11-2022

How General Data Protection Regulation Advances and Harmonizes the International Controller, Processor and Data Subject Contracts

Azam Zarechahoki

HOW GENRAL DATA PROTECTION REGULATION ADVANCES AND HARMONIZES THE INTERNATIONAL CONTROLLER, PROCESSOR AND DATA SUBJECT CONTRACTS

A dissertation submitted to Golden Gate University, School of Law in partial fulfilment of the requirement for the degree of Scientiae Juridicae Doctor – Doctor of Juridical Sciences (S.J.D)

Submitted to the Dissertation Committee Members:
Professor Dr. Christian Nwachukwu Okeke
Adjunct Professor Dr. Aileen Huang
Adjunct Professor Dr. Zakia Afrin

By

Azam Zarechahoki, Esq.

Golden Gate University
School of Law
Sompong Sucharitkul Center for Advanced International Legal Studies

November 2022

Copyright

By

Azam Zarechahoki

2022

Table of Contents

ACKNOWLEDGEMENT

I am grateful to *my committee members* for their invaluable advice and continuous support during my SJD study. Their immense knowledge and plentiful experience have encouraged me in all the time of my academic research and daily life. I would also like to express my gratitude to *my family and friends.* Without their tremendous understanding and encouragement over the past few years, it would be impossible for me to complete my study.

DEDICATION

This thesis is dedicated to all international students on F-1 visa in the United States who left their countries for the purpose of having a better life.

ABBREVIATIONS

BCRs: Binding Corporate Rules

CCPA: California Consumer Privacy Act

CJEU: Court of Justice of the European Union

CPRA: California Privacy Rights Act

CPPA: California Privacy Protection Agency

DPAS: Individual data protection authorities

DPC: Data Protection Commission

EC: European Commission

EDPB: European Data Protection Board

EDPS: European Data Protection Supervisor

EEA: European Economic Area

EU: European union

GDPR: General Data Protection Regulation

ICO: The Information Commissioner's Office

OAG: Office of the Attorney General

SA: Supervisory Authority

SCCs: Standard Contractual Clauses

CHAPTER 1: INTRODUCTION

1. The Background of the Adoption of GDPR in the European Union

In the technology and digital era, data is used daily by all businesses including insurance companies, banks, and social media sites. Many companies are involved in processing individuals' data and data could easily be transferred from one website to another which might be in another country. In fact, there are no borders in cyberspace. Generally, personal data refers to any information relating to individuals including name, address, and credit card numbers. In the cyber environment, it is challenging for people to take control of their personal information and avoid being tracked online. Data protection law is the safeguard to protect personal data and ensure that individuals are still in control of their personal data. Data protection law also benefits governments and entities from cyber-attacks and being hacked. In 2015, criminals attacked the US Office of Personnel Management and stole 21.5 million sensitive personal records of federal employees and their family members.[2] This kind of attack

[2] Kristin Finklea et al., Cyber Intrusion into U.S. Office of Personnel Management: In Brief, Congressional Research Service (2015), https://fas.org/sgp/crs/natsec/R44111.pdf.

on governments and entities is frequently happening in recent years around the world and it highlights the importance of taking actions by governments and entities to secure individuals' personal information.

Privacy right as an international human right is respected in many countries around the world.[3] Privacy rights or private life is preserved in several important documents including the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8), and the European Charter of Fundamental Rights (Article 7).[4]European Union ("EU") Treaties and Charter of Fundamental Rights have recognized privacy and data protection as two separate rights.[5] Article 8 of the EU Charter contains an explicit right to personal data protection.[6] Lisbon Treaty in 2009 gave the EU Charter the same legal value as the constitutional treaties of the EU.[7] Therefore, all EU institutions, bodies, and states have to comply with the EU Charter.[8] The EU Charter of Fundamental Rights gives individuals personal data protection right in all aspects of life including at home, at work, while shopping, when receiving

[3] European Data Protection Supervisor, Data Protection, https://edps.europa.eu/data-protection_en.
[4] *Id*.
[5] *Id*, at 5.
[6] *Id.*
[7] *Id.*
[8] *Id.*

medical treatment, at a police station, or on the Internet.[9] Although individual countries in the EU through the function of data protection regulations try to improve data protection rights, there was still a need to determine a uniform law that governs all EU countries and individuals.[10] In this context, it was necessary to create a more comprehensive legal environment to address globally data protection concerns, rather than just adopting regulations for individuals from specific EU countries.[11]

On November 4, 2010, the EU's Commission set out a strategy to strengthen EU data protection rules to protect individuals' data.[12] EU states that its data protection rules' objective is to protect the fundamental rights and freedoms of natural persons, especially data protection rights as well as data-free flow.[13] More than 90% of Europeans vote that they want the same data protection rights across the EU regardless of where their data is processed.[14]Therefore, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to protect

[9] EUROPEAN COMMISSION Press Release Database, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

[10] *Id.*

[11] *Id.*

[12] *Id*.

[13] *Id.*

[14] European Commission, Protection of personal data, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en#whattheecisdoingtoprotectyourrights.

online privacy rights and improve the EU's digital economy on May 25, 2012.[15] Accordingly, the EDPS adopted an opinion on the Commission's data protection reform package on July 03, 2012.[16] Finally, the European Parliament by voting in plenary with 621 votes in favor, 10 against, and 22 abstentions showed strong support for the General Data Protection Regulation ("GDPR") on March 03, 2014.[17] In April 2016, the EU adopted the GDPR as law across the EU and it came into force on May 25, 2018.[18]

Basically, there are two main reasons that the EU adopts GDPR to replace the 1995 European Data Protection Directive on the protection of individuals' personal data.[19]. First, based on a survey conducted by the EU, only 15% of people feel they have complete control over the information that they provide online.[20] Data protection right is a fundamental right in the EU and GDPR objective is to "protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal

[15] European Data Protection Supervisor, The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
[16] *Id*.
[17] *Id*.
[18] Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2016).
[19] European Data Protection Supervisor, The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
[20] European Commission, Data Protection, https://ec.europa.eu/justice/smedataprotect/index_en.htm.

data."[21] GDPR tends to improve trust in online services and cyber environment[22] and place Individuals in better control of their data through the function of specific rights.[23] GDPR would increase an individual's trust in online services and this would increase jobs and innovation in the European digital economy.[24] Second, GDPR is one set of rules that governs all 28 EU Countries.[25] Before GDPR, each EU country had its own rules and regulations and companies operating in different EU countries had to comply with different data protection laws.[26] There were unnecessary administrative requirements such as notifications for companies that are now removed by GDPR. Therefore, a single data protection law will reduce the cost of compliance for companies that are operating in different EU countries and would be more cost-effective.[27]

More than 120 countries around the world have passed data privacy regulations and many of these countries have articulated their law based on the privacy principles set up by GDPR. Considering the EU

[21] GDPR Article 1.
[22] EUROPEAN COMMISSION Press Release Database, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses (2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.
[23] *Id*, at 9.
[24] *Id.*
[25] Supra Note 2.
[26] *Id.*
[27]Supra Note 21.

harmonization of data protection law, GDPR not only created common data protection standards across its internal region but also among the multinational companies that apply GDPR data protection principles worldwide to avoid business costs, duplication of operational effort, and ensure their customers and employees feel trusted in permitting them to find access to their data.[28]

Although there has not been similar federal privacy legislation in the United States yet, some state-level laws have been enacted to bring GDPR-like protections. For example, the state-level data privacy laws in California are the California Consumer Privacy Act ("CCPA") and the California Privacy Rights Act ("CPRA"). The CCPA came into effect on January 1, 2020 and has been enforced since July 1st, 2020. The CPRA is a data privacy law that amended CCPA and will be in effect on January 1, 2023. The CPRA will be enforced by the California Privacy Protection Agency ("CPPA") and mandates all businesses to audit their data collection, storage, processing, and sharing mechanisms to ensure they comply with the law. Although GDPR, CCPA, and CPRA share the aim of giving individuals more control over their personal data, they take different approaches. There are some key

[28] Bhaskar Chakravorti, Why the Rest of the World can't Free Ride on Europe's GDPR Rules, Harvard Business Review (2018), https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules.

differences between GDPR and CCPA & CPRA in terms of scope, rights, and enforcement. This thesis aims to highlight these differences in the following relevant sections.

This thesis aims to examine two contact-based lawful processing between data controllers and data subjects. GDPR article 6 articulates different bases that make the processing of personal data lawful. Among which are data subject consent and the necessity of the processing for the performance of a contract. In cyberspace, controllers normally get their data subject's consent through user agreements. As such, sometimes it is challenging for the controllers to distinguish which type of lawful base for the processing they are involved in and which GDPR requirements they need to comply with. As such, this thesis examines and compares these two types of contracts to distinguish them in practice.

This thesis also analyzes GDPR protection on personal data which are accessible to the public. To better visualize the significance of the discussion, it examines the relevant US case, *hiQ Labs, Inc. v. LinkedIn Corp.*, which was decided in front of the U.S. District Court for the Northern District of California and the United States Court of Appeals for the Ninth Circuit. It particularly hypothesizes the case in front of the EU authorities

and discusses how the case decision would be different from the issued US decision. The importance of this discussion is to add GDPR data protection analysis to the US decision and recommend data protection policies to the field of data protection law in the US. This is increasingly important as adequate data protection regulations change access to the global economy, produce both new markets and increased competition, and harmonize data protection principles around the world. Furthermore, this thesis is to define and distinguish controllers, processors, and sub-processors responsibilities and liabilities towards each other and data subjects. The importance of this section is particularly in the case of GDPR non-compliance and awarding damages to data subjects. It also examines several real cases to determine the factors that GDPR authorities consider in deciding the amount of the administrative fine in case of data breaches and identifying relevant legal principles accepted by GDPR.

Finally, this thesis examines the situations that controllers or processors in the European Economic Area ("EEA") want to transfer the data to processors or sub-processors in non-EEA. More specifically, it identifies how multinational companies can transfer data from EEA to adequate and inadequate third countries such as the US and compares different methods based on multinational companies' size and activities that they are involved

in. Although there are some research articles and books about the GDPR, the contribution of this thesis to the field of data protection of the law is to identify and examine the specific above-mentioned topics in theory and practice and provide practical recommendations.

2. Scope of This Thesis and Chapter Overview

This thesis has undertaken in the following chapters to identify, organize and discuss part of international data protection law in the EEA on the subjects related to the contracts and responsibilities of controllers and processors towards data subjects. Chapter two discusses the required elements of valid consent articulated in GDPR article 4(11) through real cases to show the importance of each provision and how EU Supervisory Authorities ("SAs") are implementing GDPR and imposing fines in case of a data breach. Chapter two also examines and compares two different contract-based lawful bases to process data subjects' personal data. These are user agreements and the necessity of processing for the performance of a contract. Chapter two further analyzes the answer to the research question of whether GDPR protects personal data which are accessible to the public and examines two other relevant topics which are automated individual decision-making and profiling. To better visualize the significance of the

discussion, this thesis examines the relevant US case, *hiQ Labs, Inc. v. LinkedIn Corp.*, which was decided in front of the U.S. District Court for the Northern District of California and the United States Court of Appeals for the Ninth Circuit. It particularly hypothesizes the case in front of the EU authorities and discusses how the case decision would be different from the issued US decision.

The importance of chapter three is to define, distinguish and clarify controllers, joint controllers, processors, and sub-processors responsibilities and liabilities towards each other and data subjects. More specifically, chapter three examines several real cases to determine the factors that GDPR authorities consider in deciding the amount of the administrative fine in case of data breaches. This entails the nature, seriousness, and duration of the infringement, the negligent character of the infringement, the degree of responsibility that controllers take into account in terms of technical and organizational measures implemented to comply with the GDPR, the benefits gained from the infringement, the categories of personal data affected by the infringement, the relationship between the company's activity and the processing of personal data, the fact that the company is a large enterprise and its turnover, and the overall assessment of the case. Chapter three finally discusses relevant legal principles accepted by GDPR

regarding responsibilities and liabilities between controllers and processors in case of GDPR non-compliance and awarding damages to data subjects whose rights have been breached. These principles are particularly joint responsibility, contribution, indemnity, vicarious and contract-based liability.

Chapter four examines the situations that controllers or processors in the EEA want to transfer the data to processors or sub-processors in non-EEA. More specifically, chapter four discusses how multinational companies can transfer data from EEA to adequate and inadequate third countries and comply with GDPR chapter V requirements. Chapter four further compares different bases such as Binding Corporate Rules ("BCRs") and Standard Contractual Clauses ("SCCs") to consider what is the recommended way for multinational companies to transfer personal data considering the size and activities that they are involved with.

3. Key Definitions

This section defines key definitions based on article 4 of the GDPR.

3.1 Personal Data

Personal data is "any information relating to[29] an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[30] As such, GDPR by referring to natural persons does not intend to protect the processing of personal data of deceased persons or of legal entities.

Personal data definition is important because it determines if GDPR would apply to data actors' activity and consequently if they are subject to GDPR compliance requirements. According to the definition, the information should be related to an individual. For the purpose of being related to an individual, data actors should look at factors such as the content of the information, the purpose of processing, and the effect of the process on the

[29] UK Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), What is the meaning of 'relates to'?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/.
[30] GDPR Article 4(1).

data subject.[31] When different controllers process the same data for different purposes, the same information might be personal data for one process and not for the other one.[32] "This depends on the purpose the organization is processing the information for."[33] For example, when a newspaper journalist takes a photo of the beach including some individuals in order to show a hot day.[34] He is not processing the photo to extract anything about the individuals who are in the photo.[35] Therefore, the photo would not be personal data "as it is not used to record, learn or decide something about the individuals."[36] However, if one of the individual's colleagues scans the photo and emails it to the data subject's employer to file it in her personnel file, this would be processing personal data. Because "the photograph is being used to record, learn or decide something about the individual."[37] Thus, in order to decide whether a piece of data is personal data and relates

[31] UK Information Commissioner's Office, What is personal data? At a glance, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.
[32] *Id.*
[33] Information Commissioner's Office, What happens when different organisations process the same data for different purposes?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-happens-when-different-organisations-process-the-same-data-for-different-purposes/.
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*

to an individual, it is crucial to assess the purpose for which the controller is processing the data.[38]

Compared to the GDPR, the CCPA and CPRA define personal information instead of personal data. And personal information means information that identifies, relates to, and describes a particular consumer or household.[39] Information that is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to a particular consumer or household, is also personal information.[40] Personal information includes biometric information, geolocation data, audio, electronic, visual, thermal, olfactory, or similar information, professional or employment-related information, and education information, defined as information that is not publicly available.[41]

Given the above personal information definition, there are some differences between CCPA and CPRA in protecting personal information. CPRA protects the personal information of California employees, contractors, job applicants, and business contacts.[42] More specifically, businesses will be

[38] *Id.*
[39] CPRA 1798.140 (v)(1), Definitions.
[40] *Id.*
[41] *Id.*
[42] CPRA 1798.145(m)(4).

obligated to provide them with disclosures and rights available to California consumers.[43] While under CCPA, California employees, contractors, job applicants, and business contacts are exempted from personal information protection.[44]

Under CPRA and CCPA, household means "a group, however, identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services."[45] CCPA and CPRA define "Consumer" as a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations.[46] Whereas GDPR regulates all personal data related to living individuals in the EU. GDPR is not limited to residency or citizenship.[47] It is applicable to data processing of data subjects who are in the EU regardless of their citizenship or residency. As it is clarified in the GDPR recital 14, "the protection afforded by this Regulation should apply to natural persons,

[43] *Id.*
[44] *Id.*
[45] *CPRA 1798.140 (*q).
[46] CPRA 1798.140 (i).
[47] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1 (2019), page 14, edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

whatever their nationality or place of residence, in relation to the processing of their personal data."[48]

3.1.1 Special Categories of Personal Data

In general terms, GDPR prohibits the processing of special categories of personal data unless one of the indicated conditions in art 9(2) applies to that processing.[49] Special data are data concerning the racial and ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic data, and biometric data for the purpose of uniquely identifying a natural person, health, sex life, and sexual orientation.[50]

The CPRA also introduced a new category of protected data as sensitive personal information. This provision is fairly similar to the GDPR's Article 9 and gives consumers a right to ask a business's website to limit the use of their sensitive personal information if the business falls under CPRA regulations.[51]

[48] GDPR Recital 14.
[49] GDPR Article 9, Processing of special categories of personal data.
[50] *Id*.
[51] CPRA 1798.140(v)(1)(L); CPRA 1798.135.

3.1.2 Identifiable Natural Person

An identifiable natural person is defined as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[52]As such, entities are required to consider all the information that they are processing with all reasonable means to see if they can still identify the person even if they cannot directly identify the natural person.[53] For example, the name "John Smith" by itself may not be personal data as there are many natural persons with that name and it is not possible to say the name distinguished which of them.[54] However, if there are some other identifiers with that name such as an address, email, phone number, or workplace, then, this is normally enough to identify one person.[55]

Similarly, CPRA defines identifiers "such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol

[52] GDPR Article 4(1).
[53] *Supra* note 13.
[54] Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), What are identifiers and related factors?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/.
[55] *Id.*

address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers."[56]

3.1.3 Online Identifiers

Online identifiers such as internet protocol addresses and cookie identifiers are information provided by data subject's devices, applications, tools, and protocols.[57] MAC addresses, advertising IDs, pixel tags, account handles, and device fingerprints are other examples of online identifiers that the use of them "may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."[58]

To assess if a data subject is identifiable, controllers must consider whether all the identifiers on their own or in combination with other data can be used to distinguish one individual from another.[59] Identifiable data subject can be "either as a named individual or simply as a unique user of electronic

[56] CPRA 1798.140 (v)(1)(A).
[57] GDPR Recital 30.
[58] *Id*.
[59] *Id*.

communications and other internet services who may be distinguished from other users."[60]

3.1.4 Pseudonymization v. Anonymization

Pseudonymization_ As mentioned earlier, GDPR personal data is any information relating to an identified or identifiable natural person.[61] Pseudonymization and anonymization are two important concepts to realize if data is identifiable to any data subject. Pseudonymization is the way of processing data in which the data can no longer be related to a specific data subject unless using additional information.[62] Therefore, pseudonymization data is not identifying any specific data. However, using additional information with pseudonymization data can make the data subject identifiable. Moreover, the additional information is kept separately. Pseudonymization makes personal data less accessible, and it is one of the ways to comply with GDPR security measures.[63]

[60] *Id.*
[61] GDPR Article 4(1).
[62] GDPR Recital 26.
[63] Comlior, Pseudonymisation and Anonymization of Personal Data, https://complior.se/pseudonymization-and-anonymization-of-personal-data-what-is-the-difference/.

Anonymization_ There are no possibilities of identifying data subjects from anonymized data.[64] In fact, there is no way to restore original information and therefore, the data subject is not identified or identifiable even with additional information.[65] The principles of GDPR data protection do not apply to anonymous data and the processing of such data benefits statistical analysis or research purposes.[66] For example, directory replacement, scrambling, and masking are three different techniques that controllers can use to pseudonymize or anonymize personal data.[67]

In directory replacement, the controller removes the data that directly identifies the data subject such as the names. However, there is still a link between other values such as address and occupation. For example, the controller can use a number to identify a data subject and store the number separately.[68] In this method, the controller pseudonymizes the personal data. If the controller deletes the separate sensitive number as an identifier, then the personal data is anonymized and not subject to the GDPR.[69]

---

[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.* and Durham University, Anonymization and Pseudonymisation, https://www.dur.ac.uk/ig/dp/anonymisation/.
[68] *Id.*
[69] *Id.*

Because the rest of the stored data is not personal data, and an individual is not identified or identifiable.

Encryption and hashing are two different examples of scrambling.[70] Encryption is a mathematical process that uses a secret key value to encode data and users can read the encrypted information only with that key.[71] The controller or the processor still "have the ability to re-identify individuals through decryption of that encrypted dataset"[72]. Therefore, encryption is considered a pseudonymization method.[73] Hashing is a technique that scrambles plain text to create a unique message digest.[74] If properly designed, there is no way to reverse the hashing process to reveal the original text.[75] Hashing is a good way to store users' passwords instead of storing plain texts.[76] Hashed passwords cannot be decrypted if the controller or the processor does not use cryptographically secure hash password hashing.[77]

---

[70] *Id.*

[71] Information Commissioner's Office, What is encryption, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-is-encryption/.

[72] *Id.*

[73] *Id.*

[74] William Jackson, Why salted hash is as good for passwords as for breakfast (2013), https://gcn.com/cybersecurity/2013/12/why-salted-hash-is-as-good-for-passwords-as-for-breakfast/281485/.

[75] *Id.*

[76] *Id.*

[77] *Id.*

Similarly, CPRA defines "Pseudonymize" or "Pseudonymization" as the processing of personal information in a manner that the personal information no longer relates to a specific consumer without using additional information.[78] The additional information shall be kept separately and shall be subject to technical and organizational measures to make sure that the personal information is not related to an identified or identifiable consumer.[79] Moreover, under CPRA and CCPA, personal information "does not include consumer information that is deidentified or aggregate consumer information."[80] Aggregate consumer information is defined as information that is related to a group or category of consumers which is not linked or reasonably linkable to any consumer or household.[81] And it does not mean one or more individual consumer records that have been deidentified.[82]

3.2 Processing

GDPR Article 4 (2) defines processing as:

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by

[78] CPRA 1798.140 (aa).
[79] *Id.*
[80] CPRA 1798.140 (v)(3); CCPA 1798.140 (o)(3).
[81] CCPA 1798.140 (a) and (b).
[82] *Id*.

> automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

GDPR clearly indicated that processing covers a broad range of operations performed on personal data.[83] Staff management, payroll administration, access to the consultation of a contacts database containing personal data, sending promotional emails, shredding documents containing personal data, posting a photo of a person on a website, storing IP addresses or MAC addresses, video recording (CCTV) are all examples of data processing based on GDPR.[84]

Similarly, CPRA means processing as "any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means."[85] CPRA didn't define "operation", however, it defines "Collects," "collected," or "collection" as: "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means.

[83] European Commission, What constitutes data processing, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en.
[84] *Id.*
[85] CPRA 1798.140 (y).

This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."[86]

3.2.1 Commissioned Data Processing

GDPR defines commissioned data processing as "gathering, processing or use of personal data by a processor in accordance with the instructions of the controller based on a contract."[87]The controller must have a written data processing agreement with any third party that processes personal data on behalf of the controller. These processing services include cloud storage service, email marketing services, and website analytics software.[88] For example, a controller shares its clients' information through encrypted email and uses a third-party company to receive services.[89] The third-party company is a data processor, and the controller must have a written agreement with it.[90] Another example is using a data processor to analyze traffic on the controller's website.[91]

---

[86] CPRA 1798.140 (f).
[87] GDPR Key Issues, Processing; https://gdpr-info.eu/issues/processing/.
[88] Ben Woldford, GDPR.EU, What is a GDPR data processing agreement?, https://gdpr.eu/what-is-data-processing-agreement/.
[89] *Id.*
[90] *Id.*
[91] *Id.*

A commissioned data processing is a legally binding contract that describes the rights and obligations between the controller and the processor. Normally, there is a third-party beneficiary in such a contract who is a data subject whose personal data is processed under the contract. In subsequent sections, this research explains more about the provisions and the purpose of these contracts.

3.3 Controller

GDPR Article 4, Subsection 7 defines a controller as:

> 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

As it is clearly indicated in this article, it is the controller that determines the purposes and the means of processing personal data. Also, the processor has to process the data only based on the documented instructions from the controller. The processor will be considered as a

controller if violates GDPR by determining the purposes and means of processing.[92]

3.3.1 Joint Controller

There is a difference between processors and joint controllers. "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."[93] Joint controllers are jointly responsible for data processing and complying with the regulation.[94]

3.4 Processor

Processor defines as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[95] As aforementioned, a processor is "only allowed to process personal data based on the documented instructions from the controller."[96] The processor will be considered as a controller if violates GDPR by determining the purposes and means of processing.[97]

---

[92] GDPR Article 28 (10).
[93] GDPR Article 26 (1).
[94] *Id*.
[95] GDPR Article 4(8).
[96] GDPR Article 28(10).
[97] *Id*.

3.4.1 Sub-Processor

A sub-processor is a natural or legal person, public authority, agency, or other body which assists a processor in the processing of personal data for a controller.[98]

3.5 Cross-Border Processing

GDPR Article 4, Subsection 23 defines cross-border processing as:

> a. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

[98] Information Commissioner's Office, Contracts, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/.

CHAPTER 2: LEGAL ARRANGEMENTS BETWEEN CONTROLLERS AND DATA SUBJECTS TO PROCESS PERSONAL DATA

1. Introduction

One of the greatest achievements of the EU parliament in data protection law is GDPR. GDPR made many key changes to the EU's previous directive and its purpose is to protect personal data more efficiently.[1] GDPR regulates all personal data related to living individuals in the EU regardless of the type of data or the entity that controls or processes it. GDPR "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[2] Moreover, GDPR also "applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities" meet certain criteria provided in the GDPR article 3.[3]

[1] GDPR Key Changes, An overview of the main changes under GDPR and how they differ from the previous directive, https://eugdpr.org/the-regulation/.
[2] GDPR Article 3(1), European Data Protection Board has issued a guideline to more clarify GDPR territorial scope. For further exploration of this view, see also: https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en.
[3] GDPR Article 3(2).

Moreover, the CCPA only affects for-profit entities (businesses).[4] The CCPA describes a business as an entity that is organized or operated for the profit or financial benefit of its shareholders or other owners.[5] A business collects consumers' personal information, or on behalf of which such information is collected and alone, or jointly with others.[6] A business determines the purposes and means of processing consumers' personal information.[7] Also, a business does business in the State of California and satisfies one or more of the following criteria.[8] (A) *had* annual gross revenues of more than twenty-five million dollars ($25,000,000).[9] "(B) Alone or in combination, annually buys, sells, or shares the personal information of *100,000* or more consumers *or*, households. (C) Derives 50 percent or more of its annual revenues from selling *or sharing* consumers' personal information."[10]

The CCPA describes a business as an entity that buys, sells, or shares the personal information of 50,000 consumers or more consumer households. CPRA amended the criteria for what qualifies as a "Business". CPRA ups the CCPA threshold to 100,000. The CPRA also added the term, "sharing"

[4] CPRA 1798.145 (d)(1).
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] CPRA 1798.145 (d)(1)(A).
[10] CPRA 1798.145 (d)(1) (B) and (C).

to the CCPA's criteria of a business deriving 50% or more of its annual revenue from selling consumers' personal information. Therefore, as it is clear CA privacy law focuses on the relation between for-profit entities' revenues and the number of affected customers to determine if an entity is affected by the privacy laws. While GDPR focuses on the entities' data activities regardless of their amount of revenues, the number of affected consumers, the type of data, or the entity that controls or processes that data.

GDPR article 6 articulates different bases that make the processing of personal data lawful. Among which are data subject consent and the necessity of the processing for the performance of a contract. In cyberspace, controllers normally get their data subject's consent through user agreements. As such, sometimes it could be confusing for the controllers which type of lawful base for the processing they are involved in and which GDPR requirements they need to comply with. In addition to discussing real cases to show the importance of each provision and how EU SAs are implementing GDPR and imposing fines in case of a data breach, the significance of this chapter is to distinguish between these two types of contracts as two different bases for lawful processing and clarify the differences.

Moreover, chapter two analyzes the answer to the research question of whether GDPR protects personal data which are accessible to the public. To better visualize the significance of the discussion, this chapter further discusses a US data protection case, *HiQ Labs v. LinkedIn*, that has already been decided in the US courts and considers a *what-if situation* meaning what would be the court result if the case was in front of GDPR authorities. The purpose of this discussion is to increase data protection consistency in terms of protecting basic and commonly known rights for data subjects such as being informed of the data processing's purpose in data protection regulations across the world.

2. Contracts Between Controllers and Data Subjects

The controller shall have one of the lawful bases mentioned in Article 6 to process data subjects' personal data. Article 6(1)(a) is about the data subject's given consent "to the processing of his or her personal data for one or more specific purposes". Controllers routinely use user agreements as a means of receiving data subject's consent. User agreements are made between "the owner, administrator or provider of a web or mobile application-based service and the user of such a service, that defines the rights and responsibilities of both the parties. Privacy policies, website

terms, and conditions, etc. are all examples of a user agreement."[11] This section discusses the required elements of valid consent articulated in article 4(11). It also examines different typical types of user agreements, as contracts between a controller and data subject, to see if they fulfill GDPR requirements. Finally, this section considers article 6(1)(b) which explains the criteria of contracts that can be used as a lawful base to process data subjects' personal data. Article 6(1)(b) is divided into two main discussion areas. The first part is about "*processing is necessary for the performance of a contract to which the data subject is party*" and the second part is about processing is necessary "*in order to take steps at the request of the data subject prior to entering into a contract*." This section discusses both parts.

3. The Importance of Contracts

Having a contract between processors and controllers helps the parties to understand their responsibilities and liabilities. Contracts ensure legal certainty and avoid possible conflicts in the relation between the data actors and between the data subjects and the data protection authorities. Contracts provide certainty and help controllers and processors to prove their

[11] Upcounsel, How to write a User Agreement: Everything You Need to Know, https://www.upcounsel.com/how-to-write-a-user-agreement#:~:text=A%20user%20agreement%20is%20an,examples%20of%20a%20user%20agreement.

compliance with GDPR in transparency and accountability principles.[12] Moreover, according to the GDPR there should be a lawful base for processing data subject's personal data. So far, EU data protection authorities have decided on many infringement fees concerning the illegal processing of data subjects' personal data.

Coop Finnmark case_ For example, in Coop Finnmark case, the store manager with a mobile phone recorded a video from surveillance footage and shared the record which spread quickly.[13] The Norwegian data protection authority decided that "Coop Finnmark did not have a legal basis for the store manager's sharing of the footage from the monitoring."[14]

4. GDPR Consent Elements

Based on GDPR Article 4 (11), data subject consent means:

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

---

[12] Information Commissioner's Office, When is a contract needed and why is it important, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/.

[13] Datatilsynet, Decision on infringement fee to Coop Finnmark, https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/vedtak-om-overtredelsesgebyr-til-coop-finnmark/; https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-issues-fine-coop-finnmark_en.

[14] *Id*.

This section by using real relevant cases, decided by the EU authorities, discusses the required elements of a data subject's valid consent. It explains to what extent the wording of GDPR requires controllers to take appropriate steps and ensure GDPR compliance with regard to data subjects' consent. This section also discusses article 7 and recital 32 which further clarifies consent elements mentioned in article 4(11).

4.1.Data Subject's Consent Should Be Freely Given

The element of freely given in the consent definition indicates the importance of real choice and control for data subjects. The GDPR signifies that the consent is not valid if "the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent".[15] Accordingly, consent as a non-negotiable part of terms and conditions is presumed not to be freely given.[16] If the data subject is unable to refuse or withdraw his consent without negative effects, consent will not be considered to be freely given.[17] The GDPR also takes into consideration the specific situations of taking consent. For example, in the contract

[15] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 (2020), page 7, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
[16] *Id*.
[17] *Id*.

context, the performance of a contract including service provisions that are conditional on data processing consent while that processing is not necessary for the performance of the contract.[18] Such consent is not freely given and consequently not valid.

Imbalance of power _Public authorities and employers are two examples of the controllers that their actions of processing personal data based on data subject's consent result in an imbalance of power.

Public authorities_ The GDPR has taken into account the concept of imbalance of power between the controller and the data subject. "Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g., substantial extra costs) if he/she does not consent."[19] There is often a clear imbalance of power when public authorities rely on data subject's consent for processing of personal data. In most of the cases, the data subject has no realistic alternative. "Consent will not be free in

[18] GDPR Article 7(4).

[19] European Commission, Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (2017), page 9, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

cases where there is any element of compulsion, pressure or inability to exercise free will."[20]

In the Baby and Mother Homes Commission case, the Commission of investigation deleted recording of witness testimony as a part of 5-year investigation related to a mother and baby homes case.[21] The commission argues that survivors as data subjects "orally asked for permission to record and told the recordings would be destroyed."[22] However, the survivors answered that they were not informed that their testimonies would be deleted.[23] Consequently, the Irish DPC decided that data subject's consent for data processing must be freely given and there should be balance between the data subject and the controller.[24] DPC added when the controller is a public authority or employer the imbalance could also happen.[25]

Similarly, GDPR Recital 43 indicates that when the controller is a public authority, "there is a clear imbalance between the data subject and the

[20] *Id*.
[21] Elaine Loughlin, Irish Examiner, Data Protection commission seeks answers on destruction of mother and baby homes recordings (2021), https://www.irishexaminer.com/news/arid-40218473.html.
[22] *Id.*
[23] *Id*.
[24] *Id.*
[25] *Id*.

controller"[26] and therefore "it is unlikely that consent was freely given"[27] Thus, using data subjects' consent as a lawful base is generally not valid and public authorities shall consider another base among the choices indicated in the GDPR article 6 to processing personal data.

Employer and employee relationship_ An imbalance of power also happens in the employment relationship. Considering the dependency between employer and employee, it is unlikely that the employee is able to deny his consent to data processing without fear of negative effects due to refusal.[28] "Therefore, the EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees … this does not mean that employers can never rely on consent as a lawful basis"[29]. However, employees can only rely on freely given consent in exceptional circumstances, when the employee's denial will have no adverse consequences at all.[30] In general terms, "any element of inappropriate pressure or influence upon the data subject … which

[26] GDPR Recital 43.
[27] *Id*.
[28] *Supra* note 15, at 9.
[29] *Id*.
[30] *Id*.

prevents a data subject from exercising their free will, shall render the consent invalid."[31]

In the Provincial Healthcare Company of Enna case, the company had a biometric identity verification system that processed the biometric data of employees in order to ensure employee attendance in the company.[32] The data registration procedure involves the employee' detection of the biometric fingerprint, which is transformed into an encrypted string, stored on a secure device (badge).[33] In this case, the Italian data protection authority (GPDP) founds that processing biometric data of employees for the purpose of detecting attendance is in violation of the principle of lawfulness, fairness, and correctness, Article 5(1)(a). GPDP further considers that "in the absence of a suitable prerequisite of lawfulness", the controller's processing of biometrics data is in violation of Article 6(1)(c) and 9(2)(b) of the GDPR.[34] The authority indicates that the employer may process the special category of personal data of an employee if the processing is based on the conditions indicated in article 9(2)(b) of the

[31] *Id*.
[32] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (GPDP), Injunction order against the Enna Provincial Health Authority (2021), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542071.
[33] *Id*.
[34] *Id*.

Regulation.[35] However, the lawful basis cannot be based on the employee's consent due to the nature of the relationship between employer and employee and the existence of the imbalance between powers[36] The DPA also ordered the controller to delete its employee fingerprint data.[37]

4.2.Data Subject's Consent Should Be Specific

In addition to article 4(11), Article 6(1)(a) also indicates that the data subject's consent for the purpose of data processing should be for one or more specific purposes.[38] In fact, his requirement wants to make sure a degree of transparency and control for the data subject.[39] Furthermore, if the written agreement is also about other matters, the consent request regarding data processing shall be "clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."[40]

---

[35] *Id*.
[36] *Id*.
[37] *Id*.
[38] GDPR Article 6(1)(a).
[39] *Supra* note 15, at 11.
[40] GDPR Article 7(2).

In the Family service case, Belgian DPA fines 50,000 Euro Family Service company for breaching the GDPR.[41] "Family Service is a marketing company that distributes pink boxes that include samples, special offers, and information sheets for future parents."[42] Belgian DPA found that the company was renting and/or selling personal data for commercial purposes and did not get the informed and specific consent of the customers.[43] The core business of the third-party companies which receive customer's personal data is trading data, however, customers believed that the boxes were distributed from public sectors.[44]

CAIXABANK also got a total fine of 6.000.000 EUR due to unlawfully processing client's personal data and not sufficiently informing its clients about the processing of personal data.[45] The Spanish Data Protection Authority (AEPD) found that CAIXABANK as a controller did not provide enough information to the data subject regarding the specific purposes of personal data processing, the categories of personal data involved, and the

[41] European Data Protection Board, Belgian DPA imposes €50,000 Fine on Family Service, https://edpb.europa.eu/news/national-news/2021/belgian-dpa-imposes-eu50000-fine-family-service_en.
[42] *Id*.
[43] *Id.*
[44] *Id*.
[45] Europe Data Protection Board, Spanish Data Protection Authority (AEPD) imposes fine of 6.000.000 EUR on CAIXABANK, S.A. (2021), https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank-sa_en.

legal basis for the processing.[46] AEPD also found that the company does not have the legal basis for processing, especially the processing based on the company's legitimate interest.[47]AEPD decided that CAIXABANK had infringed GDPR Articles 13 and 14.[48]

Articles 13 and 14 are about the information that the controller shall provide to the data subject where personal data are or are not obtained from the data subjects.[49] "the categories of personal data concerned" and "the purposes of processing for which the personal data are intended as well as the legal basis for the processing" are part of the required information that the controller shall provide to the data subject.[50] However, AEPD decided that CAIXABANK did not do its obligations.[51] Moreover, the AEPD concluded that CAIXABANK did not collect the data subject's consent that fulfills all the elements of valid consent.[52] The AEPD further established that the processing activities based on the company's legitimate interest were

[46] *Id*.
[47] *Id*.
[48] *Id*.
[49] GDPR Article 13 and 14.
[50] *Id*.
[51] *Supra* note 45.
[52] *Id*.

not sufficiently justified, therefore, CAIXABANK's data processing formed a breach of GDPR Article 6.[53]

4.3.Data Subject's Consent Should Be Informed

Data subject's consent shall be informed prior to giving such consent. Moreover, withdrawing consent at any time shall be as easy as giving such consent.[54] Informed consent essentially means that the controller shall provide information to data subjects prior to obtaining their consent.[55] In other words, an informed decision would lead to informed consent. Data subjects should understand what they are agreeing to and knows about their right to withdraw their consent.[56] Article 29 Working Party (WP29) has also provided certain elements that are crucial to making an informed decision. Therefore, the controller must provide at least the following information to get a data subject's informed consent:

1. the controller's identity including joint controllers
2. the purpose of each of the processing operations for which consent is sought

[53] *Id*.
[54] GDPR Article 7(3).
[55] *Supra* note 15, at 13.
[56] *Id*.

3. what (type of) data will be collected and used by the controllers and joint controllers
4. the existence of the right to withdraw consent
5. information about the use of the data for automated decision-making in

   accordance with Article 22 (2)(c)34 where relevant, and

6. on the possible risks of data transfers due to the absence of an adequacy decision and of appropriate safeguards as described in Article 46.[57]

WP29 concludes that the controller may require to provide more information to the data subject depends on the context of each case.[58]

Clubhouse case_ Clubhouse is a social networking app that has audio chats and users can register and sign up only through invitation. The app is launched and operated by the controller, Alpha Exploration, a CA-based company, however, users are not informed about the identity of the controller. The app faces data protection breaches and tackling with court

[57] *Id*.
[58] *Id*.

action in Germany.[59] According to Article 29 Working Party, the controller must provide its identity to get the data subject's informed consent. Similarly, the Executive Director of the Federation of German Consumer Organisations (vzbv) indicates that: it is essential for German users to be informed about the Clubhouse service provider, based on section 5 of the German Telemedia Act.

In addition, Clubhouse's terms of service are only in the English language while the app got widespread among German users. Thus, vzbv found that the terms of service are not transparent and understandable for German users and their data processing consents are not informed.[60] Similarly, in 2016, vzbv ruled against **WhatsApp** that makes its terms of service available only in English for German users. vzbv indicates that WhatsApp is acting "in a non-transparent manner that disadvantages all consumers in a breach of good faith".[61] Finally, the app's users have to upload their address book in order to find access to clubhouse services while the German Federal Supreme court in **Facebook's Friend Finder tool** in 2016, already prevented

[59] Peter Hence, JDSUPRA, Clubhouse app faces court action in Germany over serious failing under data protection and consumer law (2021), https://www.jdsupra.com/legalnews/clubhouse-app-faces-court-action-in-6123803/.
[60] *Id*.
[61] *Id*.

social media platforms to ask users to upload their address books.[62] As a result of violations, Germany's consumer protection organization orders Alpha Exploration Co to stop its illegal business practice and data protection violations.[63] Not complying with data protection regulations, the company will face sanctions and fines from the data protection authorities under the GDPR as well as lawsuits from data subjects.

Grindr case_ Grindr is a globally famous gay dating app which illegally shared its users' personal data including locations and tracking codes with advertising companies such as MoPub and Twitter's mobile advertising platform.[64] Grindr has tagged its users' personal data to the advertising companies as L.G.B.T.Q[65] without getting its users' informed consent.[66] The Norwegian Data Protection Authority fined Grindr about $11.7 million.[67] According to Tobias Judin, head of the Norwegian Data Protection Authority's international department, "Grindr's data-mining practices not only violated European privacy rights but also could have put users at

[62] *Id*.
[63] *Id*.
[64] Natasha Singer and Aaron Krolik, The New York Times (2021), https://www.nytimes.com/2021/01/25/business/grindr-gdpr-privacy-fine.html; More information at: https://www.datatilsynet.no/en/news/2021/intention-to-issue--10-million-fine-to-grindr-llc2/; and https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-intention-issue-eu-10-million-fine-grindr-llc_en.
[65] The Center, LGBTQ is an acronym for lesbian, gay, bisexual, transgender and queer or questioning. https://gaycenter.org/about/lgbtq/.
[66] *Id*.
[67] *Id*.

serious risk in countries, like Qatar and Pakistan, where consensual same-sex sexual acts are illegal."[68]

According to Article 29 Working Party, controllers shall provide information in clear and plain language which is easily understandable by the average person. A data subject should easily identify who the controller is and what they are agreeing to.[69] "The controller must clearly describe the purpose of data processing for which consent is requested."[70] If data processing's consent is requested within a contract which also includes many other subjects that are unrelated to the requested consent, the issue of consent shall be distinguishable from other matters and clearly stands out.[71] It is better that the issue of consent for the use of data subject personal data be in a separate document. Consent cannot be a simple paragraph within other terms of service.[72]

Transparent Algorithm_ the company in this case processed the personal data of its members to improve their reputational profiles and credentials within a professional dynamic. The offered personal data processing was

[68] *Id*.
[69] *Supra* note 15, at 14.
[70] *Id*.
[71] *Id*.
[72] *Id*.

instrumental to the member's profiles and the processing was based on an algorithm that its functioning was not explained for data subjects. In this case, the Italian court of Cassazione ruled that there is no consent without transparency. When data processing actors ask for data subjects' consent to conduct an algorithmic process, the data subject should be adequately informed about the logic behind the algorithm. Otherwise, the consent is not transparent and informed. More specifically, the membership of a platform does not include the acceptance of an automated system which uses an algorithm to evaluate the profiles and give automated rates to the data subject's profiles. Therefore, if a data controller wants to get YES to algorithmic processing of personal data without explaining the logic of the process to the data subject.[73]

[73] Guido Scorza, Privacy Guarantor Authority, The algorithm must be transparent (2021), https://www.agendadigitale.eu/sicurezza/privacy/lalgoritmo-deve-essere-trasparente-la-cassazione-rilancia-il-gdpr/.

4.4.Data Subject's Consent Should be Unambiguous Indication of Consent

The indication of consent must be obvious. GDPR clearly indicates that the consent must be based on a clear affirmative act or a statement for the data subject.[74]Consent must be given through an active action or declaration.[75]

4.5.Consent Can Be Indicated by an Oral or Written Statement

Consent can be through written or (a recorded) oral statement.[76] Sending a written letter or emailing a typed message to the controller by the data subjects are some ways to show consent.[77] However, these consent formats do not often happen in reality.[78]

4.6.Definition of Consent by a Clear Affirmative Action

"A clear affirmative action means that the data subject must have taken a deliberate action to consent to the particular processing."[79] Therefore, controllers cannot use a pre-ticked opt-in box on their websites or mobile

[74] GDPR Article 4 (11) and Recital 32.
[75] *Supra* note 15, at 15.
[76] GDPR Recital 32.
[77] *Supra* note 15, at 16.
[78] *Id*.
[79] *Id*.

apps to comply with GDPR consent requirements.[80] Similarly, data subject silence, inactivity, or merely exploring and using controllers' services cannot be interpreted as an active indication of consent. [81] Furthermore, Opt-out formats that require the data subject to take action and prevent the agreement are not acceptable ways to get data subject consent under GDPR. [82] To fulfill the requirement for informed consent, the GDPR does not provide any specific form or shape in which the information must be. The informed consent may be in different ways including written or oral statement, audio, or video message.[83] However, the consent must fulfill the GDPR required requirements including article 4(11), article 7 and Recital 32.

4.7.GDPR Age Requirement for Digital Consent Is At Least 16 Years Old

The age of users that use controller's services are also important. If the targeted users are minors, the controller must take a further step and make the information understandable for them.[84] According to the GDPR article 8(1), controllers can directly offer information society services to at least 16

[80] *Id*.
[81] *Id*.
[82] *Id*.
[83] *Supra* note 15, at 13-14.
[84] *Id* at 14.

years old child.[85] Otherwise, data processing "shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child."[86] Moreover, "Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."[87]

So far, EU regulators have not provided definitive guidance on how the controllers verify parental consent. Therefore, companies are implementing different strategies to fulfill the GDPR requirement. For example, Microsoft is applying the verification standards offered under the U.S. Children's Online Privacy Protection Act (COPPA) to verify parental consent for children's accounts across their product platforms.[88] Under this, parents shall use a credit card or a debit card with a card verification value (cvv). Then, they will get a 50 cents charge which will be credited to an existing Microsoft account.[89] The purpose of the nominal charge is to inform parents when they receive notification from their respective card accounts or when

[85] GDPR Article 8 (1).
[86] *Id*.
[87] *Id*.
[88] Julie Brill, Microsoft begins new EU GDPR parental consent verifications for children's accounts (2018), https://blogs.microsoft.com/on-the-issues/2018/04/11/microsoft-begins-new-eu-gdpr-parental-consent-verifications-for-childrens-accounts/.
[89] *Id*.

reviewing their statements.[90] Microsoft has also given parents an option to call Microsoft for not going through the mentioned process.[91]

TikTok case_ TikTok is one of the recent cases that received the Irish Data Protection Commission ("DPC") notification due to not complying with the GDPR consent requirements. TikTok, known in China as Douyin, is a video-sharing social networking service. Users use TikTok to make a variety of short-form videos on subjects such as dance, comedy, and education. TikTok is also popular for its challenges offered by users on their personal accounts. Recently, a 10-year-old girl in Palermo, Italy participated in a blackout challenge on TikTok and died from suffocation.[92] TikTok policies require users to be at least13 years old to set up an account. However, there is no active monitoring on the app. TikTok platform is legally established in Dublin, Ireland, and therefore, the Irish Data Protection Commission (DPC) is the lead authority to decide about the TikTok case. As Irish Data Protection Act 2018 has set 18 years old as the

[90] *Id*.

[91] *Id*.

[92] Vincent Manancourt, Italy orders TikTok to stop using children's data (2021), https://www.politico.eu/article/italy-orders-tiktok-to-stop-using-childrens-data/; European Data Protection Board, Italian DPA imposes limitation on processing on TikTok after the death of a Girl from Palermo (2021), https://edpb.europa.eu/news/national-news/2021/italian-dpa-imposes-limitation-processing-tiktok-after-death-girl-palermo_en.

age of digital consent for the users, therefore, the age 16 will be considered as the age of consent in the TikTok case.[93]

After the TikTok case, inquiries started about Facebook and Instagram.[94] Italian data protection authority (The Garante) has questioned **Facebook which owns Instagram** to provide information about its policy that how children can register and manage accounts on their social media platforms.[95] As GDPR requires the controllers to make reasonable efforts to verify the children's age, the decision on TikTok and Facebook case will help controllers to understand what constitutes a reasonable effort to verify such consent.[96]

4.8.CCPA and CPRA Consent Elements

Similar to the GDPR, CPRA means "Consent" as any freely given, specific, informed, and unambiguous indication (by a statement or by a clear affirmative action) of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person

[93] Electronic Irish Statute Book (eISB), Data Protection Act 2018, Article 29, Child for purpose of application of Data Protection Regulation (2018), http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html.
[94]The Garante, Tik Tok will adapt the requests of the privacy Guarantor (2021), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533424#en.
[95] *Id*.
[96] *Id*.

acting as a conservator for the consumer, signifies an agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Moreover, "acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent."[97]

5. User Agreements as a Means of Receiving Data Subject's Consent

As mentioned before, a controller shall have one of the lawful bases indicated in article 6 to process data subject's personal data. Article 6, part 1(a) is about data subject's given consent "to the processing of his or her personal data for one or more specific purposes". The previous section examines Article 4(11), article 7 and relevant cases which examined the elements of a valid consent. This section will further discuss the required elements of a valid consent within the context of the user agreements. Web or app controllers routinely use user agreements as a means of receiving data subject consent. User agreements are between "the owner,

[97] CPRA and CCPA 1798.140.h.

administrator or provider of a web or mobile application-based service and the user of such a service, that defines the rights and responsibilities of both the parties. Privacy policies, website terms and conditions, etc. are all examples of a user agreement."[98]Browserwrap and Clickwrap are two examples of agreements that controllers apply to get their data subject's consent on the relevant websites or applications.[99]

5.1.Browserwrap Agreements as a Means of Receiving Data Subject's Consent

These are noticed type agreements which basically inform the users about the terms that they are subject to.[100] Websites by using the words such as "by continuing to use this website you agree to the terms of use of this website", inform the data subject that consented to the user agreement by using the website.[101] The controller sometimes provides a hyperlink for the user to direct him to the agreement content, however, actually reading or accepting the agreement terms is not a precondition to using the controller's

[98] Upcounsel, How to write a User Agreement: Everything You Need to Know (2020), https://www.upcounsel.com/how-to-write-a-user-agreement#:~:text=A%20user%20agreement%20is%20an,examples%20of%20a%20user%20agreement.
[99] *Id*.
[100] *Id*.
[101] *Id*.

services.[102] Controllers assume their user's consent by signing up action itself.[103] A good example of these agreements is terms of service contracts. Under GDPR, data subjects' consent should be informed prior to giving the consent and it has to be specific to one or more purposes to be valid. Moreover, GDPR recital 32 indicates that "If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."[104] Therefore, Browserwrap agreements are not appropriate types of agreements to get data subjects' consent for processing pertaining data.

Similarly, US Courts are against such contracts and did not find them enforceable unless "the website owner presents evidence that the user had actual or constructive knowledge of the terms."[105] For instance, ***in the case, Nguyen v. Barnes & Noble Inc.,*** the United States court of appeals for the ninth circuit found that "Were there any evidence in the record that Nguyen had actual notice of the Terms of Use or was required to affirmatively

---

[102] *Id*.

[103] *Id*.

[104] GDPR Recital 32.

[105] THOMSON REUTERS, PRACTICAL LAW, Glossory, Borwsewrap Agreement, https://1.next.westlaw.com/Document/I2e45ae49642211e38578f7ccc38dcbee/View/FullText.html?transitionType=Default&contextData=(sc.Default)&firstPage=true&OWSessionId=40fabf6a8d0b4d6bb49690525c5ee092&isplcus=true&fromAnonymous=true&bhcp=1.

acknowledge the Terms of Use before completing his online purchase, the outcome of this case might be different."[106] In another case, the court of appeal of Florida, fourth district, decided that "Browsewrap agreements have only been enforced when the purchaser has actual knowledge of the terms and conditions, or when the hyperlink to the terms and conditions is conspicuous enough to put a reasonably prudent person on inquiry notice."[107] It is important to notice that courts believe that new internet agreements have not changed the principles of contracts. One of these principles is the mutual manifestation of assent between the parties. The manifestation could be through written or spoken word or by conduct. However, controllers cannot such assent by only posting user agreements on their websites.[108]

5.2.Clickwrap Agreements as a Means of Receiving Data Subject's Consent

Clickwrap agreements are also known "as a clickthrough agreement and clickwrap license."[109] In Clickwrap agreements, users have to "take certain

[106] Nguyen v. Barnes & Noble Inc. (9th Cir. 2014) 763 F.3d 1171.
[107] Vitacost.com, Inc. v. Mccants (Fla.Dist.Ct.App. 2017) 210 So.3d 761.
[108] *Id*.
[109] *Supra* note 98.

affirmative action as an acknowledgement of their consent."[110] Controllers to create personal accounts for their users on their websites or applications have a sign-up process. During the process, they usually ask their users to click the checkbox at the bottom of the account registration form. Users to sing up must check "I agree" or "I accept" box to show their consent to the controller's Terms & Conditions and Privacy Policy. Users by checking the box agree that the controller processes their personal data instead of getting access to the website services.

In fact, in some cases, controllers use account registration in both mentioned agreements as an opportunity to receive the data subject's consent for processing personal data.[111]Data subjects' consent is the precondition to use the controller's services in clickwrap agreements and data subjects use clear affirmative action in showing their consent to the controller. However, "A browsewrap agreement occurs when a website merely provides a link to the terms and conditions and does not require the purchaser to click an acknowledgment during the checkout process. The purchaser can complete

[110] *Supra* note 98.

[111] Examples of "I Agree to Privacy Policy Checkboxes, FreePrivacyPolicy (2021), https://www.freeprivacypolicy.com/blog/agree-privacy-policy-checkboxes/.

the transaction without visiting the page containing the terms and conditions."[112]

To examine clickwrap agreements under GDPR, the question is how much the data subject's consent to process its personal data is informed, specific and distinguishable from the other matters in the agreement. For the purpose of data processing, controllers have to provide information in clear and plain language which is easily understandable for the average person to easily identify who the controller is and what they agree to.[113] "The controller must clearly describe the purpose of data processing for which consent is requested."[114] Therefore, controllers cannot use long privacy policies that are difficult to understand and hidden in general terms and conditions.[115] Dara processing' consent must be distinguishable from other matters in easily accessible forms.[116] To make a user agreement more specific and distinguishable, controllers can use different sections in their user agreements including privacy policy and returns & refunds. How, the problem with a single agreement is that they are lengthy. Consequently,

[112] *Supra* note 105.
[113] *Supra* note 15, at 14.
[114] *Id*.
[115] *Id*.
[116] *Id*.

having different agreements pertaining to different subjects would be better to get data subject's informed and specific consent.

Taking LinkedIn as an example, the company has different types of user agreements on its website which are named them in different tabs as user agreement, privacy policy, cookie policy, copyright policy and California privacy disclosure.[117] According to LinkedIn user agreement, user is agreeing to enter into a legally binding contract with LinkedIn by clicking "Join Now" or "Sign Up" tab. User is also subject to all terms of LinkedIn cookie and privacy policy by using the company services. However, users have choices about the data that LinkedIn collect, use, and share by changing the preferences in setting section of the app or website. The question is if LinkedIn users give informed consent to process their data before getting into binding contracts with LinkedIn. Also, whether LinkedIn users' consent are specific and distinguishable.

The US courts analyzed clickwrap agreements as forming a contract under UCC section 2-204 or an amendment, adding terms to an existing contract under UCC section 2-207.[118] Pursuant to UCC section 2-204, the data subject

[117] LinkedIn, User Agreement (2021), https://www.linkedin.com/legal/user-agreement.
[118] I. Lan Sys. v. Netscout Serv. Level Corp. (D.Mass. 2002) 183 F.Supp.2d 328.

manifested his assent to the agreement and make the agreement enforceable when he clicked on the box "I agree".[119] However, the analysis under UCC section 2-207 is different. Between merchants, UCC deems the data subject to have accepted the additional terms implicitly if the data subject never objects to the additional terms, and the additional terms are not material.[120] The comment to UCC section 2-207 indicates that "the test for materiality is whether the terms in question would result in unreasonable surprise or hardship to the party if incorporated without the party's express awareness." [121]Finally, if the additional terms are not accepted either explicitly or implicitly, but the conduct of the parties shows recognition of a contract, then the contract is accepted with initial default terms.[122]

5.3.Consent Banners Agreements as a Means of Receiving Data Subject's Consent

In this method, controllers permit users to sign up/in and use the services, however, "consent banners continue to appear at the top, bottom, or side of the users' screen asking them to click the checkbox or click the button in

[119] *Id*.
[120] *Id*.
[121] *Id*.
[122] *Id*.

order to consent to the terms of use."[123] One of the most popular consent banners is the cookie consent banner. Cookies are small text files that are processed and stored by a user's browser.[124] In spite of being functional for using websites, cookies also store a huge amount of data which is enough to potentially identify the data subject.[125]

A computer cookie or more formally HTTP is a packet of data and information.[126] When a user visits a website, his computer will store cookies in a file located in his web browser.[127] The purpose of the cookie is to keep a track of users' web activities.[128] Website controllers use cookie banners to obtain user's consents for processing their personal data.[129]

Considering the amount of data that cookies store, controllers have to receive data subject's consent in certain circumstances.[130] Some service providers deny their users' access to their service due to not consenting to all cookies and trackers on the website. This "take it or leave it" action is

[123] *Supra* note 105.
[124] GDPR.EU, Cookies, the GDPR, and the ePrivacy Directive, https://gdpr.eu/cookies/.
[125] *Id*.
[126] Norton, what are cookies (2019), https://us.norton.com/internetsecurity-privacy-what-are-cookies.html.
[127] *Id*.
[128] *Id*.
[129] The end of dark patterns in "cookie walls": German court bans deceptive designs, Peter Hence, January 21, 2021, https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/.
[130] *Id*.

called cookies wall and is not acceptable under GDPR.[131] A valid consent has to be freely given and the use of the services must not be conditional on consent. The EDPB in its consent guideline indicates that a service provider cannot use cookie walls to receive data subjects' consent.[132]

5.4.The Controller Has the Burden of Proof for a Valid Consent

Under GDPR Recital 42, "Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation."[133] This is especially important when the controller sends a written declaration on another matter to the data subject.[134] In this context, the controller shall be able to prove that the data subject has been aware of the fact and to what extent the consent is given meaning the consent shall be informed and specific.[135] If a declaration of consent is pre-formulated by the controller, the declaration

[131] Cookiebot, Cookie walls |EDBP guidelines on cookie walls and valid consent, https://www.cookiebot.com/en/cookie-walls/#:~:text=A%20cookie%20wall%20is%20a,trackers%20present%20on%20that%20website.
[132] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 (2020), page 11, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
[133] GDPR Recital 42.
[134] *Id*.
[135] *Id*.

shall be "in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms."[136]

6. Contracts Between Controllers and Data Subjects as a Lawful Base for Processing Personal Data

According to the GDPR, any processing of personal data shall be lawful. GDPR article 6 defines six lawful bases for processing data and, there should be at least one of the bases to legally process personal data. One of these bases indicated in article 6, part b is when "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;"[137]

The EDBP recognizes that processing is not "necessary for the performance of a contract" when providing the contractual services is possible without processing personal data.[138] Therefore, if the other party of the contract wants to process personal data, it is better to rely on other bases mentioned in article 6 including the data subject's freely given consent.[139] The legal base

---

[136] *Id*.

[137] GDPR Article 6(b).

[138] European Data Protection Board Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0 (2019), page 7, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

[139] *Id*.

should be identified before processing and the information should be given to the data subject to comply with GDPR articles 13 and 14.[140] To identify the appropriate lawful basis, the controller should take into account the principles of fairness and purpose limitation.[141]

With regards to the processing of special categories of personal data, "Article 9(2) does not recognize 'necessary for the performance of a contract' as an exception to the general prohibition to process special categories of data.[142] Therefore, "obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data."[143]

6.1.Necessary for the Performance of a Valid Contract Between the Controller and the Data Subject

"Necessity of processing is a prerequisite for both parts of Article 6(1)(b)."[144] The necessity of the processing for the performance of a contract is not just looking at the terms of the contract if it is permitted or not.[145] The fact that processing is mentioned in a contract does not automatically mean that the

[140] *Id*.
[141] *Id*.
[142] *Id*.
[143] *Id*, at 7-8.
[144] *Id*, at 8.
[145] *Id*.

processing is necessary for its performance.[146] "On the other hand, processing may be objectively necessary even if not specifically mentioned in the contract."[147] The controller should also consider the objection of the regulation which is the protection of personal data and fundamental right to privacy, along with the principle of the fairness.[148] The controller must first identify the processing purpose within the context of the contract and further has to specify and communicate those purposes with the data subject.[149] Moreover, the controller's assessment should be consistent with purpose limitation and transparency obligations.[150]

To do processing based on part b of article 6, the controller shall establish first, the processing is within the context of a valid contract between the controller and the data subject.[151] Secondly, the processing is objectively and genuinely necessary to the performance of that particular contract.[152] To do so, "it is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective"[153] Otherwise, the controller shall

[146] *Id*.
[147] *Id*, at 9.
[148] *Id*.
[149] *Id*.
[150] *Id*.
[151] *Id*.
[152] *Id*.
[153] *Id*.

consider another legal basis for processing.[154] The controller shall find the nexus between processing of personal data and the performance or non-performance of the service under the contract with the data subject.[155]

6.2.The Standard Criteria for the Controller to Find the Necessity of the Processing

Necessity justification refers to "the fundamental and mutually understood contractual purpose."[156] Therefore, it not only depends on the controller's perspective but also on a reasonable data subject's perspective at the time of entering into the contract.[157] The necessity of the processing also depends on the assessment of the contract to see if it can still be performed without the processing.[158] The controller should "examine carefully the perspective of an average data subject in order to ensure that there is a genuine mutual understanding on the contractual purpose."[159]

For example, in an online shopping context, a user purchases some items from a website and provides his credit card information to pay for the

[154] *Id*.
[155] *Id*.
[156] *Id*, at 10.
[157] *Id*.
[158] *Id*.
[159] *Id*.

shopping and, his home address to get the purchase delivered.[160] Then, processing personal data including credit card information and home address are necessary to perform the online contract.[161] Moreover, some other specific actions such as sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract are also necessary and foreseeable within a normal contractual relationship.[162] However, if the website controller wants to make the user's profile for the purpose of targeting advertising, he cannot rely on the legal bases that "processing is necessary for the performance of the contract."[163] Because it is not, even if profiling is mentioned in the contract.[164] Therefore, the controller shall rely on a different legal basis provided their relevant criteria are met.[165]

In a similar situation, web controllers routinely include the possibility of improvements and modifications to service in contractual terms with users. However, such processing usually cannot be considered as being objectively necessary for the performance of the contract with the user.[166] In

[160] *Id*, at 11.
[161] *Id*.
[162] *Id*.
[163] *Id*.
[164] *Id*.
[165] *Id*.
[166] *Id*, at 14.

fact, "The EDPB does not consider that Article 6(1)(b) would generally be an appropriate lawful basis for processing for the purposes of improving a service or developing new functions within an existing service. In most cases, a user enters a contract to avail of an existing service."[167]

6.3.Necessary in Order to Take Steps at the Request of the Data Subject Prior to Entering A Contract

The second part of article 6(1)(b) is about a legal base for processing, when processing is "necessary in order to take steps at the request of the data subject prior to entering into a contract." For example, a data subject gives its postal code to a specific internet provider to see if his neighborhood is covered by the provider's services. This can be regarded as an application of necessary processing "in order to take steps at the request of the data subject prior to entering into a contract".

7. GDPR Protects Personal Data Which Are Accessible to the Public

The short answer to the research question if GDPR protects publicly accessible personal data is YES. This section aims to analyze the answer to

[167] *Id.*

the question and further discusses two other relevant and important topics which are *automated individual decision-making* and *profiling*.

To better visualize the difference between GDPR and US privacy law, this section examines the relevant US case, *hiQ Labs, Inc. v. LinkedIn Corp.*, which was decided in front of the U.S. District Court for the Northern District of California and the United States Court of Appeals for the Ninth Circuit. It particularly hypothesizes the case in front of the EU authorities and discusses how the case decision would be different from the issued US decision. The importance of this discussion is to add GDPR data protection analysis to the US decision and recommend data protection policies to the field of data protection law in the US. This is increasingly important as adequate data protection regulations change access to the global economy, produce both new market and increased competition, and harmonize data protection principles around the world.

Before starting the discussion, it is worth mentioning that in the US even CA data privacy laws, pioneer privacy laws in the US, do not protect publicly available personal information or lawfully obtained, truthful information that is a matter of public concern.[168]Under CPRA, publicly

[168] CPRA 1798.140 (v)(2).

available information means information that is lawfully made available from federal, state, or local government records.[169] Publicly available information also includes information that a business has a reasonable basis to believe that is lawfully made available to the general public by the consumer or from widely distributed media.[170] It also includes information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.[171] However, biometric information collected by a business about a consumer without the consumer's knowledge is not publicly available information.[172]

7.1.Sample Case Overview: hiQ Labs, Inc. v. LinkedIn Corp

This section examines the relevant US case, *hiQ Labs, Inc. v. LinkedIn Corp,* which was decided in front of the U.S. District Court for the Northern District of California and the United States Court of Appeals for the Ninth Circuit. This case concerns data scraping by the third party, hiQ Labs, Inc. ("hiQ Labs") in the LinkedIn platform.[173] LinkedIn is a professional

[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (2021).

networking website with 810 million members in more than 200 countries.[174] LinkedIn defines its mission as creating "economic opportunity for every member of the global workforce"[175] through connecting professionals around the world.[176] LinkedIn members post their resumes and professional activities on their profiles, as well as provide feedback and comments to the other members' postings. According to LinkedIn's user agreement, members are the owner of the content, feedback, and personal information posted on LinkedIn and they only grant a non-exclusive license to LinkedIn to "use, copy, modify, distribute, publish and process"[177] the posted information. LinkedIn members have different options in privacy settings including which portions of their profile be visible to the public and which parts only be visible to direct connections or to all LinkedIn members.[178] Particularly, there is a "Do Not Broadcast" option in LinkedIn's privacy setting. If a LinkedIn member selects this option, she can update the information on her profile page, but her connections will not be notified.[179] Thus, the information is visible to

[174] Linkedin.com, About LinkedIn, https://about.linkedin.com/.
[175] *Id.*
[176] *Id.*
[177] Linkedin.com, User Agreement, https://www.linkedin.com/legal/user-agreement.
[178] *Id.*
[179] *Supra* note 173.

anyone permitted to view her profile under her general privacy setting.[180] To protect the personal data of its members from misuse or misappropriation, LinkedIn uses a text file named *robots.txt* to prohibit search engines and web robots to find access to LinkedIn servers.[181] Certain entities such as the Google search engine, have express permission from LinkedIn to access bots.[182] LinkedIn also utilizes several technological systems to detect suspicious activities and restrict automated scraping.[183]

hiQ Labs is a company that its mission is to help the human resource of entities through data science and machine learning.[184] hiQ Labs extracts public data, particularly from LinkedIn and sells the data to employers.[185] The selling data includes the predictions of employee's summaries and skills.[186] In May 2017, LinkedIn blocked hiQ Labs's data processing because of violating the US Computer Fraud and Abuse Act ("CFAA"), the Digital Millennium Copyright Act ("DMCA"), California Penal Code § 502(c), and

---

[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.* Data scraping is used to extract data including publicly accessible data from websites and to copy it into a structured format. Data scraping is typically done by a web robot or bot (Fiona Cambell, Data Scraping – Considering the Privacy Issues (2019), https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-scraping-considering-the-privacy-issues.).
[184] hiQ, Who we are, https://www.hiqlabs.com/.
[185] Epic.org, ELECTRONIC PRIVACY INFORMATION CENTER, hiQ Labs, Inc. v. LinkedIn Cor (2020), https://www.epic.org/amicus/cfaa/linkedin/.
[186] *Supra* note 173.

the California Common Law of Trespass. [187] Moreover, LinkedIn claims that hiQ Labs's data scraping is against LinkedIn's user agreement.[188] In response, hiQ Labs filed a lawsuit and sought injunctive relief and a declaratory judgment to find access to LinkedIn profile data, to which the parties subsequently agreed on a motion for a preliminary injunction. [189] The U.S. District Court for the Northern District of California granted hiQ Labs's motion and ordered LinkedIn to remove technical hurdles and grant access to public profiles.[190] Consequently, LinkedIn timely appealed, and the Ninth Circuit further affirmed the decision. LinkedIn petitioned the U.S. Supreme Court for review. Subsequently, the Supreme Court has vacated the opinion in this case and remanded with instructions to the Ninth Circuit to reconsider the decision in light of *Van Buren v. United States* case[191]. At the time of writing this article, this case has not been decided further.

The main question in this section is whether pursuant to GDPR, an EU authority can order LinkedIn to provide access to its user's personal profile to hiQ Labs which is a third-party data mining company. This section

---

[187] *Id*.
[188] *Id.*
[189] *Id*.
[190] *Id*.
[191] *LinkedIn Corp. v. hiQ Labs,* 141 S.Ct. 2752, 210 L.Ed.2d 902 (2021); *Van Buren v. United States,* 141 S. Ct. 1648 (2021).

hypothesizes the aforementioned case in front of the EU authorities and examines how the decision would be different from the issued US decision. GDPR defines personal data as "any information relating to an identified or identifiable natural person"[192] and the regulation applies to any information as it is indicated regardless of being publicly available or not. GDPR Article 4(7) defines a controller as:

> 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.[193]

The controller shall have one of the lawful bases mentioned in GDPR article 6 to process data subject's personal data. Article 6(1)(a) is about a data subject's given consent "to the processing of his or her personal data for one or more specific purposes".[194] Controllers routinely use user agreements as a means of receiving data subject's consent. Therefore, users' information on the LinkedIn platforms including websites and apps are data subjects'

[192] GDPR Article 4.
[193] GDPR Article 4(7).
[194] GDPR Article 6(1)(a).

personal data, and hiQ Labs as a third-party controller[195] must also have a legal base such as the data subject's consent to process such data.

Although GDPR has adhered to the principle of public access to official documents under which public authorities or public bodies disclose data subjects' personal data for the purpose of public interest, however, the purpose of this principle is complying with EU or member state law under which public authority or public body is subject to.[196] This principle is only for official documents and should be narrowly interpreted for public authorities and public bodies.[197] Therefore, the principle of public access to official documents is not applicable to the *hiQ Labs* case.

7.2.Making Online Profiles for Individuals and Making Automated Decisions

GDPR article 14 has set obligations for the controllers including hiQ Labs where personal data has not been obtained from the data subject. Among which, the controller shall inform the data subject about the identity of the controller, the purpose of the processing of personal data, and the recipients

[195] hiQ Labs is considered as a controller because it determines the purpose of processing personal data (GDPR article (4)).
[196] Piotr Foitzik, publicly available data under the GDPR: Main considerations (2019), https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/.
[197] *Id.*

or categories of recipients of the personal data.[198] The controller is also obligated to provide "information necessary to ensure fair and transparent processing in respect of the data subject".[199] Furthermore, if the processing involves automated decision-making including profiling, the controller shall provide meaningful information to the data subject which includes the processing logic, the significance and the foreseeable consequences of such processing for the data subject.[200]

Making online profiles for individuals and making automated decisions is one of the functions of today's technology. GDPR defines profiling as any form of automated processing that involves the use of personal data to evaluate certain personal aspects relating to a natural person.[201] Controllers particularly aim to analyze or predict economic situations, health, personal preferences, interests, reliability, behavior, location, or movements of concerning natural persons through profiling.[202] Similarly, hiQ Labs is a controller that extracts personal data of LinkedIn's users and sells the data to employers.[203] The data also includes the predictions of employee's

[198] GDPR article 14(1)(a) and (c).
[199] *Id*. *Also see*: European Data Protection Board, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) (2018), https://ec.europa.eu/newsroom/article29/items/622227.
[200] *Id*.
[201] GDPR article 4(4).
[202] *Id*.
[203] *Id*.

summaries and skills which makes hiQ Labs' processing within the meaning of GDPR profiling.

Deep machine learning, artificial intelligence and secret algorithmic processing can be misleading and cause discrimination against individuals through automatic decision making.[204] GDPR has generally condemned automatic decision making and recognized the right for the data subject, "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[205] To give an example, in the *Foodinho* case, Foodinho is a subsidiary of GlovoApp23 and was fined EUR 2.6 million by Italian SA, *Garante per la protezione dei dati personali*, due to processing its riders' data through a digital platform and using algorithms to book and assign orders for food and other products to the riders.[206]

[204] Colin J. Bennett, Personal Data Processing by and for Political Campaigns: The Application of the Council of Europe's Modernised Convention108, Council of Europe, 22 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3633976.
[205] GDPR article 22(1), *also see* European Commission, Guidelines on Automated individual decision-making, and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
[206] European Data Protection Board, ITALIAN SA SAYS NO TO ALGORITHMS CAUSING DISCRIMINATION A platform in the Glovo group fined EUR 2.6 million (2021), https://edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en.

The Italian SA reasoned that "the company had failed to adequately inform its employees on the functioning of the system and had not implemented suitable safeguards to ensure accuracy and fairness of the algorithmic results that were used to rate riders' performance."[207] Additionally, the company had no human interference to review and contest the algorithmic decisions during the procedures to exclude its employees from work assignments.[208]Accordingly, the Italian SA ordered Foodinho to stop profiling and automated decision-making to protect riders' rights and freedoms.[209] The risk in this case is about the rating and assessing system, which is based on the application of a mathematical formula. Penalties are determined based on how promptly riders accept or reject orders and the riders who accept most orders are prioritized. The company also has to stop using inappropriate and discriminatory measures such as customer feedback and comments.[210]

Foodinho was also ordered "to check accuracy and relevance of the data used by the system – chats, emails and phone calls between riders and customer care, geolocation at 15-second intervals, mapping of routes,

[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*

estimated and actual delivery time, details on the handling of current and past orders, feedback from customers and partners, device battery level, etc."[211] The Italian SA also expressed that the purpose of the order is to minimize the risk of errors and biases that might result in reducing delivery assignments to certain riders or excluding a rider from the platform.[212]

Similarly, hiQ Labs conducts algorithmic profiling for the purpose of predicting LinkedIn members' summaries and skills. The assessment is based on the information, comments, and activities that LinkedIn members have in their profiles. One of the main questions that the EU authority will consider is if hiQ Labs has adequately informed LinkedIn members on the functioning of the system and implemented suitable safeguards to ensure the accuracy and fairness of the algorithmic results that are used to assess LinkedIn members. hiQ Labs' decisions and profiling should not be solely based on automated processing and, therefore, not significantly affect the LinkedIn members' circumstances as not being considered in job applications by employers in LinkedIn or other online job platforms. Similar to Foodinho's riders, it is possible that LinkedIn members receive inappropriate and discriminatory comments about their activities on

[211] *Id.*
[212] *Id.*

LinkedIn which will negatively affect their related hiQ Labs' assessment. Also, it is not clear what course of action is hiQ Labs taking to minimize the risk of errors and biases that might result in reducing job access to certain LinkedIn members or excluding them from a certain job opening.

In comparison with the GDPR, under the CPRA "Profiling means any form of automated processing of personal information … to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[213] Moreover, CPRA added that any inferences obtained from any identified personal information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes would also be considered as personal information.[214] Under CPRA 1798.185 (a)(16), the Attorney General is obligated to solicit broad public participation and adopt regulations to further the purposes of CPRA in specific areas including Issuing regulations governing access and opt-out rights with respect to businesses'

[213] CPRA 1798.140 (z).
[214] CPRA 1798.140 (K)

use of automated decision-making technology, including profiling.[215] Also, requiring businesses to respond to access requests and include meaningful information about the logic involved in decision-making processes, as well as a description of the likely outcome of the process regarding the consumer.[216]

However, as discussed before, so far even CPRA does not protect publicly available personal information.[217]As such, in the LinkedIn case study, it could be analyzed: as LinkedIn users made their personal information available to the public then their information would be considered as publicly available personal information and not protected by the CPRA.[218]

7.3.The Data Subject Shall Have the Right Not to Be Subject to A Decision Based Solely on Automated Processing

According to the GDPR article 22, "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[219] GDPR Article 22(2) and recital 71 has set

[215] CPRA 1798.185 (a)(16).
[216] *Id*.
[217] CPRA 1798.140 (v)(2).
[218] *Id*.
[219] GDPR Article 22.

exceptions to the general prohibition rule. Under this, if the automatic decision making based on such processing is not expressly authorized by Union or Member State law, or it is not necessary for the entering or performance of a contract, the data subject's explicit consent is required for conducting such processing.[220]

Therefore, unless one of the exceptions applies, the "scraping of personal data from social media sites is generally not legal under European data protection law without explicit consent"[221] of data subjects. For instance, in *the Nationbuilder* case, the French SA, CNIL has ruled Nationbuilder Match's program as illegal, and the company has been forced to stop its services globally.[222] The program offered match services for its user's email list on Facebook, Twitter, LinkedIn, and Klout. The matching offer was based on data scraping of data subject's personal data without receiving their consent.

In the *Aquateknikk* case, the Norwegian SA has fined Aquateknikk for performing credit rating on individuals without having legal bases.[223] This

[220] GDPR Article 22(2) and Recital 71.
[221] *Supra* note 205, at 18.
[222] *Id*.
[223] European Data Protection Board, Norwegian DPA issues fine to Aqueteknikk AS (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-issues-fine-aquateknikk_en.

case is about a person's complaint who had no customer relationship or any other connection with Aquateknikk and discovered that Aquateknikk had performed a credit rating on him.[224] A credit rating is about profiling an individual for the purpose of how likely the person will be able to pay his debts.[225] "A credit rating will also include detailed information about the person's personal financial situation, such as debt-to-income ratio, payment remarks, and the person's mortgages, if any."[226] Data scraping is the way that Aquateknikk compiled personal data for the purpose of finding individuals' credit ratings. Moreover, credit rating is sensitive personal data[227] that the controller must also comply with GDPR Article 9 obligations. Similarly, in the *hiQ Labs* case, as none of the exceptions in GDPR article 22(2) applies, hiQ Labs is required to have LinkedIn members' explicit consent to conduct their data scraping and algorithmic profiling.

7.4.The Requirements for Transparent and Fair Processing

GDPR Article 5 (1)(a) indicates that personal data processing shall be lawful, fair, and transparent regarding the data subjects. Also, pursuant to the principles of fair and transparent data processing ("transparency

[224] *Id*.
[225] *Id*.
[226] *Id*.
[227] *Id*.

principle"), the data subject shall be informed of the existence and purposes of data processing.[228] It should be transparent to the data subject to what extent the personal data are or will be processed.[229] The transparency principle also requires controllers to inform their identities to data subjects. Transparency principle in data protection law is a crucial standard to build trust.[230] GDPR's purpose is to protect data subjects' personal data and increase the trust between businesses and customers. Consequently, GDPR requires controllers to receive data subjects' informed consent or have other legal bases for each specific purpose they want to process data.[231] Moreover, according to the GDPR recital 61:

> The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. [232]

---

[228] GDPR Recital 60. Transparency is not defined in the GDPR, however recital 39 of the GDPR is informative as to the meaning of the transparency. The transparency elements have also been explained in the Article 29 Data Protection Working Party's guideline (European Commission, *Article 29 Working Party: Guidelines on transparency under Regulation 2016/679* (2018), *available at* https://ec.europa.eu/newsroom/article29/redirection/document/51025).

[229] GDPR Recital 39.

[230] *Supra* note 205, at 21.

[231] GDPR Article 6.

[232] GDPR Recital 61.

In the course of a political campaign statement, the EPDB has indicated that public personal data or otherwise shared data regardless of revealing political opinions are still subject to the EU data protection law.[233] Therefore, using the same analogy, data collected through social media or other public websites such as LinkedIn for the purposes of processing cannot be used without complying with the GDPR obligations including transparency, purpose specification, and lawfulness. Accordingly, hiQ Labs who wants to process personal data sourcing from third-party controllers, has to apply due diligence to make sure that appropriate consent has been obtained and the transparency requirements are met. The transparency principle requires hiQ Labs to inform the data subject about the existence of the processing and its purposes. The hiQ Labs shall also provide the data subject with any further information necessary to ensure fair and transparent processing, considering the specific circumstances that the data is scraping and processing in this case. hiQ Labs shall provide meaningful information to the data subject which includes the existence of profiling, the processing

[233] *Supra* note 205, at 18. *Also see* European Data Protection Board, Statement 2/2019 on the use of personal data in course of political campaigns (2019), https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

logic, and the foreseeable consequences of such profiling for the data subject.[234]

7.5.The Controller Is Required to Prevent Unauthorized Access to Personal Data

GDPR requires the controller to prevent unauthorized access to personal data and ensure the appropriate security.[235] Data subjects' personal data shall be collected for specified, explicit, and legitimate purposes and furthermore, shall not be processed in a manner that is not compatible with those purposes.[236] Therefore, it is LinkedIn's duty as controller to make aware its members of potential risks and safeguards of processing their personal data. These potential harms include the risk of mis-analyzing and exposure to potential data breaches by hiQ Labs and their party companies that are going to assess and sell the information.

The purpose of data protection regulation is to protect individuals' personal data. hiQ Labs is not the only company that uses and sells scraped data since scraping data from public profiles is a straightforward way to obtain data and particularly when jurisdictions do not protect public data.

[234] GDPR Article 14(1)(a) and (c); and Recital 60.
[235] GDPR Recital 39.
[236] GDPR Article 5(1)(b).

Companies that obtain data directly from individuals are required by law to protect the data and to provide their users with basic rights such as providing information about their purpose for collecting and/or selling data pursuant to the terms of their user agreements and privacy policies.

However, in the US due to the lack of comprehensive data protection law, third-party scrapers such as hiQ Labs have permission to use individuals' personal data without being required to protect individuals' data and to provide basic data protection rights to the individuals. Rights such as being informed of the purpose of data processing are basic and commonly known rights for data subjects in data protection regulations across the world.

In the *hiQ Labs case*, not only the U.S. courts don't condemn but also support the inappropriate and unethical use of data subjects' personal data by ordering LinkedIn to remove technical hurdles and grant hiQ Labs access to public profiles. Whereas LinkedIn's members may never even know that hiQ Labs has collected, profiled, analyzed, and sold their data to employers. In this case, the decision of the U.S. District Court for the Northern District of California and the United States Court of Appeals for the Ninth Circuit is irrespective of world-known data protection principles. In fact, the

decision would be a dangerous precedent that could threaten the data protection rights in the U. S.

8. Conclusion

GDPR regulates all personal data related to living individuals in the EU regardless of the type of the data or the entity that controls or processes it. GDPR "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[237] Moreover, GDPR also "applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities" meet certain criteria provided in the GDPR article 3.[238] GDPR article 6 articulates different bases that make the processing of personal data lawful. Among which are data subject consent and the necessity of the processing for the performance of a contract. In cyberspace, controllers normally get their data subject's consent through user agreements. Thus, it could be confusing for the controllers which type of lawful base for the processing they are involved in and which

[237] GDPR Article 3(1), European Data Protection Board has issued a guideline to more clarify GDPR territorial scope. For further exploration of this view, see also: https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[238] GDPR Article 3(2).

GDPR requirements they need to comply with. This chapter discussed the difference between these two types of lawful bases in the context of contracts. Moreover, this chapter further discussed different types of real cases in the relevant sections to show the importance of each provision and how EU SAs are implementing GDPR and imposing fines in case of a data breach.

Chapter two discussed the required elements of a valid consent articulated in GDPR article 4(11). It examined different typical types of user agreements, as contracts between a controller and data subject to see if they fulfill GDPR requirements. It also demonstrated that when data processing is based on data subjects' consent, the burden of proof is on controllers to prove that the data subject has given the required consent to the processing operation. This is especially important when the controller sends a written declaration on another matter to the data subject. In this context, the controller shall be able to prove that the data subject has been aware of the fact and to what extent the consent is given meaning the consent shall be informed and specific.

Chapter two analyzed that GDPR protects personal data which are accessible to the public and analyzed two other relevant topics which are

automated individual decision-making and profiling. To better visualize the significance of GDPR protection regarding public personal data, chapter two examined the relevant US case, *hiQ Labs, Inc. v. LinkedIn Corp.*, which was decided in front of the U.S. District Court for the Northern District of California and the United States Court of Appeals for the Ninth Circuit and concluded that EU authorities will not order LinkedIn to provide access to the personal data of its users to third-party data mining company, hiQ Labs.

Finally, chapter two examined article 6(1)(b) which is about the criteria of contracts, as a lawful base to process data subjects' personal data. Article 6(1)(b) is divided in two main discussion areas. The first part is about "processing is necessary for the performance of a contract to which the data subject is party". The EDBP recognizes that processing is not "necessary for the performance of a contract", when providing the contractual services is possible without processing personal data.[239] Therefore, if the other party of the contract wants to process personal data, it is better to rely on other bases mentioned in article 6 including data subject's freely given consent.[240] The legal base should be identified before processing and the information should be given to the data subject to comply with GDPR article 13 and

[239] *Supra* note 205.
[240] *Id*.

14.[241] To identify the appropriate lawful basis, the controller should also take into account the principles of fairness and purpose limitation.[242]

The second part is about necessary processing "in order to take steps at the request of the data subject prior to entering into a contract." To do processing based on part b of the article 6, the controller shall establish first, the processing is within the context of a valid contract between the controller and the data subject.[243] Secondly, the processing is objectively and genuinely necessary to the performance of that particular contract.[244] To do so, "it is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective"[245] Otherwise, the controller shall consider another legal basis for processing.[246] The controller shall find the nexus between processing of personal data and the performance or non-performance of the service under the contract with the data subject.[247] Therefore, this section discusses the standard for the controller to find out the necessity of the processing.

---

[241] *Id.*
[242] *Id.*
[243] *Id.*
[244] *Id.*
[245] *Id.*
[246] *Id.*
[247] *Id.*

Necessity justification refers to "the fundamental and mutually understood contractual purpose."[248] Therefore, it not only depends on the controller's perspective but also on a reasonable data subject's perspective at the time of entering into the contract.[249] The necessity of the processing also depends on the assessment if the contract can still be performed without the processing.[250] The controller should "examine carefully the perspective of an average data subject in order to ensure that there is a genuine mutual understanding on the contractual purpose."[251]

[248] *Id*, at 10.
[249] *Id*.
[250] *Id*.
[251] *Id*.

CHAPTER 3: CONTROLLERS, PROCESSORS, AND SUB-PROCESSORS RESPONSIBILITIES AND GDPR PRINCIPALES IN CASE OF PAYING DAMAGES

1. Introduction: The Importance of Contracts

The concepts of the controller, joint controller, and processor play an important role in the function of the General Data Protection Regulation 2016/679 (GDPR). Because "they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice."[1] A controller determines the purposes and means of processing and will be responsible and liable for any personal data processing conducted on its behalf.[2] The processor is only permitted to process personal data based on the controller's documented instructions.[3] However, this doesn't mean that the processor doesn't have liability. He is jointly liable with the controller and his liability is limited to violations of obligations that are specific to him.[4] After all, "The controller

[1] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0 (2020), page 3, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.
[2] GDPR Recital 74.
[3] *Id.*
[4] GDPR Article 28 (2).

is the first contact for the data subject and responsible that the data processing complies with the Regulation."[5]

GDPR Article 28(3) describes the minimum requirements of the contracts between the controller and the processor. The EDPB encourages the parties to use the same wording in the contract as in the GDPR, if a clause in the contract is inspired by a GDPR clause.[6] The contract shall determine the subject matter and duration of the processing, the nature, and purpose of the processing, the type of personal data and categories of data subjects for the purpose of processing, and the obligations and rights of the controller.[7]

Having a contract between processors and controllers helps the parties to understand their responsibilities and liabilities. Contracts ensure legal certainty and avoid possible conflicts in the relationship between the data actors and between the data subjects and the data protection authorities. Moreover, contracts provide certainty and help controllers and processors to prove their compliance with GDPR in transparency and accountability

[5] GDPR Key Issues, Processing; https://gdpr-info.eu/issues/processing/.
[6] European Data Protection Board, Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR (2019), page 7, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf and https://edpb.europa.eu/news/news/2019/first-standard-contractual-clauses-contracts-between-controllers-and-processors-art_en.
[7] GDPR Article 28(3).

principles.[8] GDPR Article 28 in subsection 8 indicates an option for SAs that may adopt SCCs to facilitate the consistency mechanism mentioned in article 63.[9] Article 64 further obligates the EDPB to issue an opinion where a competent SAs intends to adopt SCC referred to in Article 28 subsection 8.[10]

The parties of the contract can choose SCCs by a SA and also add other provisions to their contracts "provided that they do not contradict, directly or indirectly, the adopted clauses or prejudice the fundamental rights or freedoms of the data subjects."[11]However, the parties who use a modified version of the clauses are not deemed to have the safeguards of the adopted SCCs for compliance purposes [12] This section not only analyzes article 28 but also will emphasize the EDPB's opinion on Danish SSCs to make clear the importance of each provision in the contracts between the controllers and the processors.

On 12 November 2020, the EC published a draft decision and SCCs between controllers and processors for the matters referred to GDPR Article 28

[8] Information Commissioner's Office, When is a contract needed and why is it important, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/.
[9] GDPR Article 28 (8), also see GDPR Article 63 and Recital 135 related to the consistency mechanism.
[10] GDPR Article 64(d)
[11] *Supra* note 6, at 5.
[12] *Id.*

subsection 3 and 4 and requested a joint opinion of the EDPB and EDPS on the basis of GDPR Article 42(1) and (2).[13] Thereafter, EDPB and EDPS issued a joint opinion limited to the EC draft decision and SCCs between controllers and processors, and processors and sub-processors for the matters referred to in GDPR Article 28 (3) and (4).[14]

The purpose of the joint opinion is to ensure consistency and an appropriate application of GDPR Article 28 with regard to the SCCs in GDPR Article 28(7).[15] Moreover, SCCs could be considered as a set of guarantees if they are used, as they are, to mitigate specific risks associated with data processing.[16]Therefore, SCCs could be considered as a strong accountability tool to prove GDPR compliance by the controllers and processors.[17]Finally, SCCs will ensure EU harmonization and legal certainty within the context of protecting personal data.[18]

Similar to the GDPR, the CCPA and CPRA also obligate "a business that collects a consumer's personal information and that sells that personal

[13] European Data Protection Board, EDPB-EDPS Opinion 1/2021 on the European Commission's Implementing Decision on standard contractual clauses between controllers and processors, page 4, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en.
[14] *Id*.
[15] *Id.*
[16] *Id*.
[17] *Id, at 5*.
[18] *Id*.

information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose" to enter into an agreement with the third party, service provider, or contractor.[19]

This chapter will discuss the allocation of responsibility and liability between controllers and processors including joint controllers and sub-processors in the data processing. Moreover, it discusses GDPR non-compliance consequences and the critical factors in determining the amount of fines and allocating the responsibilities between different data processing actors.

2. Contracts between Joint Controllers

If two or more controllers jointly determine the purposes and means of processing, they are jointly responsible for the processing and there shall be an arrangement between joint controllers.[20] Contracts are one of the means between joint controllers to determine their obligations. The contract shall provide general information on the joint processing by defining the subject

[19] CPRA 1798.100.d.
[20] GDPR Article 26(1).

matter and purpose of the processing, the type of personal data, and the categories of data subjects.[21]

2.1.Allocation of the Responsibilities

The contract shall also clearly define the respective responsibilities for compliance obligations under GDPR.[22] The parties shall particularly allocate between themselves "*who will have to do what*" with regards to the data subjects' rights unless the duties are determined by Union or Member State law to which the controllers are subject.[23] For instance, the parties have to decide who will be responsible for answering the data subject's requests or providing information to them.

The parties should consider the factors such as, "who is competent and in a position to effectively ensure data subject's rights" to allocate the obligations between themselves.[24] In fact, this analysis is part of the documentation under the accountability principle.[25] The parties do not need to allocate the duties equally between themselves, however, there are situations that both parties require to meet the same GDPR requirements,

[21] *Supra* note 1, at 43.
[22] GDPR Article 26(1).
[23] *Id.*
[24] *Supra* note 1, at 42.
[25] *Id.*

for example, complying with accountability or purpose limitation principles.[26] Overall, the parties shall ensure that the whole joint processing is fully meeting GDPR requirements.[27]

2.2.The Essence of the Arrangement Shall be Made Available to the Data Subject

According to the GDPR Article 26(2), the essence of the arrangement between joint controllers shall be made available to the data subject. Controllers must get the informed consent of their data subjects if they are using a joint controller to determine the purpose and means of processing. Therefore, a web controller must get the informed consent of their users to be allowed to use cookies or similar tools on their websites for analysis and marketing purposes, and if controllers share user's personal data with third controllers and enable them to track users while they are exploring the web.[28]

[26] *Id.*
[27] *Id.*
[28] JDSUPRA, The end of dark patterns in "cookie walls": German court bans deceptive designs, Peter Hence, January (2021), https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/.

2.3. Third-Party Beneficiary Right for the Data Subject

According to the GDPR Article 26 subsection 3, the data subject can exercise his or her rights under GDPR in respect of and against each of the controllers, regardless of the terms of the contract between joint controllers.[29]

Google Analytics, Facebook pixel, and Facebook as joint controllers_ According to the …, using third parties such as Google Analytics and the Facebook pixel by the controllers such as Facebook will result in joint controllership under GDPR Art 26 under which "the essence of the arrangement"[30] between the joint controllers must be made available to the users.[31]

ShareThis or AddThis companies_ AddThis and ShareThis offer free social bookmarking services to the web-developers.[32] Once the developers add the companies' widgets on their website, visitors to the website can bookmark or share an item on the website through using other services such as Facebook, MySpace, Google, Bookmarks, Pinterest, and Twitter.

[29] GDPR Article 26(3), *supra* note 1, at 43.
[30] GDPR Article 26(2).
[31] *Id.*
[32] Privacy International, AddThis, About Us, https://www.addthis.com/about/; https://en.wikipedia.org/wiki/AddThis and https://privacyinternational.org/case-study/4403/tracking-service-sharethis-be-profiled.

Companies like AddThis or ShareThis track web users with their apparently innocent ShareThis or AddThis buttons at the top of other websites and collect user's personal data without getting their informed consent.

From GDPR point of view, Web-developers of each website are considered as a controller and they should be aware that by integrating and adding the widgets on their websites, they are adding the pertaining tech companies as a joint controller on their web. Therefore, this action will bring new responsibilities for them as joint controllers.

3. Controller's Responsibilities When Using a Processor

GDPR Article 24 describes the responsibility of the controller. In particular, the controller has ongoing responsibility to implement appropriate and effective measures and to demonstrate the GDPR compliance based on the accountability principle. To ensure the appropriate measures, the controller should consider "the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons."[33]

[33] GDPR Recital 74.

Similarly, CCPA and CPRA obligates a business that collects a consumer's personal information to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.[34]

EDP COMERCIALIZADORA[35]- For instance in the EDP Comercializadora case, Spanish data protection authority (the AEPD) imposes a fine of 1,500,000 euros on EDP Comercializadora due to not adopting technical and organizational measures to "verify whether a person who hires Comercializadora services on behalf of another natural person has authorization to carry out the contracting."[36] The AEPD also finds that Comercializadora did not either adopt technical and organizational measures to verify whether, the person who acts on behalf of the data subject, is authorized by the data subject to consent to other processing of personal data on his behalf.

[34] CPRA 1798.100.e.

[35] European Data Protection Board, Spanish DPA imposes fine of 1,500,000 euros on EPD Comercializadora, S.A.U. for two infractions of the GDPR (2021), https://edpb.europa.eu/news/national-news/2021/spanish-dpa-imposes-fine-1500000-euros-epd-comercializadora-sau-two_en.

[36] *Id.*

3.1 Choosing Competent Processor

In choosing the processor, the controller must ensure that the processor will implement sufficient technical and organizational measures to comply with the requirements of the Regulation.[37]

3.1.1 The Processor Shall Demonstrate Sufficient Guarantee

According to GDPR Article 28(1), the controller can only use the processors that give sufficient guarantees, particularly in terms of expert knowledge, security, reliability, and resources, and apply appropriate technical and organizational measures in which the processing will fulfill the requirements of GDPR and ensure the protection of the rights of the data subject.[38] The processor's commitment to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 could be used to some extent as an element to demonstrate such sufficient guarantees.[39] Also, according to GDPR Recital 77, the controllers and the processors could demonstrate implementation of

[37] *Supra* note 5.
[38] GDPR Article 28(1) and Recital 81.
[39] GDPR Article 28(5).

appropriate measures by following guidelines provided by the EDPB or indications provided by a data protection officer.[40]

3.1.2 Approved Code of Conduct as a Means of GDPR Compliance

GDPR Code of conducts is a volunteer tool by which the controllers and processors can demonstrate their GDPR compliance. Associations and other controllers' or processors' representing bodies may write codes of conduct and submit them to the competent SA pursuant to Art 55.[41] If the draft code provides sufficient appropriate safeguards, the SA shall approve it. Otherwise, the authority will give its opinion on if the code fulfills GDPR compliance.[42] According to GDPR Art. 40, a variety of subjects such as the transfer of personal data to third countries and the collection of personal data could be addressed in the codes.[43]

3.1.3 Approved Certification as a Means of GDPR Compliance

GDPR Article 42 encourages the establishment of data protection certification mechanisms through which controllers and processors can

[40] GDPR Recital 77.
[41] GDPR Article 40(2) and (5).
[42] GDPR Article 40(5).
[43] GDPR Article 40(2).

demonstrate GDPR compliance.[44] In addition, they may demonstrate the existence of appropriate safeguards through such mechanisms.[45] The adherence to certification shall be voluntary and transparent through the relevant process and it does not reduce the responsibility of the controller and the processor.[46] Article 43 sets forth the bodies that can issue the certification.[47] Certification bodies are accredited by the competent SA and/or the national accreditation body named in article 43 (1)(b).

On 25 May 2018, EDPB adopted a guideline on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.[48] The guideline is not a procedural manual for certification and its primary purpose is to explain the key concepts, the purpose of certification, the rationale for certification as an accountability tool and what can be certified under Articles 42 and 43.[49] Some examples of accredited certification bodies are EuroPriSe, TRUSTe, and cyber-Essentials which specialize in different areas of compliance such as cybersecurity, IT

[44] GDPR Article 42(1).
[45] GDPR Article 42(2).
[46] GDPR Article 42(3) and (4).
[47]GDPR Article 42(5).
[48] European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en.
[49] *Id.*

services, and products.[50] Certifications will be valid for a maximum period of three years and if the relevant requirements are met, it is also renewable.[51]

4. Contracts Between Controllers and Processors as a Means of GDPR Compliance

A commissioned data processing contract is a legally binding contract that describes the rights and obligations between the controller and the processor. Normally, there is a third-party beneficiary in such a contract who is a group of data subjects whose personal data are processing under the contract. In subsequent sections, this research explains more about the provisions and the purpose of these contracts.

4.1 The Importance of Contracts

Having a contract between processors and controllers helps the parties to understand their responsibilities and liabilities. Contracts ensure legal certainty and avoid possible conflicts in the relationship between the data actors and between the data subjects and the data protection authorities.

---

[50] upcounsel, GDPR Certification: Everything You Need to Know, https://www.upcounsel.com/gdpr-certification#:~:text=GDPR%20certification%20is%20a%20new,are%20in%20compliance%20with%20GDPR.&text=GDPR%20also%20means%20greater%20data,other%20individuals%20in%20the%20EU.

[51] GDPR Article 42(7).

Contracts provide certainty and help controllers and processors to prove their compliance with GDPR in transparency and accountability principles.[52] Moreover, according to the GDPR, there should be a lawful base for processing data subject's personal data. So far, EU data protection authorities have decided on many infringement fees concerning the illegal processing of data subjects' personal data.

To compare with GDPR, CPRA use the word "Contractor" instead of "Processor". Similarly, CPRA obligates businesses to have contracts with contractors for processing consumers' personal information.[53] More specifically, contractor "means a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business…".[54] CCPA and CPRA also obligated businesses to have specific clauses in their contracts with contractors. This thesis discusses these clauses in the following specific subsections to provide a comparison between GDPR contract requirements and CCPA &CPRA.

[52] Information Commissioner's Office, When is a contract needed and why is it important, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/.
[53] CPRA 1798.140 (h) (j)(1).
[54] *Id.*

4.2 Standard Contractual Clauses

GDPR Article 28 in subsection 8 indicates an option for SAs that may adopt SCCs in order to aim for the consistency mechanism mentioned in article 63.[55]Article 64 further obligates the EDPB to issue an opinion where a competent SA intends to adopt SCC referred to in Article 28 subsection 8.[56] The parties of the contract can choose SCCs by a SA and also add other provisions to their contracts "provided that they do not contradict, directly or indirectly, the adopted clauses or prejudice the fundamental rights or freedoms of the data subjects."[57]However, the parties who use a modified version of the clauses are not deemed to have the safeguards of the adopted SCCs for compliance purposes.[58] This section not only analyzes article 28 but also will emphasize on the EDPB's opinion on Danish SSCs to make clear the importance of each provision in the contracts between the controllers and the processors.

Subsequently, the competent SA of Denmark has submitted its draft SCCs to the EDPB via the IMI system requesting an opinion from the EDPB

[55] GDPR Article 28. 8, also see GDPR Article 63 and Recital 135 related to the consistency mechanism.
[56] GDPR Article 64 (d).
[57] *Supra* note 6, at 5.
[58] *Id*.

pursuant to Article 64(1)(d) for a consistent approach at the Union level.[59] Hereby, the EDPB publishes its opinion. The controllers and the processors can use it to meet the requirements of the contract indicated in article 28. In its opinion, the EDPB mentioned that "that the contract between controller and processor cannot just restate the provisions of the GDPR but should further specify them, for example, with regard to the assistance provided by the processor to the controller."[60] In fact, a contract under Article 28 GDPR should further specify and clarify how the provisions of Article 28(3) and (4) will be fulfilled.[61]

On 12 November 2020, the EC published a draft decision on SCCs between controllers and processors for the matters referred to GDPR Article 28 subsection 3 and 4 and requested a joint opinion of the EDPB and EDPS on the basis of GDPR Article 42(1) and (2).[62] Thereafter, EDPB and EDPS issued a joint opinion limited to the EC draft decision and SCCs between

[59] *Id*, at 4.
[60] European Data Protection Board, First standard contractual clauses for contracts between controllers and processors (art. 28 GDPR) at the initiative of DK SA published in EDPB register, https://edpb.europa.eu/news/news/2019/first-standard-contractual-clauses-contracts-between-controllers-and-processors-art_en.
[61] *Supra* note 6, at 5.
[62] *Supra* note 60, at 4.

controllers and processors for the matters referred to in GDPR Article 28 (3) and (4).[63]

The purpose of the joint opinion is to ensure consistency and an appropriate application of GDPR Article 28 with regard to the SCCs in GDPR Article 28(7).[64] Moreover, SCCs could be considered as a set of guarantees if they are used, as they are, to mitigate specific risks associated with data processing.[65]Therefore, SCCs could be considered as a strong accountability tool to prove GDPR compliance by the controllers and processors.[66]Finally, SCCs will ensure EU harmonization and legal certainty within the context of protecting personal data.[67]

Parties to the SCCs and Annexes_ several controllers and processors could be parties to the SCCs for the processing.[68] All of the parties should be listed in a specific Annex as well as allocation of responsibilities and indicating which processor is carrying out which process on behalf of which controller and for which purposes.[69]Annexes are necessary for the parties to clarify "who is processing which personal data for whom and for what purpose,

[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id, at 5.*
[67] *Id.*
[68] *Id, at 6.*
[69] *Id, at 6 -7.*

and what instructions are applicable and who is allowed to give instructions."[70] According to the joint opinion, it is necessary to distinguish between different processing activities in the contract.[71] In a complex contract with several parties and/or several purposes, it should be clear which annex applies to a specific situation.[72]

Docking Clause_ This clause gives an option to any entity to become a new party to the contract as a controller or as a processor conditional upon the agreement of all the other parties.[73] The qualification and responsibility of such a new party should be explained in the Annex.[74]

GDPR Article 28(3) describes the minimum requirements of the contracts between the controller and the processor. The EDPB encourages the parties to use the same wording in the contract as in the GDPR, if a clause in the contract is inspired by a GDPR clause.[75] The contract shall determine the subject matter and duration of the processing, the nature, and purpose of

[70] *Id, at 10.*
[71] *Id.*
[72] *Id.*
[73] *Id, at 7.*
[74] *Id.*
[75] *Supra* note 6, at 7.

the processing, the type of personal data and categories of data subjects for the purpose of processing, and the obligations and rights of the controller.[76]

4.3 Controller's Instructions to the Processors[77]

The contract shall particularly instruct the processor to process the personal data only based on documented instructions from the controller including when the processor wants to transfer personal data to a third country or an international organization.[78] However, the processor can process the data if he is subjected to Union or Member State law to do so.[79] Even in this case, the processor shall notify the controller about processing unless the law bars disclosing.[80] The EDPB also encourages the parties to further specify the data controller's instructions in the contract by making a reference to the relevant appendices.[81] Additional instructions can also be given by the data controller throughout the duration of the contract and such instructions have to be documented, as well.[82] The parties should further

[76] GDPR Article 28(3).
[77] UDKAST, Standard Contractual Clauses, for the purpose of Article 28(3) OF Regulation 2016/679 (the GDPR) between the data controller and the data processor, page 5, https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf.
[78] GDPR Article 28(3)(a).
[79] *Id.*
[80] *Id.*
[81] *Supra* note 6, at 7.
[82] *Id.*

anticipate and consider consequences that may arise from any potentially unlawful instructions given by the data controller and provide instructions about this in the contracts between the parties.[83]

4.4 Processor's Duty of Confidence

It is the responsibility of the data processor to make sure that authorized persons to process the personal data "have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality".[84] The processor shall keep the status of authorized persons under its periodic review and access to personal data on behalf of the data controller has to be provided on a "need-to-know" basis.[85] Furthermore, GDPR Article 5 sets forth the principle of integrity and confidentiality. Based on this principle, personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".[86]

---

[83] *Id.*
[84] GDPR Article 28(3)(b).
[85] *Supra* note 6, at 7.
[86] GDPR Article 5(1)(f).

MoneyMan.pl case_ In this case, the controller, MoneyMan is the owner of a lending platform.[87] Before the data breach happened, one of the company's cyber security specialists notified the company that clients' data was publicly available on one of its servers.[88] However, the controller did not take the notification seriously and did not respond to the signal adequately.[89] Therefore, a few days after the notification, an unauthorized person stole the data and then deleted it from the server. [90]The person also asked for money to return the stolen information.[91] After that, MoneyMan started examining its security system and notified the data breach to the SA.[92]

The inadequate action led the company to lose the data. "Therefore, the President of the Personal Data Protection Office (UODO) found that the company had not implemented appropriate technical and organizational measures, which resulted in a loss of confidentiality of the personal data principle and imposed an administrative fine on the company in the

[87] European Data Protection Board, Polish DPA & ID Finance Poland: Checking potential system vulnerabilities cannot be delayed (2021), https://edpb.europa.eu/news/national-news/2021/polish-dpa-id-finance-poland-checking-potential-system-vulnerabilities_en.
[88] *Id*.
[89] *Id*.
[90] *Id*.
[91] *Id*.
[92] *Id*.

amount of over PLN 1 million (EUR 250,000)."[93] UODO further established that the controller did not take sufficient action to immediately notify the processor with information about a potential vulnerability in the server's security.[94] The controller shall also oblige the processor to deal with the case properly.

If the controller had taken adequate and immediate action to the notification, the data breach would not have happened. According to the Personal Data Protection Office, "the controller should maintain the ability to identify any breaches quickly and effectively in order to be able to take appropriate action. Moreover, the controller should be able to quickly investigate the incident in terms of whether there has been a data breach and take appropriate remedial action."[95] The SA also found that a critical element of technical and organizational measures is that the controller shall be able to detect, address, and notify data breaches.[96]

In determining the amount of the fine, the UODO considered the factors such as the scope of the breach, the controller's delay in taking preventive measures, and the scope of the stolen data. Therefore, the loss of the

[93] *Id*.
[94] *Id*.
[95] *Id*.
[96] *Id*.

confidentiality of personal data due to the controller's negligence is expensive. In this case, since unencrypted passwords have also leaked, it is possible to use this data to log in to different customer accounts, if they used the same login (e.g., e-mail) and password on other websites. Thus, unencrypted data was another factor to impose a higher fine on the controller.

4.5 The Controller and the Processor Shall Take Appropriate Security Measures[97]

The controller and the processor shall take all required steps to fulfill obligations under GDPR Art 32 regarding the security of processing.[98] They shall take appropriate technical and organizational security measures which are appropriate to the level of risk.[99] The EDPB encourages the parties to use the specific wording "taking into account the state of art" as it is indicated in art 32 to make sure that the level of security applied to the processing of personal data is always in line with the latest technological evolutions.[100]

[97] *Supra* note 60, at 5.
[98] GDPR Article 28(3)(c).
[99] GDPR Article 32(1).
[100] *Supra* note 6, at 8.

EDPB and EDPS in their joint opinion believe that the controller particularly should assess the security risks "in consideration of the purpose of the processing set by the controller."[101]For example, in cases when the processor is only for hosting data, he is not aware of the exact purpose of the processing and it is initially the controller's duty to assess the security risks and provide all useful information to the processor to comply with security measures.[102]

In 2020, the French data protection authority (CNIL) fined EUR 150,000 against a controller and EUR 75,000 against his subcontractor regarding their respective liability for not taking appropriate security measures against credential stuffing attacks on the website of the data controller and making accessible the data of approximately 40,000 website customers to unauthorized third parties.[103] In this attack, the controller has a website on which millions of customers do shopping. The controller assigned a subcontractor to manage the website.[104] An attacker obtained a list of users

[101] *Supra* note 12, at 8.
[102] *Id*.
[103] CNIL (French administrative regulatory body, National Commission on Informatics and Liberty), "Credential stuffing": the CNIL sanctions a data controller and his subcontractor (2021), https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant. To read more about credential stuffing attack on a website and doing appropriate measures in case of attack go to: https://www.cnil.fr/fr/la-violation-du-trimestre-attaque-par-credential-stuffing-sur-un-site-web.
[104] *Id*.

and their personal data including passwords, last names, first names, email addresses, date of birth of customers, number and balance of their loyalty card, and information related to their orders.[105]

The restricted committee of the CNIL decided that the two companies did not effectively do their duties to protect the security of customers' personal data, according to article 32 of the GDPR.[106] In fact, these companies received several notifications regarding data breaches on their website, however, "they had decided to focus their response strategy on developing a tool to detect and block attacks launched from robots"[107]. As it took a year from the first attack for the companies to develop the security tool, CNIL, the restricted committee considered that the companies did not take appropriate measures to effectively fight against the repeated attacks.[108] The committee believed that the companies in the meantime should have taken faster measures such as limiting the number of requests allowed per IP address on the website to prevent further attacks.[109] CNIL stressed that the controller had to give documented instructions to its subcontractor in order

[105] *Id*.
[106] *Id*.
[107] *Id*.
[108] *Id*.
[109] *Id*.

to implement security measures.[110] In addition, the subcontractor must take the most appropriate technical and organizational solutions and offer them to the controller to guarantee the protection of customers' personal data.[111]

4.6 Processors' Obligations in Using Sub-Processors[112]

The processor shall ensure the conditions in GDPR Art. 28, subsection 2 and 4, regarding choosing another processor (sub-processor) to assist in the processing of personal data for the controller.[113] A processor cannot receive assistance from another processor (meaning sub-processor) "without prior specific or general written authorization of the controller."[114] If a processor wants to use controller's general authorization, "the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes."[115]

The EDPB recommends the parties add the list of sub-processors which are accepted by the data controller at the time of the signature of the contract.[116]

---

[110] *Id*.
[111] *Id*.
[112] *Supra* note 60, at 6.
[113] GDPR Article 28(3)(d).
[114] GDPR Article 28(2).
[115] *Id*.
[116] *Supra* note 6, at 9.

The list should be included as an appendix and should be based on a general or specific authorization.[117] The processor shall ensure that even in cases of general authorization, the data controller remains informed about the list of sub-processors as well as further changes.[118]

4.7 Processors Shall Assist Controllers in Ensuring the Compliance

According to the GDPR Article 28 subsection 3 part f, the processor shall "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".[119] The parties should specify in a separate appendix the minimum level of security and measures that should be implemented by the data processor.[120] The details on assistance to the data controller with regard to the security of the processing should also be included in the instructions under the appendix.[121]

The controller has also some obligations to reply to data subjects' requests regarding their rights which are in GDPR, Chapter III. Accordingly, the processor shall give commitments in the contract to assist the controller

[117] *Id*.
[118] *Id*.
[119] GDPR Article 28(3)(f).
[120] *Supra* note 6, at 12.
[121] *Id*.

with this regard through suitable technical and organizational measures.[122] The contract has to provide details on the list of possible rights to be exercised and on the manner in which the processor must provide assistance.[123]

The contract should further set out the steps to be taken by the data processor when directly receiving a request from a data subject relating to the exercise of his/her rights.[124] For example, it has to be clear in the contract that the data processor is not allowed to have any contact with the data subjects, and how the processor needs to inform the controller when it comes to data subjects' rights.[125] Under another scenario, "the data controller instructs the data processor to answer the data subject's requests according to instructions given. Another option could be that the data processor would make the technical implementations instructed by the data controller with respect to data subject rights."[126]

[122] GDPR Article 28(3)(e).
[123] *Supra* note 6, at 11.
[124] *Id*.
[125] *Id*.
[126] *Id*.

4.8 Processors Without Undue Delay Shall Notify Controllers in Case of Personal Data Breach

"In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach."[127] It is the data controller's responsibility to assess whether or not the data breach has to be notified to the competent SA.[128] Therefore, the contract shall emphasize that the processor has to notify any personal data breach to the data controller.[129] "The data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority."[130] The parties in a separate appendix have to "define all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority."[131]

[127] *Supra* note 60, at 9.
[128] *Supra* note 6, at 13.
[129] *Id*.
[130] *Supra* note 60, at 9.
[131] *Id.*

4.9 Third-Party Beneficiary Right for Data Subject

the contract should provide individuals with the right to enforce third-party beneficiary rights under BCRs, SCCs, and any standard clauses adopted by a SA and approved by the Commission.

4.10 End-of-Contract Provisions

At the end of the processing services, the processor shall delete or return all the personal data to the controller at the choice of the controller.[132] The processor can only keep the existing copies of the personal data if Union or Member State law requires it to do so.[133]

4.11 Audit and Inspection Requirements

The data processor shall provide all the necessary information to assist the controller (or another auditor mandated by the controller) for the purpose of demonstrating his compliance obligations regarding audits and inspection provisions.[134] If in the processor's opinion, the controller's instructions are against GDPR or other Union or Member State data

[132] GDPR Article 28(3)(g).
[133] *Id*.
[134] GDPR Article 28(3)(h).

protection provisions, the processor shall immediately inform the controller.[135]

4.12 GDPR v. CPRA: Contract Accountability

Similar to the GDPR, the CPRA also obligates businesses to enter into a contract with contractors, subcontractors, third parties, and service providers. CPRA provides the contract requirements between businesses and contractors in section 1798.140 (j)(1) and 1798.100 (d).

More specifically, according to the CPRA section 1798.140 (j)(1), the contract shall prohibit the contractor from selling and sharing personal information.[136] The contract shall also prohibit the contractor from retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract or as otherwise permitted by CPRA.[137] Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business shall be prohibited in the contract.[138] The contractor shall also be prohibited from combining the personal

[135] GDPR Article 28(3).
[136] CPRA 1798.140 (j)(1)(A)(i).
[137] CPRA 1798.140 (j)(1)(A)(ii).
[138] CPRA 1798.140 (j)(1)(A)(iii).

information that the contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons or collects from its own interaction with the consumer.[139] However, service providers and contractors may combine consumers' personal information obtained from different sources consistent with consumers' expectations, and further define the business purposes, except as provided for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.[140]

The contract shall include a certification made by the contractor that the contractor understands the restrictions mentioned in the previous paragraph and will comply with them.[141] The contract shall also permit the business to monitor the contractor's compliance with the contract through measures.[142] This entails ongoing manual reviews, automated scans, regular assessments, audits, or another technical and operational testing at least once every 12 months.[143] Moreover, the contractor shall notify the business if the contractor engages any other subcontractor to assist it in processing personal information on behalf of the business, or if any subcontractor

[139] CPRA 1798.140 (j)(1)(A)(iv).
[140] CPRA 1798.185 (a)(10).
[141] CPRA 1798.140 (j)(1)(B).
[142] CPRA 1798.140 (j)(1)(C).
[143] *Id*.

engages another subcontractor to assist in processing personal information. And all the engagements shall be pursuant to a written contract binding subcontractors to observe all the requirements set forth in the contract between the business and the contractor.[144]

According to the CPRA 1798.100 (d), businesses shall enter into an agreement with third parties, service providers, or contractors. They should specify in the contracts that the personal information is sold or disclosed by the business only for limited and specified purposes.[145] The business shall obligate the third party, service provider, or contractor to comply with applicable obligations under CPRA and provide the same level of privacy protection as is required by CPRA.[146] The third party, service provider, or contractor shall also grant the business rights to take reasonable and appropriate steps to help ensure that the personal information is transferred in a manner consistent with the business's obligations under CPRA.[147] It also requires the third party, service provider, or contractor to notify the business if it determines that it can no longer meet its obligations under CPRA.[148] The contractor shall also grant the business the right, upon notice

[144] CPRA 1798.140 (j)(2).
[145] CPRA 1798.100 (d)(1).
[146] CPRA 1798.100 (d)(2).
[147] CPRA 1798.100 (d)(3).
[148] CPRA 1798.100 (d)(4).

to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.[149]

5. Processors' Responsibilities and Liabilities

A processor shall gather, process, or use personal data in accordance with the instructions of the controller based on a contract.[150] In a GDPR controller-processor relationship, the processor or any person acting under the authority of the processor who has access to personal data is only permitted to process personal data based on the documented instructions from the controller.[151] The only exception is when a processor is "required to do so by Union or Member state law."[152] To fulfill its obligations, a processor shall obtain the prior specific or general written authorization of the respective controller in order to involve another processor (sub-processor). Even in case of general authorization, the processor must inform the controller about any relevant changes regarding the processing.[153]

---

[149] CPRA 1798.100 (d)(5).
[150] *Supra* note 5.
[151] GDPR Article 29 and *supra* note 5.
[152] *Id*.
[153] *Supra* note 5.

5.1 Processors' Direct Responsibility for Data Damages

A processor is liable for the damage caused by processing only when it has not complied with obligations of this Regulation specifically directed to processors or when it has conducted outside or against lawful instructions of the controller.[154] According to the GDPR, the controller determines the purposes and means of the processing. If a processor infringes the regulation and determines the purposes and means of processing, he will be considered as a controller in respect of that processing.[155]

6. Contracts between Processors and Sub-Processors

As it is mentioned before, the processor cannot receive assistance from another processor meaning the sub-processor without the prior specific or general written authorization of the controller.[156] If the processor wants to choose another processor for processing personal data on behalf of the controller, there has to be a written contract or other legal act between the processor and sub-processor that reflects the same data protection obligations which are in the contract between the controller and processor.

[154] GDPR Article 82(2).
[155] GDPR Article 28(10).
[156] GDPR Article 28(2).

[157] "The whole chain of processing activities needs to be regulated by written agreements."[158]"It is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same."[159] "The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process that data except on instructions from the controller, unless required to do so by Union or Member State law."[160]

6.1 Third-Party Beneficiary Right for the Data Controller

In the agreement between processor and sub-processor there should be a clause about third party beneficiary rights for the data controller. The controller shall have the right to enforce the agreement against the sub-processor in the events such as processor bankruptcy. The right enables the controller to instruct the sub-processor to delete, return or process based on the controller's instructions.[161]

[157] GDPR Article 28(4).
[158] *Supra* note 1, at 40.
[159] *Id.*
[160] GDPR Article 29.
[161] *Supra* note 60, at 6.

6.2 Non-Compliance Consequences

The initial processor will remain completely liable to the controller, if the sub-processor fails to comply with its data protection obligations.[162]

7. Damages

According to the GDPR Recital 146, "The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation."[163] The kind of damage that data subject can claim could be material or non-material.[164]Moreover, the recital has broadly interpreted the concept of damage in the light of the case-law of the Court of Justice to fully reflect the objectives of the GDPR.[165]

EDPB and individual data protection authorities (DPAs) located in 27 EU member states enforce the GDPR. GDPR enforcement bodies are independent of the government, and they investigate complaints, provide advice on data protection issues, and determine when the GDPR has been breached. Under GDPR, non-compliance and data breaches can result in

[162] GDPR Article 28(4).
[163] GDPR Recital 146.
[164] GDPR Article 82(1).
[165] GDPR Recital 146.

fines as high as 20 million euros or 4% of the violating company's annual global turnover, whichever amount is higher.

Compared with the GDPR, the CCPA is enforced by the California Office of the Attorney General (OAG). The Attorney General's office is responsible for deciding about appropriate fines and penalties for entities in violation of CCPA. The CPRA created an entirely new authority responsible for enforcing the privacy law. The CPRA will be enforced by the California Privacy Protection Agency (CPPA), which has investigative and enforcement powers. The Attorney General also retains civil enforcement authority.

The CCPA and CPRA only impose penalties after a breach occurs. As such, non-compliance does not result in fine. The penalties involved under CCPA are $2,500 for violations, $7,500 for intentional violations and $100 - $750 in damages in civil courts. CPRA adds additional $7,500 fine if consumer privacy rights of a minor are violated. Also, businesses can avoid the fines if they address and rectify the issues within a 30-day period after being notified by the Attorney General.

7.1 Factors in Determining the Amount of Fine

When deciding on the amount of the administrative fine, GDPR authorities have considered several factors including the nature, seriousness, and duration of the infringement; the negligent character of the infringement; the degree of responsibility of the controller taking into account technical and organizational measures implemented to comply with the GDPR; the benefits gained from the infringement; the categories of personal data affected by the infringement; the relationship between the company's activity and the processing of personal data; and the fact that the company is a large enterprise and its turnover.[166] In addition to the administrative fine, GDPR authorities also ask data violators to bring their processing operations into compliance with the GDPR to prevent similar breaches in the future.[167]

[166] European Data Protection Board, News, Spanish Data Protection Authority (AEPD)imposes fine of 6.000.000 EUR on CAIXABANK, S.A. (2021), https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank_en.
[167] *Id*.

7.1.1 The Controller's Size and the Relationship Between the Data Subject and the Controller

CAIXABANK Case_ For instance, in this case, Spanish Data Protection Authority (AEPD) imposes a fine of 6.000.000 EUR. In determining the amount of fine, AEPD considers the scope of violations, the relationship between the data subject and CAIXABANK as well as other factors such as the company's size.

7.1.2 Controller's Inadequate Response to the Data Breach

ID Finance Poland case, Owner of MoneyMan.pl _Similarly, in this case, the Polish data protection authority, the President of the Personal Data Protection Office (UODO) considered the scale of the breach and the scope of the stolen data in determining the amount of fine.[168] In this case, the data subject's unencrypted passwords have also leaked. As a result, it is possible to use the stolen data to log in to different customer accounts, if they used the same username and password on other websites. In establishing the amount of the fine, UODO also considered the controller's delay in taking

[168] European Data Protection Board, News, Polish DPA & ID Finance Poland: checking potential system vulnerabilities cannot be delayed, https://edpb.europa.eu/news/national-news/2021/polish-dpa-id-finance-poland-checking-potential-system-vulnerabilities_en.

preventive measures.[169] "The punished company (owner of a lending platform MoneyMan.pl) did not respond adequately to the signal about gaps in its security. It did not check quickly enough the information that its client's data was available on one of its servers."[170]

7.1.3 Controller's Inadequate Cooperation with Data Protection Authorities

Foodinho Case, a subsidiary of GlovoApp23_ The company was fined EUR 2.6 million by the Italian SA (GARANTE).[171] In calculating the amount of the fine, the Italian SA also considered "the poor cooperation provided by the company during the inquiries as well as the considerable number of the riders concerned in Italy".[172] Therefore, EUR 19,000 of the fine is related to the unsatisfactory cooperation between the controller, Foodinho and the data protection authority.[173]

---

[169] *Id*.
[170] *Id*.
[171] European Data Protection Board, News, RIDERS; ITALIAN SA SAYS NO TO ALGORITHMS CAUSING DISCRIMINATION A platform in the Glovo group fined EUR 2.6 million (2021), https://edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en.
[172] *Id*.
[173] *Id*.

7.1.4 Controller's Insufficient Risk Assessment and the Number of Data Subjects Affected

Norwegian Confederation of Sport Case_ The Norwegian DPA fined the Norwegian Confederation of Sport (NCOS) EUR 125,000 because of making available online the personal data of 3.2 million Norwegian for 87 days.[174] The GDPR violation was a result of an error related to the testing of a cloud computing solution.[175] In determining the amount of fine, DPA considers the large quantity of personal data that was involved and NOCS was not able to establish satisfactory security measures for the testing.[176] Moreover, the Data Protection Authority mentioned that "It is very important to thoroughly test any solution before it is put into production".[177] He also recommends the controllers use fictitious data in the testing process to mitigate the security risks considerably.[178]

[174] European Data Protection Board, News, Norwegian DPA: Norwegian Confederation of Sport fined for inadequate testing (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-norwegian-confederation-sport-fined-inadequate-testing_en.
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *Id.*

7.1.5 Private Information and Sensitive Data

BRAbank ASA, formerly Easybank ASA Case_ This case involves insufficient risk assessment concerning a customer portal for banking services.[179] "My Page" is a customer platform where BRAbank customers can view information about their loan agreements.[180] As a result of technical errors, the bank customers could get access to the loan, address and contact information of other customers upon launching their personal "My Page" account.[181] Norwegian Data Protection Authority (DPA) concluded that the bank, as a controller, did not meet GDPR requirements regarding risk assessment and appropriate technical measures in connection with the customer portal. GDPR requires the data controller to conduct a risk assessment and apply technical measures, such as testing, to protect the data subject's personal data.[182] In this case, DPA considers the private nature of the customer's financial data as an aggravating factor in determining the amount of fine imposed on the controller, BRAbank ASA.[183] DPA also mentioned that unlike information about income,

[179] European Data Protection Board, News, Norwegian DPA: BRAbank ASA fined (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-brabank-asa-fined_en.
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*

financial information related to the loans and refinancing are not publicly available information and the private nature of the information make the data breach more serious.[184]

Municipality of Oslo Case_ in a similar case, the Norwegian Data Protection Authority fined the Municipality of Oslo EUR 40,000 for making public sensitive personal data including health information and employee's personal life.[185]

7.1.6 Overall Assessment of the Case

Moss Municipal Council Case_ In this case, the municipalities of Rygge and Moss combined

IT systems for various municipal service areas.[186] The administrative system combined the personal information related to the employees with the health data related to the children and young people.[187] Patient data was made accessible to healthcare personnel who did not have a professional need to access the data. The data protection error violated the principles of

[184] *Id.*
[185] European Data Protection Board, News, Norwegian DPA: Municipality of Oslo fined (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-municipality-oslo-fined_en.
[186] European Data Protection Board, News, Norwegian DPA: Moss Municipal Council fined (20221), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-moss-municipal-council-fined_en.
[187] *Id.*

confidentiality, integrity, and accessibility.[188] As a result of the breach, 2,000 people could have been affected; however, no specific individuals have actually been impacted.[189] Even if the data protection error was quickly corrected and under control, the Norwegian Data Protection Authority decided to impose a EUR 50,000 fine based on an overall assessment of the case.[190] This case is an example that even if there was not any actual damage, however, DPA decided to fine the controller based on the overall assessment of the case and data protection violations.

7.2 The Allocation of Responsibilities to Pay Damages

7.2.1 Joint Responsibility Principle

To ensure effective compensation of the data subject, there is a **jointly and severally liability principle** in the GDPR. When a data subject is damaged by two or more controllers' or processors' processing acts, each data processing actor is "jointly and severally liable" for the damage caused to the data subject. This means that the data subject may recover the entire

[188] *Id.*
[189] *Id.*
[190] *Id.*

damage from any controller or processor who is involved in the same processing causing the damage. [191]

However, the joint responsibility does not necessarily indicate equal responsibility of the various processors and controllers involved in the processing of personal data.[192] On the contrary, the Court of Justice of the European Union ("CJEU") has clarified that data processing actors may be involved at different levels of the processing.[193] Therefore, the level of responsibility of each actor must be assessed based on the relevant circumstances of each particular case.[194]

7.2.2 Comparative Contribution Principle

When a controller or processor has paid full compensation for the damage, that controller or processor is entitled to claim back from the other controllers or processors involved in the same processing. In fact, contribution enables any controller or processor who is required to pay more than his share of damage to a data subject to claim back the excess in

[191] GDPR Article 82(4).
[192] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0 (2020), page 18, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.
[193] *Id.*
[194] *Id.*

a claim against the other data processing actors.[195] However, the open question is if the data processing actors are international companies that have different entities in different countries whether the whole entity is jointly and severally liable for the damage, or just the specific legal entity that caused the infringement is responsible. This is a critical question as it potentially limits the data subject's compensation.[196]

GDPR follows the comparative contribution principle in case of damage caused by different data processing actors based on which "compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured."[197]

7.2.3 Indemnity As a Means of Liability Exemption

The controller and the processor both can exculpate themselves from liabilities. However, they must prove that they were not in any way

[195] GDPR Article 82(5).
[196] DLA PIPER, GDPR: DLA Piper GDPR Fines and Data Breach Survey: 2021, https://www.dlapiper.com/en/uk/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/.
[197] GDPR Recital 146.

responsible for the event causing the damages.[198] Indemnity shifts the entire loss to other data processing actors involved in the same processing.

Contract-based_ controllers and processors may agree in a contract that each party agrees to indemnify another against the consequences of his own negligence.

Vicarious liability_ Indemnity may arise when there is a vicarious relationship between the parties. For example, a processor may seek indemnity for the acts of a sub-processor.

8. Conclusion

The concepts of controller, joint controller, and processor play an important role in the function of the GDPR. The controller determines the purposes and means of processing and will be responsible and liable for any personal data processing conducted on its behalf.[199] The processor is only permitted to process personal data based on the controller's documented instructions.[200] However, this doesn't mean that the processor doesn't have

[198] GDPR Article 82(3), GDPR Recital 146, *supra* note 5.
[199] GDPR Recital 74.
[200] *Id.*

liability. He is jointly liable with the controller and his liability is limited to violations of obligations that are specific to him.[201]

GDPR enforcement mechanism is mainly based on stopping the data breach through legal remedies such as injunctions and imposing fines. When deciding on the amount of the administrative fine, GDPR authorities have considered several factors so far including the nature, seriousness, and duration of the infringement; the negligent character of the infringement; the degree of responsibility of the controller taking into account technical and organizational measures implemented to comply with the GDPR; the benefits gained from the infringement; the categories of personal data affected by the infringement; the relationship between the company's activity and the processing of personal data; and the fact that the company is a large enterprise and its turnover.[202]

Injunctions aim to stop data breaches and prevent controllers and processors from running their businesses unless they correct the violation. Moreover, stopping data infringement may cause controllers from

[201] GDPR Article 28(2).
[202] *Supra* note 148.

functioning. Therefore, it makes compliance measures and appropriate data protection safeguards critical for conducting businesses

CHAPTER 4: INTERNATIONAL ARRANGEMENTS BETWEEN CONTROLLERS AND PROCESSORS TO TRANSFER EUROPEAN UNION PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (THIRD COUNTRIES)

1. Introduction

GDPR requires the controllers and the processors to comply with further requirements if they want to transfer personal data to third countries meaning outside the EEA for.[1] Not only the data transfer itself should be within the definition of data processing and has to meet one of the legal bases mentioned in GDPR article 6 for being lawful, but also the transfer to the third country should also be permitted under GDPR.[2] GDPR chapter V specifies mechanisms to permit transfer of personal data to a third country or an international organization. The purpose of chapter V is to prevent undermining the level of protection provided for EEA personal data when the personal data is transferred to third countries or international organizations.

[1] GDPR Article 44.
[2] GDPR Key Issues, Third Countries, https://gdpr-info.eu/issues/third-countries/.

Chapter three of this research evaluates the type of contracts between controllers and data subjects in which processing does not require transferring personal data to third countries or international organizations. The international aspect of the targeted contracts in chapter three is because the EU consists of 27 countries and GDPR governs all of them. Therefore, even if personal data actors do not transfer data to third countries they are still involved in international arrangements. For instance, when the parties of a data protection contract are from Germany and France, they are from different countries within the EU area and consequently, the contract between them still has international aspects.

Chapter four examines the additional legal arrangements when the controllers or the processors want to transfer the data to non-EEA. This chapter discusses GDPR appropriate safeguards for transferring personal data to third countries, outside the EEA.

2. Criteria to Qualify a Processing as a Transfer of Personal Data to a Third Country or to an International Organization

This section intends to clarify if a personal data processing establishes a transfer to a third country or an international organization and the data actors must consequently comply with the specified conditions provided in

the GDPR chapter V. It is essential to notice that "regardless of whether the processing takes place in the EU or not, controllers and processors always have to comply with all relevant provisions of the GDPR".[3] The EDPB has recognized the following criteria that fulfill the definition of a transfer to a third country or an international organization. If all three criteria are met, then there is a transfer to a third country or to an international organization in accordance with the GDPR Chapter V.[4] Consequently, the data exporter[5] needs to comply with the specified conditions mentioned in chapter V to transfer data to the data importer[6].

2.1. The Data Exporter is Subject to the GDPR for Processing Data (Data Transfer)

The first criterion requires that the data exporter, a controller or processor, is subject to the GDPR for the given transferring, data processing.[7] All companies which process the personal data of individuals residing in the

[3] European Data Protection Board (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 (2021); https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en.
[4] *Id, at 9.*
[5] Data exporter is the controller or processor transferring the personal data to a third country.
[6] Data importer is the controller or processor receiving the personal data.
[7] *Supra* note 3, at 5.

EU are subject to the GDPR.[8] From the GDPR point of view, it does not matter that the company's location is not in the EU if the company processes the personal data of data subjects in the EU.[9] In addition, the regulation applies to the processing of personal data by controllers and processors in the EU even if the processing itself is not in the EU.[10]

Establishment Clause _ Pursuant to the GDPR Article 3 subsection 1, "processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union"[11] is subject to the GDPR and this is regardless of whether the processing is carried out in the Union or not.[12] This section has important elements that should be noticed when analyzing a case to see if it is subject to the GDPR territorial scope or not. These elements include controller and processor definition, establishment definition, personal data processing in the context of the activities of an establishment and considering the establishment of a controller or a processor separately. This article is also regardless of whether the processing takes place in the EU or not.

---

[8] GDPR Article 3 and European Commission, Who does the data protection law apply to?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en.
[9] *Id.*
[10] *Id*.
[11] GDPR Article 3(1).
[12] *Id*.

Controller and processor definitions are important and the first elements to determine if an entity's personal data processing would be subject to the GDPR. According to the GDPR article 4(7), the controller is defined as "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."[13] Also, GDPR article 4 subsection 8 defines a processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[14] Thus, the processor and controller could be individuals or legal entities, and a processor processes personal data on behalf of a controller. As such, it is possible that a company to be a controller or processor at the same time. It is also possible that a processor is a processor for different controllers, and it depends on the processing activities taken on behalf of which entity or individual.

Establishment definition _ Another important element in analyzing GDPR Article 3 subsection 1 is the establishment definition. GDPR Recital 22 states that an establishment "implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not

[13] GDPR Article 4(7).
[14] GDPR Article 4(8).

the determining factor in that respect."[15] The determining factors in this definition are the effective and real exercise of activities, as well as stable arrangements. Recital 22 specifies that having branches or subsidiaries in the EU is not determining factor in defining stable arrangements. Therefore, even if an entity does not have a branch or subsidiary in the EU, it could still be considered to have a stable arrangement in the EU.

Additionally, personal data processing of an established entity in the EU should be in the context of the activities of the company's establishment in the EU.[16] Therefore, it is important to find a link between the activity and the establishment. For example, when a company with a headquarter in the US has a branch in France to supervise its business in Europe, the branch can be considered as a stable arrangement, which exercises real and effective activities within the meaning of the GDPR. In addition, the France branch could also be considered as a stable establishment in the EU. Even if the company has a stable representative in the EU who acts within a sufficient degree of stability, that could also be within the GDPR definition of stable arrangement.

[15] GDPR Recital 22.
[16] GDPR Article 3(1).

The place of processing _ GDPR applies to the establishment of a controller or a processor in the union, regardless of whether the processing takes place in the Union or not. Therefore, the place of processing is not a factor in determining if personal data processing in the context of the activities of the establishment in the EU is within the GDPR territorial scope. Therefore, based on the facts in the previous example, if personal data processing is in the context of the activities of the France branch and the processing activities are in the U.S., GDPR still applies to such processing in the U.S.

Processing of personal data carried out in the context of the activities of an establishment_ *A*rticle 3 subsection 1 of the GDPR provides that the regulation applies to the personal data processing in the context of the activities of an establishment of a controller or a processor in the EU. It is not necessary that the processing is done by the relevant EU establishment itself.[17] When the personal data is processed in the context of the activities of its relevant establishment in the EU, it is enough to make the controller or the processor subject to the GDPR.[18] EDPB recommends that raising

[17] European Data Protection Board (edpb), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1 (2019), page 7, edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.
[18] *Id.*

revenue in the EU by a local establishment can be indicative of processing carried out in the context of the activities of the EU establishment.[19]

Moreover, in considering the establishment activities we should consider both controller and processor establishment in the EU. As GDPR used the word "or", it does not matter that one of the controllers or processors does have establishment in the union or not. For instance, a processor has a stable arrangement such as a representative or agent in the EU and processes personal data in the context of the activities of that arrangement on behalf of a controller that does not have any establishment in the EU and is not subject to other GDPR's provisions. In this case, the data processor is subject to the GDPR and is required to comply with the processor obligations even if the data controller is not required.

Targeting Clause _ GDPR article 3 subsection 2 defines another criterion for its territorial scope. It provides that:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

[19] *Id, at 8.*

a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
b. the monitoring of their behaviour as far as their behaviour takes place within the Union.[20]

The determining factors of the targeting clause include personal data processing of data subjects who are in the Union, a controller or processor not established in the EU, offering goods or services, irrespective of whether a payment of the data subject is required to data subjects located in the EU, and monitoring of data subject's behavior as far as the behavior itself takes place within the EU. Firstly, it is important to notice that the application of the targeting clause is for processing personal data of data subjects who are in the EU. This means that the data processing of a data subject who is not in the EU is not subject to this clause. This requirement must be assessed when the related activity takes place. For example, it could be at the moment of offering of goods or services or at the moment of monitoring the behavior.[21]

Secondly, the targeting clause is not limited to residency or citizenship.[22] It is applicable to data processing of data subjects who are in the EU regardless of their citizenship or residency. As it is clarified in the GDPR

[20] GDPR Article 3(2).
[21] *Supra* note 17, at 15.
[22] *Id, at 14.*

recital 14, "the protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data."[23]

The targeting clause is specifically for a controller or processor that is not established in the EU, but they are offering goods or services or monitoring data subjects' behavior within the EU.[24] As it is mentioned in the GDPR Article 3 subsection 2, offering goods or services is irrespective of whether a payment of the data subject is required. Therefore, a company established in the U.S. that has no stable arrangement in the EU and provides application services targeting people present in the EU is subject to the GDPR regardless of receiving money for the services that it provides.[25]

To sum up, the targeting clause has three key elements that should be satisfied to require an entity to comply with the GDPR. First, the controller or processor is not established in the EU. Second, there should be processing personal data of an individual in the EU by the processor or controller. Third, targeting individuals in the EU either by offering goods or services to them or by monitoring their behavior in the Union. Therefore,

[23] GDPR Recital 14.
[24] *Supra* note 21.
[25] *Id.*

when a U.S. citizen is in the EU for his holiday and uses an application that is exclusively for the U.S. market, the processing of his personal data by the U.S. company is not subject to the GDPR because the U.S. company does not target individuals in the EU.[26] Moreover, processing personal data of EU citizens or residents who are not in the EU as long as the processing is not targeting EU individuals is not subject to the GDPR.[27] For example, some EU citizens live in China and use a Chinese bank's application with regard to their accounts in China and the Chinese bank is not active in the EU market. In this case, the Chinese bank's processing of the personal data of EU citizens is not subject to the GDPR because it does not directly target EU citizens.[28]

2.2. The Data Exporter Discloses Personal Data to the Data Importer

The second criterion requires a data exporter, which could be a controller or processor, to disclose personal data by transmission or making available otherwise to another controller or processor, meaning the data importer.[29] It is worth noticing that in a scenario when the data subject disclosed his or her data to the recipient, there is no controller or processor (exporter) which

[26] *Supra* note 17, at 16.
[27] *Id*.
[28] *Id*.
[29] *Supra* note 3.

makes the data available to the importer.[30] Therefore, the second criterion should not be considered fulfilled in this case and there is no data transfer to a third country.[31] For example, the data subject, Maria is living in Europe and she enters her personal data on a controller's website in order to do her online shopping.[32] The controller is established in Singapore with no presence in the EU.[33] This case doesn't include the transfer of personal data since the data is not disclosed by an exporter (controller or processor) but by the direct action of the data subject.[34] Therefore, this case is not subject to the GDPR Chapter V. Nonetheless, the Singaporean controller needs to check if its data processing is subject to the GDPR article 3(2).[35]

A data transfer may be done by a controller or processor. Therefore, there may be a transition when a controller discloses data to a processor, or a processor transfers data to another processor or even to a controller as instructed by its controller.[36] The concept of transfer of personal data in the second criterion only applies when the disclosure of personal data is between two separate parties.[37] There must be a data exporter disclosing

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id, at 6.*
[37] *Id.*

data to a different controller or processor as the data importer.[38] Thus, if the data exporter and importer are not different controllers or processors, the transfer of data is not considered as a transfer subject to the GDPR chapter V. However, according to the GDPR article 32, the data actors are obliged to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.[39]

It is essential to mention that data actors which are "part of the same corporate group may qualify as separate controllers or processors. Consequently, data disclosures between entities belonging to the same corporate group (intra-group data disclosures) may constitute transfers of personal data."[40] For example, the Irish Company A is a subsidiary of the U.S. parent Company B. Company A discloses the personal data of its employees to Company B in order to be stored in a centralized HR database by the parent company in the U.S.[41] In this case, the Irish Company A, as a controller, discloses its employees' data to the parent company as a processor which is situated in a third country.[42] Company A is subject to the GDPR pursuant to article 3(1) for this processing and Company B is situated

[38] *Id.*
[39] *Id, at 7.*
[40] *Id.*
[41] *Id.*
[42] *Id.*

in a third country.[43] "The disclosure, therefore, qualifies as a transfer to a third country within the meaning of Chapter V of the GDPR."[44]

2.3. The Importer Is in A Third Country or Is an International Organization, Irrespective of Whether This Importer Is Subject to the GDPR in Respect of The Given Processing in Accordance With Article 3

The third criterion requires the importer to be in a third country or be an international organization irrespective of whether the processing is under the GDPR territory.[45] For instance, Company A is a controller without an EU establishment and provides goods and services to the EU market.[46] The French company B processes personal data on behalf of company A and re-transfer the data to A.[47] In this case, "The processing performed by the processor B is covered by the GDPR for processor specific obligations pursuant to article 3(1), since it takes place in the context of the activities of its establishment in the EU. The processing performed by A is also covered by the GDPR since Article 3(2) applies to A."[48] Since Company A is

[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id, at 8.*
[47] *Id.*
[48] *Id.*

geographically located in a third country, therefore, the disclosure of data from B to A is considered as a transfer to a third country and Chapter V applies to the transmission.[49]

3. Transferring Personal Data to a Third Country or to an International Organization

This section elaborates on GDPR Chapter V requirements when a data processing (transfer) meets all the three criteria explained in the previous section. Chapter V mechanisms aim to protect personal data after they have been transferred to a third country or an international organization.[50]

These mechanisms include the adequacy decision specified in the GDPR article 45. In this method, the EC recognizes "the existence of an adequate level of protection in the third country or international organization to which the data is transferred"[51]. In the absence of the adequacy decision, the exporter (controller or processor) can implement appropriate safeguards as mentioned in article 46 to transfer data.[52] Moreover, article 49 explains some specific situations and certain conditions that personal data

[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*

can be transferred to a third country or an international organization even without the existence of an adequacy decision or appropriate safeguard.[53]

3.1. Transferring Data to Adequate Third Countries: Adequacy Decision

Adequacy decision is one of the GDPR methods that data actors can rely on when transferring EU personal data to third countries or an international organization outside the EEA.[54] In this method, the EC recognizes that a third country, a territory, or a specified sector within that third country or international organization can ensure an adequate level of data protection that is essentially equivalent to that within the EU.[55] The transfer based on an adequacy decision doesn't require any specific authorization.[56]Article 45 describes the factors that the EC shall consider for assessing the adequacy decision. The factors are included but not limited to the rule of law, respect for human rights, the existence and effective functioning of one or more independent SAs and the international commitments that the third country or the international organization have or has entered.[57]

---

[53] *Id.*
[54] GDPR Article 45.
[55] GDPR Article 45(1).
[56] *Id.*
[57] *Id.*

The EC after assessing the specified factors will decide and the decision will be reviewed by the EC for at least every four years to make sure that the third country or international organization still ensures an adequate level of protection within the meaning of GDPR article 45 subsection 2.[58] According to the GDPR, the EC shall publish in the Official Journal of the EU and on its website, a list of the third countries, territories and specified sectors within a third country and international organizations for which it has decided that an adequate level of protection is or is no longer ensured.[59]

3.1.1. The Adequacy Decision Between the EU and the US

In the global digital economy era, personal data transfer is one of the essential bases for the transatlantic relationship between the EU and the whole world including the US. Regarding the economic relationship between the EU and the US, the adequacy decision between the EU and the US provides a GDPR mechanism for companies on both sides of the Atlantic to comply with data protection requirements.

Safe Harbor Agreement and The Schrems I case _ In 2000, the Safe Harbor agreement between the U.S. government and the EC was closed for the

[58] GDPR Article 45(3).
[59] GDPR Article 45(8).

purpose of transferring electronic personal data from the EU to the US.[60] More than 4,000 U.S. companies signed up to the agreement in order to transfer data from the EEA to the U.S.[61] The CJEU invalidated the Safe Harbor in October 2015 as a result of its decision in case C-362/14, Maximilian Schrems v. Data Protection Commissioner.[62] In this case, known as Schrems I, ECJ concluded that the agreement doesn't provide an adequate level of protection for transferring personal data from the EU to the U.S. as required by the EU Data Protection Directive 95/46/EC, the complying EU data protection regulation at that time.[63]

Maximilian Schrems is an Austrian law student that challenged the Irish Data Protection Commissioner ("IDPC")'s decision in the Facebook case.[64] In this case, Facebook in violation of EU data protection laws was allegedly transferring information to the U.S. intelligence services.[65] However, the IDPC decided that the existence of the Safe Harbor prohibited the Irish agency from asking Facebook to stop transferring data from Ireland to the

[60] JONES DAY, EU-U.S. Data Protection Safe Harbor: Not Safe Anymore (2015), https://www.jonesday.com/en/insights/2015/10/euus-data-protection-safe-harbor-not-safe-anymore.
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*

U.S.[66] Following the opinion of the Advocate General, the ECJ decided that the Safe Harbor does not provide adequate protection to the EEA electronic data and therefore, the Safe Harbor agreement should get invalidated.[67] As a result of this decision by the ECJ, international data transfers could not be made by customers and businesses between the EU and U.S. Therefore, companies using Safe Harbor as a basis for their data transfers to the U.S. had to seek another valid base to ensure complying with EU data protection law.

***Privacy Shield and Schrems II case*[68]**_ Privacy Shield is an agreement between the EU-U.S. and Swiss-U.S. that its frameworks were established by the U.S. Department of Commerce, the EC, and Swiss Administration.[69] Privacy Shield was adopted on July 12, 2016, and its framework was enforced from August 1st, 2016.[70] The Privacy Shield allows transferring of individuals' personal data from the EU to a company in the United States.[71]

---

[66] *Id.*
[67] *Id.*
[68] European Parliament, Exchanges of Personal Data After the Schrems II Judgment (2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf.
[69] European Commission, EU-US Privacy Shield, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en.
[70] *Id.*
[71] European Commission, Guide to the EU-U.S. Privacy Shield, page 7 (2016), https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf.

However, the processing company in the U.S. is required to comply with specific data protection rules.[72]

Privacy Shield provides a mechanism for companies on both sides of the Atlantic to comply with data protection requirements.[73] The agreement's purpose is to provide a reliable mechanism for transferring data from the EU to the US while EU data subjects will benefit from EU data protection rules compliance.[74] The Department of Commerce in the U.S through this agreement aims to develop international commerce and facilitate trade and commerce between the United States and the EU.[75]

There are different ways to transfer data from the EU to the U.S. including contractual clauses, BCRs, and the Privacy Shield. Privacy Principles in the framework contain companies' obligations.[76] On the US side of the agreement, the U.S. Department of Commerce is in charge of managing and administering the privacy shield and making sure that companies fulfill their commitments.[77] If the U.S. companies want to use the privacy shield

---

[72] *Id.*
[73] Privacy Shield Framework, Privacy Shield Overview, https://www.privacyshield.gov/Program-Overview.
[74] The U.S. Department of Commerce, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE 1 (2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.
[75] *Id.*
[76] *Id*.
[77] *Id.*

to transfer data, they must first sign up for the privacy shield framework with the U.S. Department of Commerce.[78] Moreover, companies have to have a privacy policy in accordance with privacy principles, get certified with the U.S. Department of Commerce, and annually renew their membership with the privacy shield.[79] However, this situation changed in July 2020, following the decision of the CJEU in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems.[80]

In this decision, the CJEU concluded that the EC's adequacy determination for the EU-U.S. Privacy Shield Framework is invalid because of invasive US surveillance programs.[81]. Therefore, this decision has made the transfer of personal data from the EEA to the US based on the privacy shield illegal. And, "the companies that continue to transfer data on the basis of an invalid mechanism risk a penalty of €20 million or 4 % of their global turnover, pursuant to Article 83(5)(c) GDPR."[82] Moreover, according to the decision,

[78] *Id.*
[79] *Id.*
[80] International Association of Privacy Professionals, Frequently Asked Questions & Resources on "Schrems II" (2021), https://iapp.org/resources/article/frequently-asked-questions-resources-on-schrems-ii/.
[81] Hendrik Mildebrath, European Parliamentary Research Service, The CJEU judgment in the Schrems II case (2020), https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.
[82] *Id.*

data controllers or processors must comply with stricter requirements, SCCs, and "must ensure that the data subject is granted a level of protection essentially equivalent to that guaranteed by the GDPR and the EU Charter of Fundamental Rights.[83]

Pursuant to invalidating the privacy shield by the CJEU, the US Department of Commerce decided to continue to administer the Privacy Shield Framework and asked U.S. participants to comply with their obligations under the Framework. This also includes processing submissions for self-certification and recertification and maintaining the Privacy Shield List.[84] Therefore, if an organization does not comply with its Privacy Shield commitments, it could still be subject to legal action by the U.S. Federal Trade Commission.[85]

Privacy Shield II_ On March 25, 2022, the US and the EC entered into a new Trans-Atlantic Data Privacy Framework to address the concerns raised by the CJEU which invalidated EU-US privacy shield framework.[86] Based on

[83] *Id.*
[84] Privacy Shield Framework, Privacy Shield Overview, https://www.privacyshield.gov/program-overview.
[85] *Id.*
[86] FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

the framework, the US has committed to implementing new safeguards to "ensure the privacy of EU personal data and to create a new mechanism for EU individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities."[87] Accordingly, on October 7, 2022, President Biden signed an executive order to enhance safeguards for the United States Signals Intelligence Activities (E.O.).[88] The executive order outlines the steps that the US will take to implement its commitments under the new framework announced on March 25, 2022.[89]

This research in subsequent sections will examine the alternatives to the adequacy decision that are available to the companies located in inadequate countries to transfer personal data from the EEA to a non-adequate third country.[90]

---

[87] *Id.*
[88] FACT SHEET: President Biden Signs Executive Order to Implement the European Union- U.S. Data Privacy Framework (2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.
[89] *Id.*
[90] Privacy Shield Framework, Privacy Shield Overview, https://www.privacyshield.gov/program-overview.

3.2. Transferring Data to Non-Adequate Third Countries: Appropriate Safeguards

According to the GDPR article 46, in the absence of an adequacy decision for the transfer of personal data from the EU to a third country, the controller or the processor may provide appropriate safeguards to transfer data.[91] The contents of the safeguards depend on each specific situation. GDPR in subsections 2 and 3 of article 46 has enlisted the appropriate safeguards which include: a legally binding and enforceable instrument between public authorities or bodies, BCRs, SCCs adopted by the EC, SCCs adopted by a SA and approved by the EC, an approved code of conduct, and an approved certification.[92]

Moreover, subject to the authorization from the competent SA, contractual clauses between the controller or processor and the controller, processor, or the recipient of the personal data in the third country or international organization; or provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and

[91] GDPR Article 46(1).
[92] GDPR Article 46(2) and (3).

effective data subject rights could also be considered as appropriate safeguards under GDPR.[93]

3.2.1. A Legally Binding and Enforceable Instrument Between Public Authorities or Bodies

GDPR Article 46(2) and (3) discuss transferring personal data from EEA public authorities or bodies ("public bodies") to public bodies in third countries or international organizations. Public bodies may choose this mechanism or other relevant appropriate safeguard tools provided in the GDPR article 46.[94] More specifically, article 46 (2)(a) is about "a legally binding and enforceable instrument between public authorities or bodies"[95].

3.2.2. Binding Corporate Rules: Corporate Rules for Transferring Data Within Multinational Companies

BCRs is one of the appropriate safeguards that entities can use for the international transfer of personal data from the EEA. BCRs are suitable for

[93] GDPR Article 46(3).
[94] European Data Protection Board, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, Version 2.0 (2020), page 5, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf.
[95] GDPR Article 46(2)(a).

transferring data from controllers established in the EU to the other group controller or processor members outside the EU.[96] BCRs apply to enterprises involved in a joint economic activity, including their employees.[97] They are legally binding rules within multinational group companies to internally transfer personal data.[98] BCRs permit multinational companies to transfer personal data globally within the same corporate group, even if members are located in a country that does not provide an adequate level of data protection as required by the GDPR.[99]

The main difference between BCRs and other adequacy instruments is that the burden on assessing BCR is on SAs. GDPR article 47 describes the mechanism and the essential information that should be included in BCRs. The EC has also provided guidelines on the approval procedure of the BCRs for controllers and processors to assist enterprises in drafting their own BCR.[100]

BCR v. Adequacy Decision_ When it comes to the selection between BCRs and adequacy decisions such as Safe Harbor between the EU and the U.S.,

---

[96] pwc, Binding Corporate Rules, https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf.
[97] GDPR Article 47(1)(a).
[98] *Supra* note 96.
[99] *Id.*
[100] European Commission, Binding Corporate Rules, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

many multinational companies prefer BCRs as it permits transferring data between their entities globally. In contrast, the adequacy decision is limited to transferring data between the EU and the country subject to the decision. On the other hand, smaller companies can find the cost of BCRs unattractive. In addition, BCRs don't cover transfers to third parties and other means such as adequacy decisions will be required when the organization is transferring personal data outside of its corporate group.

3.2.3. Standard Contractual Clauses as a Means of Transferring Personal Data to a Third Country or to an International Organization

According to the GDPR Article 46 (2), SCCs adopted by the EC or adopted by a SA and approved by the EC are considered as appropriate safeguards to transfer data to third countries.[101] SCCs are pre-approved contract clauses by the EC.[102] On June 4, 2021, the EC adopted two sets of SCCs for use between controllers and processors and for the transfer of personal data to third countries.[103] The EC considers the joint opinion of the EDPB and EDPS,

[101] GDPR Article 47(1)(a).
[102] European Commission, Standard Contractual Clauses (SCC), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
[103] European Commission, European Commission adopts new tools for safe exchange of personal data (2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

feedback from stakeholders during a broad public consultation, and the opinion of Member States' representatives to draft the new set of SCCs.[104]

The purpose of SCCs is to ensure appropriate data protection safeguards for the transfer of data between controllers and processors and international data transfers to third countries. Data exporters and importers are free to add other clauses or additional safeguards to SCCs, only if they do not contradict, directly or indirectly the SCCs, or prejudice the fundamental rights and freedoms of data subjects.[105] In addition to transferring data freely across borders, controllers and processors can use SCCs as a tool to demonstrate their compliance with the GDPR.[106]

BCRs v. SCCs_ BCRs establish a higher standard for GDPR compliance within the enterprises which reduces the risk of potential data breaches.[107] BCRs as a company's internal policy improve data protection awareness and compliance within a corporate group and can be used to demonstrate GDPR accountability. Additionally, the competent SA does not require to

[104] *Id*.
[105] COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, page 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.
[106] *Supra* note 96.
[107] *Supra* note 103.

approve non-material updates to BCRs.[108] This means saving both time and costs for the companies which is not available in other adequacy mechanisms.[109]

Generally, SCCs work better for smaller companies and bilateral data transferring between controllers and processors.[110] SCCs may not be suitable for complex data processing for large multinational companies, as large multinational companies normally have many global affiliates and need to implement hundreds of SCCs which can be expensive and time-consuming.[111] Also, some EU member states require additional formalities, such as filing and approval of SCCs by the SA which make the process of implementing SCCs both lengthy and costly.[112]

3.2.4. Approved Code of Conduct as a Means of Transferring Personal Data to a Third Country or to an International Organization

GDPR has recognized codes of conduct that are approved by the competent SA and received general validity by the EC, as an appropriate mechanism

[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*

to transfer data to third countries.[113]In order to provide appropriate safeguards for transferring data to third countries, the approved and validated code of conduct may also be followed and used by controllers or processors located in third countries and not subject to the GDPR.[114] "such controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code."[115]

3.2.5. Certification as a Means of Transferring Personal Data to a Third Country or to an International Organization

GDPR Article 42(2) considers sealed or marked approved certification as an appropriate safeguard to transfer data to third countries. To provide such safeguards, the sealed or marked and approved certification may be followed and used by controllers or processors located in third countries and not subject to the GDPR.[116] Such controllers and processors are required

[113] GDPR Article 40(3) and 46(2)(e); European Data Protection Board (edpb), Guidelines 04/2021 on codes of conduct as tools for transfers (2021), page 4, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en.
[114] *Id.* In July 2021, in accordance with Article 46(2)(e), the European Data Protection Board issued a guideline on codes of conduct as tools for transferring personal data from EEA to third countries. The guideline has practical information regarding the content of such codes of conduct, their adoption process, the actors involved and the conditions to be fulfilled and assured to be provided by a code of conduct. See at: European Data Protection Board, Guidelines 04/2021 on codes of conduct as tools for transfers (2021), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en.
[115] *Id*.
[116] GDPR Article 42(2).

to "make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards"[117] provided by the certification.

The certification is voluntary and limited to a maximum period of three years. The certification "may be renewed under the same conditions, provided that the relevant criteria continue to be met."[118] Additionally, the certification is withdrawable "by the certification bodies referred to in Article 43 or by the competent supervisory authority where the criteria for the certification are not or are no longer met."[119] Controllers or processors who received the sealed or marked as approved certification may receive data from different exporters as long as the transfer is within the defined scope of the certification.

3.2.6. Ad hoc Contractual Clauses as a Means of Transferring Personal Data to a Third Country or to an International Organization

According to the GDPR article 46 (3)(a), data controllers and processors can use contractual clauses as an appropriate safeguard to transfer data from

[117] *Id*.
[118] GDPR Article 42(7).
[119] *Id.*

the EU to third countries. Unlike SCCs which are pre-approved by the EC, these contractual clauses are subject to authorization from the competent SA to ensure appropriate data protection safeguards are met.[120]

3.2.7. Administrative Arrangements Between Public Authorities or Bodies as a Means of Transferring Personal Data to a Third Country or to an International Organization

GDPR Article 46(3)(b) accepts provisions to be inserted into administrative arrangements between public authorities or bodies as a safeguard to transfer data between the EEA and third countries.[121] These provisions are subject to a case-by-case authorization from the competent SA.[122] Regardless of the type of legal instrument adopted between the parties, these provisions must include enforceable and effective data subject rights.[123]

[120] GDPR Article 46(3)(a).
[121] GDPR Article 46(3)(b).
[122] *Id.*
[123] *Supra* note 105, at 16-18.

3.2.8. International Agreements as a Means of Transferring Personal Data to a Third Country or to an International Organization

EU's member states may establish international agreements to transfer personal data to third countries or international organizations[124] Such agreements must have appropriate safeguards to protect the fundamental rights of the data subjects and do not affect GDPR or any other provision of Union law.[125] International agreements such as mutual legal assistance treaties are appropriate safeguards that facilitate the international cooperation between the EC and third countries with regards to transferring data globally.[126]

According to international law principles, countries may exercise their legislative, executive, or judicial powers within their own territories and jurisdictions. However, some third countries may adopt laws, regulations, and other legal acts which may directly regulate the activities of individuals and legal entities under other counties' jurisdiction. The extraterritorial application of those legal acts may be in breach of international law. Within

[124] GDPR Recital 102.
[125] *Id*.
[126] *Supra* note 96.

the context of data protection law, for example, this could be court judgments or administrative decisions in third countries requiring a controller or processor to transfer or disclose EU personal data. According to the GDPR, such transfers should only be allowed where the conditions of the GDPR for a transfer to third countries are fulfilled. In such situations, GDPR article 48 considers international agreements, such as mutual legal assistance treaties, in force between the requesting third country and the union or a member state as an appropriate mechanism to transfer data to third counties.[127]

4. Exceptions (Derogations for Specific Situations) to Process Personal Data

This section seeks to examine the specific situations based on which, data actors can transfer data even in the absence of an adequacy decision pursuant to article 45(3), or an appropriate safeguard pursuant to article 46. Based on GDPR Article 49, there are specific situations in which international data transfer may take place in the absence of an adequacy decision or appropriate safeguards. However, the derogations provided by article 49 are limited and "must be interpreted restrictively and mainly

[127] GDPR Article 48 and Recital 115.

relate to processing activities that are occasional and non-repetitive."[128] Therefore, derogations under article 49 are exemptions from the general principle to transfer personal data to a third country.[129]

4.1. Data Subjects' Consent to Process Personal Data

As discussed in chapter three, data subjects' consent is one way to process personal data. However, such a consent must meet GDPR conditions such as being explicit, informed, and specific to be acceptable. Similarly, GDPR article 49 has also specified that the data subject's consent must be explicit, specific to the proposed transfer, and informed of the possible risks of transfers in the absence of an adequacy decision and appropriate safeguards.[130] It is worth mentioning that the consent provided by a data subject cannot be considered as a feasible long-term solution for transferring data to third countries since it can be withdrawn at any time by the data subject.[131]

[128] *Supra* note 68, at 6.
[129] *Supra* note 103, at 4.
[130] GDPR Article 49.1.a.
[131] *Supra* note 103, at 8.

4.2. Performance of a Contract between the Data Subject and the Data Controller as a Lawful Base to Process Personal Data

Another derogation is when the personal data transfer is necessary for the performance of a contract between the data subject and the controller, or the transfer is necessary for implementing the pre-contractual measures at the data subject's request.[132] This derogation is limited by two criteria, necessity, and occasional transfers.[133]

The necessity test _ The necessity test requires "a close and substantial connection between the data transfer and the purposes of the contract."[134] For example, this derogation cannot be used when a corporate group transfers its employee's information to a third country for business purposes as there is "no direct and objective link between the performance of the employment contract and such transfer."[135] However, other grounds for transfer such as standard contractual clauses or BCRs may be appropriate for the transfer.

[132] GDPR Article 49(1)(b).
[133] *Supra* note 105.
[134] *Id*.
[135] *Id*.

On the other hand, a travel agent company can use its clients' consent to transfer their data to hotels located in a third country as this transfer is necessary for the client to stay abroad and also necessary for performing the contract between the travel agent and the client.[136] In this example, "there is a sufficient close and substantial connection between the data transfer and the purposes of the contract" [137] which is the organization of clients' travel.

The occasional test _ The occasional test requires the data transfer to be on an occasional basis. This would be determined on a case-by-case basis.[138] For instance, a sales manager travels to third countries to arrange meetings according to his employment contract. If a bank in the EU transfers his personal data to a bank in a third country to perform the sales manager's request for making a payment, this transfer is occasional as long as it "does not occur in the framework of a stable cooperation relationship between two banks."[139] However, the personal data transfer of a multinational company that organizes training within a third country and transfers the personal data of its employees to attend a training course, would not be

[136] *Id, at 9*.
[137] *Id*.
[138] *Id*.
[139] *Id*.

considered as occasional. Because the transfers are regular and repeated. Therefore, in this example, the data transfers may not be based on Article 49(1)(b).[140] Additionally, public authorities cannot use this derogation to transfer data based on their public powers.[141]

4.3. The Personal Data's Transfer Is Necessary for Important Reasons of Public Interest.

According to the GDPR article 49(1)(d), the public interest derogation applies when "the transfer is necessary for important reasons of public interest."[142] Article 49(4) of the GDPR specifies that the public interest "shall be recognised in Union law or in the law of the Member State to which the controller is subject."[143] However, it is not enough that the public interest exists in an abstract sense in EU or Member State law. The derogation only applies when it can also be construed:

> From EU law or the law of the member state to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation. The existence of an international agreement or convention which recognises a certain objective and provides for international cooperation to foster that objective can be an indicator when assessing the existence of a public interest

[140] *Id*.
[141] *Id* and GDPR Article 49(1)(3).
[142] GDPR Article 49(1)(d).
[143] GDPR Article 49(4).

> pursuant to Article 49 (1) (d), as long as the EU or the Member States are a party to that agreement or convention. [144]

According to the GDPR recital 112, the important criterion for this derogation is the existence of important public interest and the transfer doesn't depend on the nature of the organization which transfers or receives the data.[145] Therefore, the derogation can apply to the transfer of personal data by public, private, or international organizations or they can be the recipient of the data.[146]

4.4. The Transfer Is Necessary for the Establishment, Exercise, or Defense of Legal Claims

According to the GDPR article 49 (1) (e), a transfer may happen when "the transfer is necessary for the establishment, exercise or defense of legal claims."[147] A transfer can take place when it is "occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies."[148]

---

[144] *Supra* note 103, at 10.
[145] *Id, at 11.*
[146] *Id.*
[147] GDPR Article 49(1)(e).
[148] GDPR Recital 111.

In fact, with using the terms "legal claim" and "procedure", Recital 111 implies that the procedure related to the transfer could be out of the court procedure and it doesn't need to be judicial or administrative procedures.[149] However, it should have a basis in law and there should be a close link between the procedure and the transfer.[150] For example, the recital covers the actions by the data exporter to start procedures in a third country to commence litigation or to get approval for a merger and acquisition.[151] Additionally, data controllers and processors need to be aware of the "blocking statutes" of the national law which prohibit or restrict them "in transferring personal data to foreign courts or possibly other foreign official bodies."[152] This derogation should also follow the necessity and occasional test similar to the performance of a contract derogation.[153]

4.5. The Transfer Is Necessary in Order to Protect the Vital Interests of the Data Subject or of Other Persons

Pursuant to the GDPR article 49(1)(f), the vital interest derogation applies when "the transfer is necessary in order to protect the vital interests of the

[149] *Supra* note 103, at 11.
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *Id.*

data subject or of other persons, where the data subject is physically or legally incapable of giving consent"[154]. GDPR restricts the use of this derogation to the existence of a medical emergency and data transfer is directly necessary in order to give the medical care required.[155] Therefore, for example, "where the personal data is required to prevent eviction from a property, this would not fall under this derogation as, even though housing be considered as a vital interest, the person concerned can provide his/her consent for the transfer of his/her data."[156]

Additionally, "the data transfers could be to an international humanitarian organization to satisfy a task under the Geneva Conventions or to comply with international humanitarian law applicable in armed conflict."[157] Finally, the transfer of personal data could be after the occurrence of natural disasters such as floods, earthquakes, and hurricanes and providing personal data to the entities and persons for the purpose of rescue and retrieval operations.[158] In such situations, the concerned data subject needs to be physically or legally incapable of giving consent.[159]

---

[154] GDPR Article 49(1)(f).
[155] *Id, at 12.*
[156] *Id, at 13.*
[157] *Id.*
[158] *Id.*
[159] *Id* and Recital 112.

4.6. Data Transfer from Registers Which Is Intended to Provide Information to the Public

This derogation permits data transfer from registers "which according to Union or Member State law is intended to provide information to the public"[160]. Therefore, private registers in charge of private bodies such as creditworthiness are not within the conditions of the public register derogation.[161] Moreover, the register must be "open to consultation either by the public in general or by any person who can demonstrate a legitimate interest"[162]. Some examples of these registers are "registers of companies, registers of associations, registers of criminal convictions, (land) title registers or public vehicle registers."[163] Transfers from these registers must be "only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case."[164]

Data exporters including data processors and controllers should notice that a transfer under this derogation "shall not involve the entirety of the personal data or entire categories of the personal data contained in the

[160] GDPR 49(1)(g).
[161] *Supra* note 103, at 13.
[162] GDPR 49(1)(g).
[163] *Supra* note 103, at 14.
[164] GDPR 49(1)(g).

register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients."[165]Additionally, according to the GDPR article 49(3), activities carried out by public authorities in the exercise of their public powers would be within the scope of this derogation.

4.7. Transferring Personal Data for the Compelling Legitimate Interest of Data Controllers

This derogation permits data transfer to a third country or an international organization only when a transfer cannot be done based on the previously mentioned provisions and derogations.[166] For example, "binding corporate rules may often not be a feasible option for small and medium-sized enterprises due to the considerable administrative investments they imply."[167] Or "where the data importer has expressly refused to enter into a data transfer contract on the basis of standard data protection clauses."[168]

The transfer should not be repetitive and should concern only a limited number of data subjects.[169] This limitation depends on the context of the

[165] GDPR 49(2).
[166] GDPR 49(1).
[167] *Supra* note 103, at 15.
[168] *Id.*
[169] GDPR 49(1).

data transfer. The number of concerned data subjects should be appropriately small considering the type of transfer in each situation.[170] For instance, a data controller requires to discover a serious security case to protect its entity. And to achieve this compelling legitimate interest, the controller needs to transfer personal data. The controller can transfer only a certain number of data restricted to its purpose.[171] Additionally, the transfer should be "necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject"[172]

Therefore, the interests of a data exporter, data processor, or data importer are not relevant factors to determine the application of this derogation.[173]Only compelling interests of data controllers are relevant.[174] This situation might involve compelling interests of the controller when the controller is required to transfer the personal data to protect its entity from serious immediate harm or a severe penalty that would seriously affect its business.[175] Even in a compelling interest situation, the controller has to

[170] GDPR Article 49(1)(3).
[171] *Id*.
[172] GDPR 49(1).
[173] *Supra* note 103, at 15.
[174] *Id*.
[175] *Id*.

assess all the circumstances and provide appropriate safeguards to protect the personal data.[176] The controller must also inform the relevant SA and the data subject about the transfer.[177]

5. Conclusion

Chapter four examined how multinational companies can transfer data from EEA to safe and unsafe third countries. As discussed, GDPR requires the controllers and the processors to comply with further requirements if they want to transfer personal data to third countries or international organizations outside the EEA. Firstly, the data transfer itself should be within the definition of data processing. Secondly, the data transfer must meet one of the legal bases mentioned in article 6 to be lawful. Finally, the transfer must be permitted under one of the adequacy safeguards specified in the GDPR chapter V.

Chapter four concluded that every data transfer from EEA to non-EEA is not subject to the GDPR chapter V. The EDPB has recognized three criteria that fulfill the definition of a transfer to a third country or an international organization. If all the three criteria are met, then there is a transfer to a

[176] *Id*.
[177] *Id* and GDPR 49(1).

third country or to an international organization in accordance with the GDPR Chapter V[178] and the data exporter[179] needs to comply with the specified conditions mentioned in chapter V to transfer data[180]. Consequently, chapter four examined GDPR chapter V requirements when a data processing (transfer) meets all the three criteria. A restricted transfer of personal data can be covered by an EU commission adequacy decision, appropriate safeguards, or exceptions.[181] As such, chapter four discussed in different subsections possible ways to transfer data outside the EEA.

More specifically, chapter four concluded that when it comes to the selection between BCRs and adequacy decisions such as Safe Harbor between the EU and the U.S., many multinational companies prefer BCRs as it permits transferring data between their entities globally. In contrast, the adequacy decision is limited to transferring data between the EU and the county subject to the decision. However, smaller companies can find the cost of BCRs unattractive. In addition, BCRs don't cover transfers to third parties and other means such as adequacy decisions will be required when the organization is transferring personal data outside of its corporate group.

[178] *Id.*
[179] Data exporter is the controller or processor transferring the personal data to a third country.
[180] Data importer is the controller or processor receiving the personal data.
[181] *Id.*

Data importers and exporters can also enter a contract that contains SCCs adopted by the Commission or a SA and then approved by the Commission.[182] Data exporters and importers are free to add other clauses or additional safeguards to SCCs, only if they do not contradict, directly or indirectly the SCCs, or prejudice the fundamental rights and freedoms of data subjects.[183] In addition to transferring data freely across borders, controllers and processors can use SCCs as a tool to demonstrate their compliance with the GDPR.[184]

Chapter four compared BCRs and SCCs and concluded that BCRs establish a higher standard for GDPR compliance within the enterprises and they reduce the risk of potential data breaches.[185] BCRs as a company's internal policy improve data protection awareness and compliance within a corporate group and can be used to demonstrate GDPR accountability. Additionally, the competent SA does not require to approve non-material updates to BCRs.[186] This means saving both time and costs for the companies which is not available in other adequacy

[182] *Id.*
[183] COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, page 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.
[184] *Supra* note 103.
[185] *Supra* note 96.
[186] *Id*.

mechanisms.[187]However, SCCs work better for smaller companies and bilateral data transferring between controllers and processors.[188] SCCs may not be suitable for complex data processing for large multinational companies, as large multinational companies normally have many global affiliates and need to implement hundreds of SCCs which can be expensive and time-consuming.[189] Also, some EU member states require additional formalities, such as filing and approval of SCCs by the SA which make the process of implementing SCCs both lengthy and costly.[190]Finally, chapter four discussed GDPR Article 49(1) to examine the potential exceptions when a restricted transfer is not under article 45(3), adequacy decision, nor article 46, appropriate safeguards.

[187] *Id*.
[188] *Id*.
[189] *Id*.
[190] *Id*.

CHAPTER 5: CONCLUSION AND RECOMMENDATION

1. Findings of the Research

The main purpose of this dissertation is to assess GDPR as part of international data protection law and examine how it advances and harmonizes international contracts between controllers, processors, and data subjects. This dissertation concluded that GDPR is advancing and harmonizing international data protection law since, firstly, GDPR sovereignty passes EU countries' borders and internationally governs all companies which operate in EU countries and are involved with personally identified or identifiable living individuals' data. These companies could be based in the EU, offer goods or services to an individual in the EU, or monitor an individual in the EU. Secondly, more than 120 countries around the world have passed data privacy regulations and many of these countries have articulated their law based on the privacy principles set up by GDPR. Finally, many multinational companies apply GDPR data protection principles worldwide to avoid business costs, and duplication of operational efforts and ensure their customers and employees feel trusted in permitting them to find access to their data.

Chapter one is the introduction chapter of this dissertation. Chapter one provided some detailed background on the adoption of GDPR in the EU and the scope of this research work. Chapter one also defined some key terms and concepts for the purpose of GDPR discussion and it also compared some key definitions with similar concepts in CCPA and CPRA.

Chapter two examined two types of GDPR contract bases that make the processing of personal data lawful. These are the data subject's consent and the necessity of the processing for the performance of a contract. In cyberspace, controllers normally get their data subjects' consent through user agreements. As such, sometimes it could be challenging for the controllers to distinguish which type of lawful base for the processing they are involved in and which GDPR requirements they need to comply with. Thus, chapter two described and compared these two contract bases of personal data processing. Chapter two also discussed the elements of valid consent articulated in GDPR article 4(11) through real cases to highlight the importance of each consent element in GDPR contract bases for processing data subject's personal data.

In considering the type of contracts between controllers and data subjects, chapter two examined different types of user agreements, as contracts

between controllers and data subjects to see if they fulfill GDPR compliance requirements. It further demonstrated that when data processing is based on data subject's consent, the burden of proof is on controllers to prove that the data subject has given a valid consent to the processing operation. This is especially important when the controller sends a written declaration on another matter to the data subject. In this context, the controller shall be able to prove that the data subject has been aware of the fact and to what extent the consent is informed and specific.

GDPR article 6 is about processing data subject's personal data, which is necessary for the performance of a contract. Chapter two recognized that processing is not considered necessary for the performance of a contract when providing the contractual services is possible without processing personal data. Therefore, if the other party of the contract wants to process personal data, it is better to rely on other bases mentioned in article 6, including data subject's freely given consent.

Finally, chapter two identified that GDPR protects personal data which are accessible to the public. To better visualize the significance of the discussion, chapter two examined the US case, *hiQ Labs, Inc. v. LinkedIn Corp.*, which was decided in front of the U.S. District Court for the Northern

District of California and the United States Court of Appeals for the Ninth Circuit. It particularly hypothesized the case in front of the EU authorities and discussed how the case decision would be different from the issued US decision. The importance of this discussion is to add GDPR data protection analysis to the US decision and recommend data protection policies to the field of data protection law in the US. Chapter two also compared GDPR and CPRA in terms of processing and profiling public personal data and concluded that in the US, even California data privacy law, the pioneer privacy law in the US, does not protect publicly available personal information.

Basically, processing EU personal data shall be based on the principles mentioned in the GDPR article 5, which includes the accountability principle. Based on the accountability principle, the controller shall be responsible for and be able to demonstrate compliance with the GDPR principles. As such, chapter three highlighted the importance of contracts between controllers and processors not only for demonstrating accountability compliance under article 5(2) but also for proving GDPR article 28 compliance. Under the GDPR article 28(3), every time that data is transferred between controllers and processors or processors and sub-processors, there should be a contract to govern the processing activity.

Furthermore, according to the GDPR article 26, if two or more controllers jointly determine the purposes and means of processing, they are jointly responsible for the processing and there shall be an arrangement between joint controllers. Therefore, chapter three examined contracts as one of the means between joint controllers to determine their obligations. Chapter three compared GDPR, CCPA and CPRA and demonstrated that CCPA and CPRA also considered contracts as an important means to provide certainty and transparency and help controllers and processors to prove their compliance.

Chapter three distinguished and clarified controllers, joint controllers, processors, and sub-processors' responsibilities and liabilities towards each other and data subjects in the context of contracts. Chapter three concluded that the concepts of controller, joint controller, and processor play an important role in implementing the GDPR since they are jointly liable, and their liabilities are limited to violations of obligations that are specific to each data actor.

Chapter three also discussed responsibilities and liabilities between controllers and processors in case of GDPR non-compliance and awarding damages to data subjects whose rights have been breached. Chapter three

concluded that when a data subject is damaged by two or more controllers' or processors' processing acts, each data processing actor is "jointly and severally liable" for the damage caused to the data subject and the data subject may recover the entire damage from any controller or processor who is involved in the same processing causing the damage. However, GDPR comparative contribution principle enables any controller or processor who is required to pay more than his share of damage to a data subject to claim back the excess in a claim against the other data processing actors.

Chapter four recognized three criteria that fulfill the definition of a transfer to a third country or an international organization. If all three criteria are met, then there is a transfer to a third country or to an international organization in accordance with the GDPR Chapter V. Consequently, the data exporter needs to comply with the conditions mentioned in chapter V to transfer data to the data importer.

Chapter four also examined the EC adequacy findings for the US, which are invalid due to US surveillance programs, and it further explained appropriate safeguards, which are additional ways for the transfer of data to inadequate territories outside the EEA where there is no EC adequacy

decision about them. More specifically, chapter four examined and compared popular safeguards such as BCRs and SCCs between multinational companies including small companies, Joint ventures, and franchises to transfer personal data in the absence of an adequacy decision.

2. Recommendations

The followings are recommended by this dissertation regarding the above-mentioned research findings:

1. The US should consider some world-known data protection principles such as transparency and fairness in its court procedures especially when personal data processing is involved with machine learning, profiling, and automated decision-making. This is increasingly important to protect data subjects' human rights. Moreover, adequate data protection regulations change access to the global economy, produce new markets, increase competition, and harmonize data protection principles around the world. It is also recommended that the US protects public personal data to avoid discrimination against data subjects. This is because deep machine learning, artificial intelligence and secret algorithmic processing can

be misleading and cause discrimination against individuals through automatic decision-making.

2. Contracts are recommended as powerful means to provide certainty and transparency and help controllers and processors to prove their compliance with GDPR. Contracts not only protect data subjects' personal data but also, help data actors to understand their responsibilities and liabilities under the GDPR. Contracts further ensure legal certainty and avoid possible conflicts in the relationship between the data actors and between the data subjects and the data protection authorities.
3. BCRs are recommended for enterprises involved in a joint economic activity such as big multinational entities, joint ventures, and franchises for transferring data from EEA to Non-EEA. BCRs permit multinational companies to transfer personal data globally within the same corporate group, even if members are in a country that does not provide an adequate level of data protection as required by the GDPR. When it comes to the selection between BCRs and adequacy decision such as Safe Harbor between the EU and the U.S., many multinational companies prefer BCRs as it permits transferring data between their entities globally, whereas the adequacy decision is

limited to transferring data between the EU and the county subject to the decision. However, smaller companies can find the cost of BCRs unattractive. In addition, BCRs don't cover transfers to third parties and other means such as adequacy decisions will be required when the organization is transferring personal data outside of its corporate group.

4. It is also recommended that BCRs establish a higher standard for GDPR compliance within the enterprises and reduce the risk of potential data breaches. BCRs as a company's internal policy improve data protection awareness and compliance within a corporate group and can be used to demonstrate GDPR accountability. Additionally, the competent SA does not require to approve non-material updates to BCRs. This means saving both time and costs for the companies which is not available in other adequacy mechanisms.
5. Finally, it is recommended that SCCs work better for smaller companies and bilateral data transferring between controllers and processors. SCCs might not be suitable for complex data processing for large multinational companies, as large multinational companies normally have many global affiliates and need to implement

hundreds of SCCs which can be expensive and time-consuming. Also, some EU member states require additional formalities, such as filing and approval of SCCs by the SA which make the process of implementing SCCs both lengthy and costly.

3. Research Limitations

How GDPR harmonizes international contracts in data protection law is a relatively new approach in academic research and I recognize that there are a few limitations to my research. First, GDPR evolved over time and initially, the application of the law was not clear in terms of new terms that are used in the 88-page GDPR. Over years, different SAs issued decisions in this regard and EDPB published related guidelines and explained the application of new terms. In fact, organizations are still challenged to make sure that their efforts and approaches to comply with GDPR are enough. Since sometimes they have a specific understanding of a GDPR term and a subsequent SA's decision or EDPB guideline puts their compliance efforts under question. Moreover, it was challenging to keep up to date with reviewing and adding various EDPB guidelines and court decisions related to 27 SAs in the EU as the implication of the law was constantly changing over time. Accordingly, it was challenging to track and find out the

harmony between different authorities' decisions in terms of GDPR breaches and implication.

4. Suggestions for Further Research

The future of international data protection law depends on how different jurisdictions address the fundamental principles of data protection law in their respective legislation. This entails avoiding discriminatory and unethical processing and following fundamental data protection principles such as fairness and transparency to process data subjects' personal data. Even if many countries around the world are following the GDPR framework to pass their data protection law, however, there are still countries such as the US that do not have a unique set of data protection legislation to direct and harmonize the states in complying with data protection fundamentals. Therefore, further research is required to address the differences and encourage countries to harmonize the fundamentals of data protection law to mitigate the risk of conflict and advance international comity between countries.

BIBLIOGRAPHY

1. Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.
2. Kristin Finklea et al., Cyber Intrusion into U.S. Office of Personnel Management: In Brief, Congressional Research Service (2015), https://fas.org/sgp/crs/natsec/R44111.pdf.
3. European Data Protection Supervisor, Data Protection, https://edps.europa.eu/data-protection_en.
4. EUROPEAN COMMISSION Press Release Database, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.
5. European Commission, Protection of personal data, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en#whattheecisdoingtoprotectyourrights.
6. European Data Protection Supervisor, The History of the General Data Protection Regulation, https://edps.europa.eu/data-

protection/data-protection/legislation/history-general-data-protection-regulation_en.

7. Information Commissioner's Office, What is personal data? At a glance, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.
8. Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), What are identifiers and related factors?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/.
9. Comlior, Pseudonymisation and Anonymization of Personal Data, https://complior.se/pseudonymization-and-anonymization-of-personal-data-what-is-the-difference/.
10. Durham University, Information Governance, Anonymization and Pseudonymisation, https://www.dur.ac.uk/ig/dp/anonymisation/.
11. Information Commissioner's Office, What is encryption, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-

to-the-general-data-protection-regulation-gdpr/encryption/what-is-encryption/.

12. William Jackson, Why salted hash is as good for passwords as for breakfast, https://gcn.com/articles/2013/12/02/hashing-vs-encryption.aspx#:~:text=Encryption%20is%20a%20two%2Dway,to%20reveal%20the%20original%20password.
13. European Commission, What constitutes data processing, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en.
14. Ben Woldford, GDPR.EU, What is a GDPR data processing agreement?, https://gdpr.eu/what-is-data-processing-agreement/.
15. Contracts, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/.
16. Upcounsel, How to write a User Agreement: Everything You Need to Know, https://www.upcounsel.com/how-to-write-a-user-agreement#:~:text=A%20user%20agreement%20is%20an,examples%20of%20a%20user%20agreement.
17. Information Commissioner's Office, When is a contract needed and why is it important, https://ico.org.uk/for-organisations/guide-to-

data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/.

18. Datatilsynet, Decision on infringement fee to Coop Finnmark, https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/vedtak-om-overtredelsesgebyr-til-coop-finnmark/.
19. European Data Protection Board, Norwegian DPA issues fine to Coop Finnmark, https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-issues-fine-coop-finnmark_en.
20. European Commission, Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
21. European Data Protection Board (edpb), Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 (2020), page 7, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
22. Elaine Loughlin, Irish Examiner, Data Protection commission seeks answers on destruction of mother and baby homes recordings (2021), https://www.irishexaminer.com/news/arid-40218473.html.

23. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (GPDP), Injunction order against the Enna Provincial Health Authority (2021), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542071.
24. European Data Protection Board, Belgian DPA imposes €50,000 Fine on Family Service, https://edpb.europa.eu/news/national-news/2021/belgian-dpa-imposes-eu50000-fine-family-service_en.
25. Europe Data Protection Board, Spanish Data Protection Authority (AEPD) imposes fine of 6.000.000 EUR on CAIXABANK, S.A., https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank-sa_en.
26. Peter Hence, Clubhouse app faces court action in Germany over serious failing under data protection and consumer law (2021), https://www.jdsupra.com/legalnews/clubhouse-app-faces-court-action-in-6123803/.
27. Natasha Singer and Aaron Krolik, The New York Times (2021), https://www.nytimes.com/2021/01/25/business/grindr-gdpr-privacy-fine.html.

28. The Center, LGBTQ is an acronym for lesbian, gay, bisexual, transgender and queer or questioning, https://gaycenter.org/about/lgbtq/.
29. Guido Scorza, Privacy Guarantor Authority, The algorithm must be transparent, https://www.agendadigitale.eu/sicurezza/privacy/lalgoritmo-deve-essere-trasparente-la-cassazione-rilancia-il-gdpr/.
30. Julie Brill, Microsoft begins new EU GDPR parental consent verifications for children's accounts (2018), https://blogs.microsoft.com/on-the-issues/2018/04/11/microsoft-begins-new-eu-gdpr-parental-consent-verifications-for-childrens-accounts/.
31. Vincent Manancourt, Italy orders TikTok to stop using children's data (2021), https://www.politico.eu/article/italy-orders-tiktok-to-stop-using-childrens-data.
32. European Data Protection Board, Italian DPA imposes limitation on processing on TikTok after the death of a Girl from Palermo (2021), https://edpb.europa.eu/news/national-news/2021/italian-dpa-imposes-limitation-processing-tiktok-after-death-girl-palermo_en.

33. Electronic Irish Statute Book (eISB), Data Protection Act 2018, Child for purpose of application of Data Protection Regulation, http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html.
34. The Garante, Tik Tok will adapt the requests of the privacy Guarantor, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533424#en.
35. Upcounsel, How to write a User Agreement: Everything You Need to Know, https://www.upcounsel.com/how-to-write-a-user-agreement#:~:text=A%20user%20agreement%20is%20an,examples%20of%20a%20user%20agreement.
36. THOMSON REUTERS, PRACTICAL LAW, Glossory, Borwsewrap Agreement, https://1.next.westlaw.com/Document/I2e45ae49642211e38578f7ccc38dcbee/View/FullText.html?transitionType=Default&contextData=(sc.Default)&firstPage=true&OWSessionId=40fabf6a8d0b4d6bb49690525c5ee092&isplcus=true&fromAnonymous=true&bhcp=1.
37. Nguyen v. Barnes & Noble Inc. (9th Cir. 2014) 763 F.3d 1171.
38. Vitacost.com, Inc. v. Mccants (Fla.Dist.Ct.App. 2017) 210 So.3d 761.

39. FreePrivacyPolicy, Examples of "I Agree to Privacy Policy Checkboxes, FreePrivacyPolicy (2021), https://www.freeprivacypolicy.com/blog/agree-privacy-policy-checkboxes/.
40. Linkedin.com, *User Agreement (2021)*, https://www.linkedin.com/legal/user-agreement.
41. I. Lan Sys. v. Netscout Serv. Level Corp. (D.Mass. 2002) 183 F.Supp.2d 328.
42. JOM, Inc. v. Adell Plastics, Inc., 193 F.3d 47, 52-59 (1st Cir. 1999) (en banc).
43. GDPR.EU, Cookies, the GDPR, and the ePrivacy Directive, https://gdpr.eu/cookies/.
44. Norton, what are cookies (2019), https://us.norton.com/internetsecurity-privacy-what-are-cookies.html.
45. JDSUPRA, The end of dark patterns in "cookie walls": German court bans deceptive designs, Peter Hence (2021), https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/.

46. Cookiebot, Cookie walls |EDBP guidelines on cookie walls and valid consent, https://www.cookiebot.com/en/cookie-walls/#:~:text=A%20cookie%20wall%20is%20a,trackers%20present%20on%20that%20website.
47. European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 (2020), page 11, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
48. European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0 (2020), page 7, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.
49. *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (2021).
50. Linkedin.com, *About LinkedIn*, https://about.linkedin.com/.
51. Fiona Cambell, Data Scraping – Considering the Privacy Issues (2019), https://www.fieldfisher.com/en/services/privacy-

security-and-information/privacy-security-and-information-law-blog/data-scraping-considering-the-privacy-issues.).

52. hiQ, Who we are, https://www.hiqlabs.com/.
53. Epic.org, ELECTRONIC PRIVACY INFORMATION CENTER, *hiQ Labs, Inc. v. LinkedIn Cor (2020)*, https://www.epic.org/amicus/cfaa/linkedin/.
54. *LinkedIn Corp. v. hiQ Labs*, 141 S.Ct. 2752, 210 L.Ed.2d 902 (2021).
55. *Van Buren v. United States*, 141 S. Ct. 1648 (2021).
56. Piotr Foitzik, publicly available data under the GDPR: Main considerations (2019), https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/.
57. European Data Protection Board, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) (2018), https://ec.europa.eu/newsroom/article29/items/622227.
58. Colin J. Bennett, Personal Data Processing by and for Political Campaigns: The Application of the Council of Europe's Modernised Convention108, Council of Europe, 22 (2020),

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3633976.

59. European Commission, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
60. European Data Protection Board, ITALIAN SA SAYS NO TO ALGORITHMS CAUSING DISCRIMINATION A platform in the Glovo group fined EUR 2.6 million (2021), https://edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en.
61. European Data Protection Board, Norwegian DPA issues fine to Aqueteknikk AS (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-issues-fine-aquateknikk_en.
62. European Commission, Article 29 Working Party: Guidelines on transparency under Regulation 2016/679 (2018), https://ec.europa.eu/newsroom/article29/redirection/document/51025.

63. European Data Protection Board, Statement 2/2019 on the use of personal data in the course of political campaigns (2019), https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.
64. European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0 (2020), page 3, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.
65. European Data Protection Board, Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR (2019), page 7, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf and https://edpb.europa.eu/news/news/2019/first-standard-contractual-clauses-contracts-between-controllers-and-processors-art_en.

66. European Data Protection Board, EDPB-EDPS Opinion 1/2021 on the European Commission's Implementing Decision on standard contractual clauses between controllers and processors, page 4, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en.
67. Peter Hence, The end of dark patterns in "cookie walls": German court bans deceptive design (2021), https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/.
68. AddThis, About Us, https://www.addthis.com/about/; https://en.wikipedia.org/wiki/AddThis and https://privacyinternational.org/case-study/4403/tracking-service-sharethis-be-profiled.
69. European Data Protection Board, Spanish DPA imposes fine of 1,500,000 euros on EPD Comercializadora, S.A.U. for two infractions of the GDPR (2021), https://edpb.europa.eu/news/national-news/2021/spanish-dpa-imposes-fine-1500000-euros-epd-comercializadora-sau-two_en.

70. European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en.
71. upcounsel, GDPR Certification: Everything You Need to Know, https://www.upcounsel.com/gdpr-certification#:~:text=GDPR%20certification%20is%20a%20new,are%20in%20compliance%20with%20GDPR.&text=GDPR%20also%20means%20greater%20data,other%20individuals%20in%20the%20EU.
72. European Data Protection Board, First standard contractual clauses for contracts between controllers and processors (art. 28 GDPR) at the initiative of DK SA published in EDPB register, https://edpb.europa.eu/news/news/2019/first-standard-contractual-clauses-contracts-between-controllers-and-processors-art_en.
73. UDKAST, Standard Contractual Clauses, for the purpose of Article 28(3) OF Regulation 2016/679 (the GDPR) between the data controller and the data processor, Page 5,

https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf.

74. European Data Protection Board, Polish DPA & ID Finance Poland: Checking potential system vulnerabilities cannot be delayed, https://edpb.europa.eu/news/national-news/2021/polish-dpa-id-finance-poland-checking-potential-system-vulnerabilities_en.
75. CNIL, "Credential stuffing": the CNIL sanctions a data controller and his subcontractor (2021), https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant.
76. European Data Protection Board, Spanish Data Protection Authority (AEPD)imposes fine of 6.000.000 EUR on CAIXABANK, S.A. (2021), https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank_en.
77. European Data Protection Board, Polish DPA & ID Finance Poland: Checking potential system vulnerabilities cannot be delayed (2021), https://edpb.europa.eu/news/national-news/2021/polish-dpa-id-finance-poland-checking-potential-system-vulnerabilities_en.

78. European Data Protection Board, RIDERS: ITALIAN SA SAYS NO TO ALGORITHMS CAUSING DISCRIMINATION A platform in the Glovo group fined EUR 2.6 million (2021), https://edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en.
79. European Data Protection Board, Norwegian DPA: Norwegian Confederation of Sport fined for inadequate testing (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-norwegian-confederation-sport-fined-inadequate-testing_en.
80. European Data Protection Board, Norwegian DPA: BRAbank ASA fined (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-brabank-asa-fined_en.
81. European Data Protection Board, Norwegian DPA: Municipality of Oslo fined (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-municipality-oslo-fined_en.
82. European Data Protection Board, Norwegian DPA: Moss Municipal Council fined (2021), https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-moss-municipal-council-fined_en.
83. European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0

(2020), Page 18, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

84. European Data Protection Board, 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 (2021); https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en.
85. European Commission, Who does the data protection law apply to?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en.
86. European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1 (2019), Page 7, edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.
87. JONES DAY, EU-U.S. Data Protection Safe Harbor: Not Safe Anymore (2015),

https://www.jonesday.com/en/insights/2015/10/euus-data-protection-safe-harbor-not-safe-anymore.

88. European Parliament, Exchanges of Personal Data After the Schrems II Judgment (2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf.

89. European Commission, Guide to the EU-U.S. Privacy Shield, Page 7 (2016), https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf.

90. Privacy Shield Framework, Privacy Shield Overview, https://www.privacyshield.gov/Program-Overview.

91. The U.S. Department of Commerce, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE 1 (2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.

92. The International Association of Privacy Professionals, Frequently Asked Questions & Resources on "Schrems II" (2021), https://iapp.org/resources/article/frequently-asked-questions-resources-on-schrems-ii/.

93. Hendrik Mildebrath, European Parliamentary Research Service, The CJEU judgment in the Schrems II case, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

94. European Data Protection Board, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, Version 2.0 (2020), page 5, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf.

95. pwc, Binding Corporate Rules, https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf.

96. European Commission, Standard Contractual Clauses (SCC), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

97. European Commission, European Commission adopts new tools for safe exchange of personal data (2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.
98. COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, page 3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.
99. European Data Protection Board, Guidelines 04/2021 on codes of conduct as tools for transfers (2021), page 4, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en.