply with GDPR. In this context, a vertical or horizontal relation would not make a difference.

While data may freely flow from entities across several Member States (as cross-border processing) within the EEA without affecting the data subjects as long as they had been properly informed, the disclosure to offices outside the EEA might require more work, as commented in 5.5.2.6.

[200] Following Article 23(3) GDPR.
[201] Controller Guidelines (n 5) para 89. See also 4.4.

6. Conclusions

After this journey into the concept of 'group of undertakings' and EU Data Protection Law, I will attempt to answer my research questions.

6.1 The Entities within a Group of Undertakings which may be Data Controllers

Despite navigating the different use of concepts from the GDPR, the EDPB and EU Law in general, the existing framework for groups of undertakings seems to indicate that both subsidiaries and branches may be deemed controllers if their internal organisational structures allowed them to determine purposes and essential means of processing operations. While this was straightforward for subsidiaries with independent legal standing, a combined interpretation of the GDPR and the EDPB's guidelines was required to consider branches as controllers when given the right factual conditions (having their own management, being equipped to negotiate business).[202] However, this recognition has not yet been fully developed by EU Data Protection Law nor addressed by the WP29 nor EDPB.

Despite this, allowing branches as data controllers also has a benefit: because they generally act on a specific geographical area, the allocation of responsibilities to decentralised entities ensures that the controller is subject to the laws that data subjects are familiar with, helping to ensure their rights.

6.2 Who is Responsible for the GDPR Compliance in a Group of Undertakings?

In what may be a disappointing result, both controllers and processors are required to comply with GDPR obligations under Chapter 4 based on their roles, meaning that all the entities within a group which process personal data must comply up to the extent based on its intervention. But to determine which entity has each role, it is necessary to investigate each relationship, how groups structure processing operations across different establishments, and any influence that may be exerted by a principal in a vertical relation over specific processing operations. An analysis on a micro-level may also impact these results.[203]

With GDPR placing obligations based on a functional approach, entities may be controllers or processors for different processing operations. For every controller, compliance would require the implementation of data protection by default and by design, observing the principles of data minimisation, transparency, keeping a ROPA, respecting the access rights by individuals, performing impact assessments, celebrating agreements with processors, and the list goes on. The "advantage" here is that for every establishment acting as an independent

[202] See *Somafer SA* (n 78) 12.
[203] See 4.2.5.

controller, these obligations may only apply for the specific operations where they determine the purpose and essential means, although the challenge may reside in identifying the decision-making source for each. Nonetheless, if an establishment merely adhered to its principal's practices, it may be perceived as not being the one making the final decision on the specific operation.

With the GDPR lacking specific rules for groups of undertakings, their obligations and relations are regulated as for any other independent controller and do not seem to be indulgent just for being part of the same group or even the same legal person.

6.3 Interplay of GDPR Roles in Groups of Undertakings

For each possible relationship between entities, the analysis of the factual elements might be the only way to effectively determine who acts as a controller. The influence exerted from a vertical relationship, the autonomy of an establishment to determine processing operations and the imposition of legal obligations (for example for employers to collect data) will guide this assessment.

Common databases are a perfect example: based on the specific system, who operates it, who predetermined the data to be collected, access rights, etc., entities may be in any of the different relationships mentioned under 5.3. But when based on a legal obligation such as employment for example, the employer may not escape its role as a controller for the personal data of its employees.

Regulating entity relations also differs from subsidiaries to branches. While the former as independent legal persons may use agreements or even binding corporate rules,[204] the latter may incline for internal rules instructing how to handle personal data within the same legal person and across its branches. As commented in 5.5.2.6, this may be a problem when it comes to processing activities which include the disclosure of personal data outside the EEA.

6.4 Compatibility between EU Data Protection and Company Law

Without a doubt, group-structures present an extra challenge for EU Data Protection Law due to the necessity to identify the entity determining the purpose and essential means of a processing operation but also dealing with potential influence that may be exerted by other entities controlling it.

For subsidiaries, when holding companies exert their influence on the subsidiaries' operations and condition their determination, EU Data Protection Law can use the notion of 'piercing through the veil' to analyse factual circumstances, legitimised by public law

[204] Article 47 GDPR, although may not be so easily accessible for SMEs.

provisions, respect for fundamental rights and the benefit of the data subjects.[205] This is no different from other areas such as employment or consumer law, where the main focus is to protect the weaker party in the relationship.

By accepting branches as potential controllers, the GDPR imposes compliance obligations to entities which have no independent legal personality, despite their "whole personas" being capable of contracting obligations. Although this does not seem to be a problem within the EU, when branches of an EU-based company are located outside the safe area of the EEA and personal data is shared, this disclosure seems to be in a grey area where it may not fit as a "transfer" but still be associated with risks,[206] and thus require a special treatment similar to a subsidiary but without having the independent legal personality to celebrate agreements with its counterparts in the EU. Even when non-compliance by a non-EU branch might still be enforced to the legal person still partially in the EU for being the controller of the disclosure operation or given that the branch, as an establishment, might still be under the scope of the GDPR if it had received (thus processed) personal data involving subjects in the Union, the enforcement may be hindered for being outside the EU.

Although I would not refer to these regimes as incompatible, there still seems to be a lack of clarity when it comes to branches acting as data controllers (and even more when these are located outside the EEA), that might hinder a consistent and homogenous application throughout the EU and even discourage economic operators willing to expand beyond the EU without reasonable prospects on how to regulate internal relations within their entities.

6.5 Moving Forward

To provide legal certainty and transparency to groups of undertakings as economic operators, the first and most immediate step required should be addressing the situation of branches as potential independent data controllers. This would provide groups of undertakings clear expectations about the extent of the responsibilities that each of their entities is subject to, but also help data subjects to understand how and where their data is being processed.

Furthermore, clarifications in relation to compliance responsibilities for entities part of a group would also be welcomed by business operators, as to understand to which extent subsidiaries and branches need to implement data EU Data Protection principles and document operations about their practices when acting as controllers, and if these should correlate with practices performed by their principals even when the latter are not involved in the specific processing operations.

---

[205] See *Google Spain* (n 38).

[206] See 5.5.2.6. While recital (48) GDPR indicates that transfers to third countries in the context of groups of undertakings shall remain unaffected, it does not give instructions for data flows which are not actual "transfers".

Finally, in relation to EU-based groups of companies with branches outside the EEA, the existence of personal data “non-transfers” or disclosures to third countries within a same legal person certainly requires some regulation to help groups of undertakings navigate these complex scenarios and ensure that their data flows are aligned with the GDPR’s requirements. As a preliminary step, the inclusion of branches in intergroup agreements regulating data flows would ensure that potential disclosures to entities abroad receive the treatment required by EU Data Protection Law and respect the rights of the data subjects involved.

In the context of the internal market, clear and harmonised rules for groups of undertakings are fundamental to promote the GDPR’s goal of free personal data flows within the Union and maximise the objectives of the EU’s digital strategy.

7. List of References

7.1 Legal Sources

7.1.1 European Union

7.1.1.1 Treaties & Agreements

- The Treaty on European Union.
- Treaty on the Functioning of the European Union (Consolidated version 2016) OJ C 202/47.
- EU Charter of Fundamental Rights [2016] OJ C 202/02.

7.1.1.2 Regulations

- Regulation (EU) 2016/679 of the European Parliament and of the Council 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) [2016] OJ L 119/59.

7.1.1.3 Directives

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201/37.

7.1.1.4 Official Documents, Reports and Communications

- EC, '2030 Digital Compass: the European way for the Digital Decade' COM (2021) 118 final <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118> accessed 06 May 2022.

7.1.1.5 Guidelines and Recommendations

- WP29, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' WP128 adopted on 22 November 2006.
- WP29, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP169 adopted on 16 February 2010.
- WP29, 'Guidelines of identifying a controller or processor's lead supervisory authority' WP244 rev.01 adopted on 13 December 2016 as last revised and adopted on 5 April 2017.

- WP29, ‘Guidelines on transparency under Regulation 2016/679’ WP260 rev.01 adopted on 29 November 2017 as last revised and adopted on 11 April 2018.
- EDPB, ‘Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data’ Version 2.0 adopted on 18 June 2021.
- EDPB, ‘Guidelines 07/2020 on the concept of controller and processor in the GDPR’ Version 2.0 adopted on 07 July 2021.
- EDPB, ‘Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR’ adopted on 18 November 2021.

7.1.2 National Legislation

7.1.2.1 Germany

- Hesssisches Datenschultzgesetz [1970] GVBl I 625.

7.1.3 International Organisations

7.1.3.1 Conventions

- Council of Europe, CETS No. 108 [Convention 108] for the Protection of Individuals with regard to Automatic Processing of Personal Data <https://rm.coe.int/1680078b37> accessed 12 March 2022.

7.1.3.2 Guidelines and Recommendations

- OECD, ‘Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ [1980] www.oecd.org <https://perma.cc/9CRF-4NPW> accessed 12 March 2022.

7.2 Journals and Articles

- Paolo Balboni and others, ‘Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation’ (2014) Computer Law & Security Review 30 <https://www.sciencedirect.com/science/article/abs/pii/S0267364914000934> accessed 23 May 2022.
- Bhageshpur K., ‘Data is the New Oil - - And That’s a Good Thing’ (*Forbes’ Technology Council Blog*, 15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=160380007304> accessed 19 March 2022.

- Bing J., 'Data Protection, Jurisdiction and the choice of law' (1999) Privacy Law & Policy Reporter <http://www.austlii.edu.au/au/journals/PrivLawPRpr/1999/65.html> accessed 11 March 2022.
- Böckli P. and others, 'A proposal for reforming group law in the European Union – Comparative observations on the way forward' (*European Company Law Experts – ECLE Website*, October 2016) <https://europeancompanylawexperts.wordpress.com/publications/reforming-group-law-in-the-eu/#_ftn23> accessed 22 May 2022.
- CNIL, 'Record of processing activities' (*GDPR Toolkit*, 19 August 2019) <https://www.cnil.fr/en/record-processing-activities> accessed 24 April 2022.
- Dewey J., 'The Historic Background of Corporate Legal Personality' (1926) Yale Law Journal Vol. XXXV No. 6., pp. 655-673.
- Froud D., 'GDPR: It's not just about EU citizens, or residents' (*Froud on Fraud Blog*, 2018) <www.davidfroud.com/gdpr-not-just-eu-citizens-or-residents/> accessed 11 March 2022.
- Heine I., '3 Years Later: An Analysis of GDPR Enforcement' (*Center for Strategic & International Studies - CSIS Blog*, 13 September 2021) <https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement> accessed 17 March 2022.
- Kurtz C. and others, 'Accountability of platform providers for unlawful personal data processing in their ecosystems-A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR' (2022) Journal of Responsible Technology, Volume 9, April 2022, ScienceDirect - Elsevier <https://www.sciencedirect.com/science/article/pii/S2666659621000111> accessed 14 March 2022.
- Moerel L., 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? (2011) International Data Privacy Law, Issue 2011, Vol. 1, No. 1, Oxford University Press, pp. 28-46.
- Moerel L., 'Back to basics: when does EU data protection law apply?' (2011) International Data Privacy Law, Issue 2011, Vol. 1., No. 2, Oxford University Press, pp. 92-110.
- Peters B., 'The Age of Big Data' (*Forbes' Blog*, 12 July 2012) <https://www.forbes.com/sites/bradpeters/2012/07/12/the-age-of-big-data/?sh=7b6d85a44f66> accessed 19 March 2022.

- Sancho D., 'The concept of establishment and data protection law: rethinking establishment' (2017) European Law Review 2014 42(2), Sweet & Maxwell, p. 491-508.
- Sørensen K.E., 'Branches of Companies in the EU: Balancing the Eleventh Company Law Directive, National Company Law and the Right of Establishment' [2013] Nordic & European Company Law Working Paper No. 10-37 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2264091> accessed 27 March 2022
- Van Gestel R., Micklitz H.W. & Poiares Pessoa Maduro L.M., 'Methodology in the New Legal World' (2012) Working Paper, EUI LAW <https://cadmus.eui.eu/handle/1814/22016> accessed 8 March 2022.
- Viljoen S., 'A Relational Theory of Data Governance' (2021) Yale Law Journal, Vol. 131 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3727562> accessed 11 March 2022 (forthcoming).
- Zwenne G.J. and Erents C., 'De reikwijdte Wbp:enige opmerkingen over artikel 4, eerste lid, Wbp' (2009) Privacy & Informatie 2009/2, English translation available from Zwenne's Blog <https://zwenneblog.weblog.leidenuniv.nl/files/2009/10/GJZ-CER-ScopeofDDPATranslationOct09.pdf> accessed 18 April 2022.

7.3 Books

- Arnull A., *The European Union and its Court of Justice* (2nd edn, OUP 2006)
- Craig P. and de Burca G., *EU Law: Text, Cases, and Materials* (6th edn, OUP 2015).
- Ezrachi A., 'The Concept of Undertaking' in *EU Competition Law: An Analytical Guide to the Leading Cases* (Hart 2014) pp. 1-30.
- Lynskey O., *The Foundation of EU Data Protection Law* (OUP 2015).
- Perez Font J., 'Group of Companies and International Jurisdiction over Individual Contracts of Employment' in *Cuadernos de Derecho Transnacional* (Vol. 13 Issue 2, UC3M 2021), pp. 863-869.
- Streinz T., 'The Evolution of European Data Law' in Craig P. and de Búrca g. (eds) *The Evolution of EU Law* (3rd edn, OUP 2021), pp. 902-936 also available <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762971> accessed 11 March 2022.

7.4 Cases

7.4.1 Court of Justice of the European Union

- Case 33/78 *Somafer SA v Saar-Ferngas AG* [1978] EU:C:1978:205.

- Case 139/80 *Blanckaert & Willems PVBA v Luise Trost* [1981] EU:C:1981:70.
- Case 205/84 *Commission of the European Communities v Federal Republic of Germany (Insurance Services)* [1986] EU:C:1986:463.
- Case 81/87 *The Queen v H.M. Treasury and Commissioners of Inland Revenue, ex parte Daily Mail and General Trust plc.* [1988] EU:C1988:456.
- Case C-221/89 *The Queen v Secretary of State of Transport, ex parte Factortame Ltd and Others* [1991] EU:C:1991:320.
- Case C-55/94 *Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano* [1995] EU:C:1995:411.
- Case C-309/99 *J. C. J. Wouters and Others v Algemene Raad van de Nederlandse Orde van Advocaten* [2001] Opinion of AG Léger EU:C:2001:390.
- Case C-101/01 *Bodil Lindqvist* [2003] EU:C:2003:596.
- Case C-208/00 *Überseering BV v Nordic construction Company Baumanagement FmbH (NCC)* [2002] EU:C:2002:632.
- Case C-222/04 *Ministero dell'Economia e delle Finanze v. Cassa di Risparmio di Firenze SpA and Others* [2006] EU:C:2006:8.
- Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert v Land Hessen* [2010] EU:C:2010:662.
- Case C-378/10 *VALE Építési kft.* [2012] EU:C:2012:440.
- Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317.
- Case C-25/17 *Proceedings brought by Tietosoujavaltuutettu* [2018] EU:C:2018:57, Opinion of AG Mengozzi.
- Case C-210/16 *Wirtschaftsakademie* [2018] EU:C:2018:388.
- Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* [2020] EU:C:2020:559.
- Case C-645/19 *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit* [2021] EU:C:2021:483.

7.4.2 France

- Conseil d'Etat, Judgement of 19 June 2020, No. 430810 (*Société Google LLC*) <https://www.cnil.fr/sites/default/files/atoms/files/council-of-state-decision-google-2020-06-19_en_0.pdf> accessed 19 May 2022 (English translation).