universität wien

MASTER THESIS

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

„A Comparative Analysis of the European Union’s General Data Protection Regulation v. the California Consumer Privacy Act“

verfasst von / submitted by

Dan Jana Linetzky

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

Master of Laws (LL.M.)

Wien, 2022 / Vienna 2022

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Dr. Stephanie Nitsch

ACKNOWLEDGMENTS

First and foremost, I would like to express my gratitude to my family and friends, whose unconditional support from different countries and time zones has been essential for my success in the LL.M. and my new life in Vienna. New ventures always face unpredicted challenges, and through this process, I have always felt their love and care.

I would like to express my sincere appreciation and thanks to my supervisor, Dr. Stephanie Nitsch, who guided me throughout this study and whose guidance was crucial in making my Master's thesis.

I would also like to thank Dr. Siegfried Fina and Dr. Maria Sturm for making the LL.M. European and International Business Law a world-class academic experience.

Finally, my thanks go to all the people who work at the University of Vienna and made this experience possible, who made it possible to attend classes in-person and online in optimal conditions, facing with great success the difficult times of the pandemic.

ABSTRACT

In today's globalized digital economy, companies collect, process, and use personal data from users at an ever-increasing rate from multiple sources. The internet of things and the mass evolution of technology in people's lives have created an immense amount of personal data collected by companies, in a relatively short period of time. This issue has become highly sensitive for people all around the world. As a response to this phenomenon, better and more comprehensive regulations of the rights to privacy and data protection have been demanded. Under this context, the European Union's General Data Protection Regulation 2016/679 ("GDPR") entered into effect on 25 May 2018 and the California Consumer Privacy Act of 2018 ("CCPA") came into effect on the 1st of January, 2020. Bad data privacy practices harm not only consumers but also companies which can suffer great liabilities for infringements to any of these two legal frameworks. Each jurisdiction has adopted its own approach to regulate and impose penalties on infringers of data privacy rules, and therefore, protect consumer rights. Even though the goal of these two laws is to protect personal data and the right to privacy, differences appear evident between both of them, as their approaches to certain conceptual topics are just a reflection of how the European Union on one side, and California in the other, understand what are the key principles upon which their societies should develop when it comes to data privacy and the relation between businesses and data subjects.

This thesis aims to compare the GDPR and the CCPA in its most important guiding principles and rules, to establish the main differences and commonalities between the most comprehensive legal frameworks dealing today with data privacy in the world. By contrasting the GDPR and CCPA scopes of application, legal basis, concepts of data transfers, rights of users, and damages regulations, a consistency rate will be delivered in each chapter. The consistency rate will be determined by the relevance of the differences or similarities in each topic. Relevant legislation, case law, and literature are compared and discussed to outline the differences and commonalities in both approaches undertaken.

ABSTRAKT

In der heutigen globalisierten digitalen Wirtschaft sammeln, verarbeiten und nutzen Unternehmen personenbezogene Daten von Nutzern in immer größerem Umfang aus mannigfaltigen Quellen. Das Internet der Dinge und die massenhafte Entwicklung der Technologie im Leben der Menschen haben dazu geführt, dass Unternehmen in relativ kurzer Zeit eine riesige Menge an personenbezogenen Daten gesammelt haben. Dieses Thema ist für Menschen auf der ganzen Welt äußerst sensibel geworden. Als Reaktion auf dieses Phänomen wurden fortlaufend bessere und umfassendere Regelungen des Rechts auf Privatsphäre und Datenschutz gefordert. In diesem Zusammenhang sind die Datenschutz-Grundverordnung 2016/679 ("DSGVO") der Europäischen Union am 25. Mai 2018 und der California Consumer Privacy Act von 2018 ("CCPA") am 1. Januar 2020 in Kraft getreten. Schlechte Datenschutzpraktiken schaden nicht nur den Verbrauchern, sondern auch den Unternehmen, die bei Verstößen gegen eine dieser beiden gesetzlichen Rahmenbedingungen umfassend haftbar gemacht werden können. Jedes der beiden Gesetze hat seinen eigenen Ansatz gewählt, um Verstöße gegen die Datenschutzvorschriften zu regeln und zu ahnden, und so die Verbraucherrechte zu schützen. Auch wenn das Ziel dieser beiden Gesetze der Schutz personenbezogener Daten und des Rechts auf Privatsphäre ist, bestehen offensichtliche Unterschiede zwischen ihnen, da ihre jeweiligen Ansätze zu bestimmten konzeptionellen Themen lediglich widerspiegeln, wie die Europäische Union auf der einen und Kalifornien auf der anderen Seite die Grundprinzipien verstehen, nach denen sich ihre Gesellschaften entwickeln sollten, wenn es um den Datenschutz und die Beziehung zwischen Unternehmen und von Datensammlung betroffenen Personen geht.

Ziel dieser Arbeit ist es, die DSGVO und das CCPA in ihren wichtigsten Leitprinzipien und Regeln zu vergleichen, um die hauptsächlichen Unterschiede und Gemeinsamkeiten dieser weltweit umfassendsten rechtlichen Rahmenbedingungen für den Datenschutz zu ermitteln. Durch die Gegenüberstellung der Anwendungsbereiche der DSGVO und des CCPA, der jeweiligen Rechtsgrundlage, der Konzepte der Datenübermittlung, der Rechte der Nutzer und der Schadensersatzregelungen wird in jedem Kapitel ein Konsistenzgrad ermittelt. Der Konsistenzgrad wird durch die Relevanz der Unterschiede oder Ähnlichkeiten bei jedem Thema bestimmt. Einschlägige Rechtsvorschriften, Rechtsprechung und Literatur werden verglichen und erörtert, um die Unterschiede und Gemeinsamkeiten der beiden Ansätze hervorzuheben.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS ……..... 6
1. INTRODUCTION ……. 7
2. KEY DEFINITIONS ……. 9
2.1 GDPR …… 9
2.2 CCPA …… 9
2.3 Compared analysis …… 11
3. SCOPE OF APPLICATION …… 13
3.1 Material Scope ……. 13
3.1.1 GDPR ……. 13
3.1.2 CCPA ……. 16
3.1.3 Compared analysis ……. 17
3.2 Territorial Scope ……. 18
3.2.1 GDPR ……. 18
3.2.2 CCPA ……. 20
3.2.3 Compared analysis ……. 22
4. LEGAL BASIS …….. 24
4.1 GDPR …… 24
4.2 CCPA …… 26
4.3 Compared analysis …… 27
5. RIGHTS OF USERS ……..… 28
5.1 Right to Erasure – Right to Deletion ……. 28
5.1.1 GDPR ……. 28
5.1.2 CCPA ……. 30
5.1.3 Compared analysis ……. 32
5.2 Right to be Informed ……..... 33
5.2.1 GDPR ……. 33

5.2.2 CCPA ……. 35

5.2.3 Compared analysis ……. 36

5.3 Right of Access ……..... 36

5.3.1 GDPR ……. 36

5.3.2 CCPA ……. 38

5.3.3 Compared analysis ……. 41

6. ENFORCEMENT ……..... 43

6.1 Monetary Penalties …….. 43

6.1.1 GDPR ……. 43

6.1.2 CCPA ……. 44

6.1.3 Compared analysis ……. 46

6.2 Civil Remedies ……. 46

6.2.1 GDPR ……. 46

6.2.2 CCPA ……. 50

6.2.3 Compared analysis ……. 52

6.3 Representation of data subjects or consumers ……. 53

6.3.1 GDPR ……. 53

6.3.2 CCPA ……. 56

6.3.3 Compared analysis ……. 57

7. CONCLUSION ...……... 58

8. BIBLIOGRAPHY ……. 61

LIST OF ABBREVIATIONS

CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Commission	European Commission
CA AG	California Attorney General
CCPA	California Consumer Privacy Act
DPA	Data protection authority (also called ‘supervisory authority’)
DPD	Data Protection Directive - Directive 95/46/EC
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation—Regulation (EU) 2016/679
TFEU	Treaty on the Functioning of the European Union
The U.S.	United States of America

1. INTRODUCTION.

The European Union's General Data Protection Regulation 2016/679[1] and the California Consumer Privacy Act of 2018[2] can be considered today as one of the most comprehensive data protection frameworks in the world. Both of them aim to strongly guarantee and protect individual personal data and regulate how businesses can collect, use, or share consumer data. On the one hand, the GDPR entered into effect on 25 May 2018. On the other one, the California State Legislature passed the CCPA law in 2018, which came into effect on the 1st of January, 2020. By many, the CCPA is considered as modeled after, or at least inspired by, the GDPR[3]. As of today, these laws have a global impact on the market relevance of the EU and California (home of some of the largest data processing companies such as Facebook or Google).

Under both laws, when personal data has been exposed due to a company's security failures, the right to seek compensation is regulated to protect the data subject whose rights have been infringed. Careless corporate practices, human error, and cybercrime mean that personal information is not as protected as it should be. When this type of information falls into the wrong hands, it can lead to serious financial loss, mental distress, and loss of privacy.

This thesis aims to make a detailed comparison between the GDPR and the CCPA, to establish the most significant differences and commonalities between these two regulations. Even if the CCPA can be considered modeled after the GDPR, as we will review in the next chapters these two laws are fairly divergent when read carefully. Each chapter of this thesis will begin with a study of the relevant provisions of the GDPR, followed by the ones of the CCPA to finally make an analysis and comparison of how both legal frameworks regulate specific matters.

With the structure of analysis described in the last paragraph, this thesis will be divided into five chapters. In each one of these sections, the fundamental concepts will

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1 of 4 May 2016 [hereinafter GDPR].

[2] Assembly Bill No. 375 of 28 June 2018, the California Consumer Privacy Act of 2018, codified in Title 1.81.5 Part 4 of Division 3 of the Civil Code of California, published on 29 June 2018 [hereinafter CCPA].

[3] Albert Molins Renter, 'Primera ley de privacidad en línea de EE.UU. entra en vigor en California' (La Vanguardia, 5 January 2020) < https://www.lavanguardia.com/vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html> accessed on 20 June 2022.

be defined and analyzed as pertinent for each section. In chapter one, the key definitions upon which these laws are constructed will be reviewed. In chapter two, the scope of application of both regulations will be studied, in particular the material and territorial scope. Chapter three will review the legal basis of each regulation. Chapter four will cover the topic of the rights of users, including the right to erasure, the right to be informed, and the right to access. Finally, chapter five will review the enforcement mechanisms. Within this chapter, first, the monetary penalties in cases of non-compliance will be explained, followed by a review of the civil remedies contemplated in each regulation, including whether non-material damages are compensated and whether punitive damages are awarded within it.

In each chapter, a "consistency rate" will be determined, to understand how alike or not these regulations rule specific matters. Depending on their degree of connection, and the importance of certain similarities or discrepancies, it will be concluded in each topic if these two laws are consistent, fairly consistent, fairly inconsistent, or inconsistent.

"*Consistent means the GDPR and CCPA bear a high degree of similarity in the rationale, core, scope, and application of the provision considered. Fairly consistent means the GDPR and CCPA bear a high degree of similarity in the rationale, core, scope, and application of the provision considered, however, the details governing its application differ. Fairly inconsistent means the GDPR and CCPA bear several differences about the scope and application of the provision considered, however, its rationale and core present some similarities. Finally, inconsistent means the GDPR and the CCPA bear a high degree of difference about the rationale, core, scope, and application of the provision considered*"[4].

[4] Data Guidance One Trust, *Comparing privacy laws: GDPR v. CCPA, 2018, 6* *https://fpf.org/blog/comparing-privacy-laws-gdpr-v-ccpa/* accessed on July 29 2022

2. KEY DEFINITIONS.

2.1 GDPR.

To understand to whom the GDPR is applicable, the concepts and definitions of 'personal data', 'data subject', 'data controller', and 'data processor' delineate the legal grounds to understand to which persons and entities this regulation is applicable.

'Personal data' is defined in Article 4(1)[5], and means any information relating to an identified or identifiable natural person, defined as 'data subject'. Under Article 3[6] it is possible to conclude that a data subject may be any individual whose personal data is processed and does not specifically require that the data subject holds EU residency or citizenship, or is located either within or outside the EU. In this regard, recital 14[7] reinforces two key concepts when analyzing the personal scope of application of the GDPR: first, that the regulation applies only to natural persons and does not extend to legal persons; and, second, that applies to any natural person, with the independence of their nationality or place of residence, about the processing of their personal data. In this same line, Recital 27[8] limits the personal scope of application of this regulation only to living individuals and excludes its application to the personal data of deceased persons, a matter that according to the GDPR must be regulated by each Member State.

The GDPR also applies to 'data controllers'[9] and 'data processors'[10]. The first ones can be defined as natural or legal persons, public authorities, agencies, or other public bodies, who alone or jointly with others, determine the purposes and means of the processing of personal data[11]. The second ones are defined as natural or legal persons, public authorities, agencies, or other public bodies which process personal data on behalf of the controller[12]. It is important to note that according to the GDPR, both of them –the data controllers and data processors- may be in either case, public bodies.

2.2 CCPA.

[5] Article 4(1) GDPR.
[6] Article 3 GDPR.
[7] Recital 14 GDPR.
[8] Recital 27 GDPR.
[9] Article 4(7) GDPR.
[10] Article 4(8) GDPR.
[11] Article 4(7) GDPR
[12] Article 4(8) GDPR.

In the case of the CCPA, the personal scope of application is demarcated by the concepts of 'personal information', 'consumer', 'businesses', and 'service providers'.

First of all, 'personal information' means information that: identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household[13]. Under the CCPA, 'consumer' means a natural person who is a California resident[14]. The term 'resident' for the CCPA must be understood as either (i) every individual who is in the State of California for other than a temporary or transitory purpose; or, (ii) every individual who is domiciled in the State of California who is outside the State for a temporary or transitory purpose[15]. All individuals who fall out of these two categories are nonresidents of the CCPA, and for that reason, they would be out of the scope of this Regulation. It is also important to note that the CCPA addresses whether its protection extends to deceased persons.

Instead of 'data controllers' as defined in the GDPR, the CCPA refers to 'businesses', understood as "*limited sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for profit … that collects consumers' personal information … and does business in the State of California" who must satisfy at least one of the following thresholds: (i) has annual gross revenues in excess of 25 million dollars; (ii) alone or in combination, annually buys, sells, or shares the personal information of 50,000 or more consumers, households or devices; or (iii) derives 50 percent or more of its annual revenues from selling or personal information*[16]. Under the CCPA, businesses are primarily responsible for complying and demonstrating compliance with this regulation[17]. The CCPA also applies to any entity that controls or is controlled by the business[18].

The equivalent for 'data processors' in the GDPR is the 'service providers' in the CCPA. The concept of 'service providers' includes legal entities for profit that process information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose under a written contract[19]. According to the CCPA, service providers have restrictions on how information can be disclosed or

[13] Cal. Civ. Code § 1798.140 (o).
[14] Cal. Civ. Code § 1798.140 (g).
[15] Section 17014 of Title 18 of the California Code of Regulations.
[16] Cal. Civ. Code § 1798.140 (c)(1).
[17] Bukaty, P. (2019) *The California Consumer Privacy Act (CCPA): An implementation guide*. Ely: ITGP. Chapter 1
[18] Cal. Civ. Code § 1798.140 (c)(2).
[19] Cal. Civ. Code § 1798.140 (v).

utilized. For example, service providers are prohibited from retaining, using, or disclosing the personal information they receive for any purpose other than the specified in their services contract[20].

In resume, it can be summarized that the personal scope of application of the CCPA is limited solely to California residents and entities doing business in the state of California, while activities that occur wholly outside of California fall outside of the scope of this Regulation.

2.3 Compared analysis.

When contrasting the key definitions and the personal scope of the GDPR and CCPA, it can be stated that both of them are fairly inconsistent. Between the similarities, it can be observed that both regulations: (i) only protect natural persons and do not cover protection for legal entities; and (ii) define the same way data controller or businesses, by the fact that it establishes the means and purposes of the processing.

However, it is the significance of the differences that permits establishing that these two regulations are fairly inconsistent in terms of personal scope. The main divergences that can be pointed out are the following: (i) Article 3[21] together with Recitals 2[22] and 14[23] provide that the data subject may be any individual whose personal data is processed, and do not specifically require that the data subject holds EU residency or citizenship. As we saw before, the CCPA is only applicable to consumers, who must be California residents within the meaning of Section 17014 of Title 18 of the California Code of Regulations; (ii) data controllers under the GDPR, can have their main activity either for profit or non-profit, they can have any size and they can be private or public entities. On the other hand, for the CCPA to apply to businesses, there are several limitations: it has to be a legal entity for profit, that either alone or jointly with others determines the purpose and means of the processing of consumers' personal information, that does business in the California State[24], and fulfills one of the three thresholds reviewed in the previous section; (iii) when comparing the data controller concept to the businesses one, it can be seen that the GDPR follows an ampler term, which binds to a larger group of data processors, compared to the limited scope of application to the concept of businesses provided by the

[20] Ibid.
[21] Article 3 GDPR.
[22] Recital 2 GDPR.
[23] Recital 14 GDPR.
[24] Cal. Civ. Code § 1798.140 (c)(1).

CCPA; and, finally, (iv) data processors under the GDPR have more obligations, as they face direct enforcement and serious penalties if they do not comply with the regulation, in the example the ones provided in Recital 81[25] and Article 28(1)[26] and (3)[27]. In the case of the CCPA, there are no obligations directed directly to the service providers, other than using the personal information solely at the direction of the business they serve.

[25] Recital 81 GDPR.
[26] Article 28(1) GDPR.
[27] Article 28(3) GDPR.

3. SCOPE OF APPLICATION.

3.1 Material Scope.

3.1.1 GDPR.

Under Article 2(1) [28] the GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system. For this purpose, 'processing' must be understood as any operation or set of operations that are performed on personal data or sets of personal data, whether or not by automated means[29]. Recitals 14[30] to 21[31] are important when analyzing the material scope.

To understand the limits of the material scope, the key concepts of this definition are "automated means", "wholly or partly by automated means" and "part of a filing system".

First of all, automated means it is not defined in the GDPR. However, it can be understood broadly as all procedures in which at least part of the data processing is carried out automatically, using a given program, without further human intervention[32]. The data processed must be fully or partially automated. A data processing activity is understood as partially automated when it is carried on one part manually and on the other automatically[33]. Recital 15[34] aggregates that when manual processing of personal data is not contained or intended to be contained in a filing system, falls out of the scope of this regulation. The rationale behind excluding the purely manual and unstructured processing of personal data is that only the new technologies that emerged through computers and the internet have made it possible to structure and search personal data in a massive systematized way. However, when the data is intended to be part of a filing system, understood as any structured set of personal data which are accessible according to specific criteria (Article 4(6)), even when it is done manually, the collection of such data will immediately be considered within the scope of the regulation, even before it is

[28] Article 2(1) GDPR.
[29] Article 4(2) GDPR.
[30] Recital 14 GDPR.
[31] Recital 21 GDPR.
[32] *Bäcker,* in Wolff, Brink, BeckOK Datenschutzrecht, Article 2 GDPR, margin number 2 (C.H. Beck 2021, 38th edition).
[33] *Bäcker,* in Wolff, Brink, BeckOK Datenschutzrecht, Article 2 GDPR, margin number 3 (C.H. Beck 2021, 38th edition).
[34] Recital 15 GDPR.

organized into a filing system[35]. In this regard, the ruling of the CJEU in the *Jehovah todistagat case*[36] concluded that the definition of "filing system" is fulfilled when "*data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use. For such a set of data to fall within that concept, it is not necessary that they include data sheets, specific lists, or other search methods*"[37].

According to Recital 26[38], the material scope of the GDPR does not apply to anonymous information, as long as this information does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable[39]. On the other hand, pseudonymization does fall under the scope of the GDPR.

In resume, in all of the cases in which the elements contained in Article 2(1)[40] are fulfilled, the GDPR will apply, unless the processing falls under one of the four categories of exemptions indicated in letters a) to d) of paragraph 2 of Article 2, in which case the GDPR would be inapplicable. The exemptions can be resumed into four main categories: (i) Activities that fall outside the scope of the EU Law: the creation of an internal market where, among other things, the free movement of data is guaranteed is one of the primary responsibilities of the EU regulated in the TFEU. Therefore, any data processing actions connected to this objective, whether directly or indirectly, are governed by EU law and therefore excluded from this exemption.

(ii) EU common foreign and security policy: Article 4(2) TFEU provides that "national security remains the sole responsibility of the individual Member States". As a result, all actions about national security, such as the processing of data by intelligence agencies, are not covered by EU legislation. In this regard, Recital 16 GDPR confirms these criteria, as it excludes the application of the GDPR to the processing of personal data by the Member States when carrying out activities about the common foreign and security policy of the EU[41].

[35] Gdpr hub, 'Article 2' (*GDPR Hub*, 4 july 2022) <https://gdprhub.eu/Article_2_GDPR#cite_ref-2> accessed 10 July 2022.
[36] Case C-25/17, *Tietosuojavaltuutettu v Jehovan todistajat* [2018] CJEU.
[37] Ibid, paragraph 62.
[38] Recital 26 GDPR.
[39] Ibid.
[40] Article 2(1) GDPR.
[41] Recital 16 GDPR.

(iii) Processing by a natural person in the course of purely personal or household activities[42]: this exception was originally included under Directive EC/95/46[43], and it has been reiterated in Article 2(2)(c) of the GDPR. This provision manifests that the GDPR does not apply when a natural person processes data solely for domestic or personal purposes. It is key that a natural person carries out the processing for the exemption to be valid. Therefore, the exemption does not apply to processing carried out by legal entities, regardless of their legal structure (including NGOs), and such processing is nevertheless subject to the GDPR. In this topic, it is important to point out that the GDPR does not define "personal" or "household activities". However, the CJEU has interpreted in different cases the scope of applicability of these concepts. For example, in *Ryneš Case*[44], the CJEU followed the Opinion of Advocate General Jääskinen and agreed with his definitions that "personal activities" are those that are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others[45]; and that "household activities" are linked to family life and normally take place at a person's home or in other places shared with family members, such as second homes, hotel rooms or private cars[46]. According to *Ryneš case*, only actions that are performed within the context of a person's private or family life are covered by the exclusion of exclusively personal or household activities. In this regard, an activity cannot be considered to be purely domestic or personal if its goal is to make the data collected accessible to an unlimited number of people or if it extends, even partially, to public space and is thus directed outwards from the private setting of the person processing the data in that way.

(iv) Processing by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties[47]: Directive (EU) 2016/680 now regulates this area.

Lastly, Article 3(3)[48] makes applicable Regulation (EC) No 45/2001 for the processing of personal data by the EU public institutions provided that these regulations

[42] Ibid 33.
[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 2 281/31.
[44] Case C-212/13, Ryneš v Úřad pro ochranu osobních údajů, CJEU [2014], paragraph 33
[45] Case C-212/13, Ryneš v Úřad pro ochranu osobních údajů, CJEU [2014] AG Opinion, para. 51
[46] Ibid., paragraph 56.
[47] Ibid 33.
[48] Article 3(3) GDPR.

comply with the GDPR, and Article 3(4)[49] clarifies that the rules of Directive 2000/31/EC shall not be affected by the rules provided in the GDPR.

In any of the provisions previously reviewed, the GDPR does not make a differentiation between the public and private sectors, thus both of them are covered and fall within the material scope of the regulation.

3.1.2 CCPA.

Unlike the GDPR, the CCPA does not specifically delineate a material scope, but its obligations cover the concepts of 'collecting' 'selling' or 'sharing' personal information, and from such concepts, the material scope of application of this regulation can be determined.

On one hand, 'collecting' under the CCPA means buying, renting, gathering, obtaining, receiving, or accessing any personal information about a consumer by any means[50]. Therefore, it can be concluded that this provision covers all types of operations by which a business acquires personal information, either directly from the consumer or indirectly (e.g. through observation). On the other one, 'selling' includes renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal information for monetary or other valuable consideration[51]. As reviewed earlier in section 2.2, personal information covers information that directly or indirectly relates to or could reasonably be linked to a particular consumer or household. It is out of the scope of the concept of personal information aggregate consumer information[52] and de-identified data[53].

The CCPA has excluded from its applicability the collecting and sharing of certain categories of personal information[54], such as medical information and protected health information,[55] information collected as part of a clinical trial, the sale of information to or from consumer reporting agencies, and publicly available information, between others. The CCPA also excludes several specific processing activities from the definition of selling, including (i) where a consumer uses or directs a business to intentionally disclose

[49] Article 3(4) GDPR.
[50] Cal. Civ. Code § 1798.140 (e).
[51] Cal. Civ. Code § 1798.140 (t).
[52] Cal. Civ. Code § 1798.140 (a).
[53] Cal. Civ. Code § 1798.140 (h).
[54] Bukaty, P. (2019) *The California Consumer Privacy Act (CCPA): An implementation guide*. Ely: ITGP. Chapter 2.
[55] Cal. Civ. Code § 1798.140 (c)(1).

personal information to a third party, via one or more deliberate interactions; (ii) hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party; (iii) sharing with a third parties identifier signals a consumer opt out from selling data; (iv) where a business shares personal information with a service provider that is necessary for a business purpose; and, (v) the transfer of data to a third party in the context of a merger[56].

Another very important limitation to the applicability of the CCPA is that the rights afforded and the obligations imposed on businesses do not apply if they are related to the non-commercial activities of a person[57].

3.1.3 Compared Analysis.

When contrasting the material scope of the GDPR and CCPA, it can be stated that both of them are fairly consistent. The definition of personal data and personal information have similar reach and both exclude certain data from their scope of application, such as anonymous data in the case of the GDPR, and aggregate consumer information and deidentified data in the case of the CCPA. Also, it can be stated that the concept of processing in the GDPR is fairly similar to the collecting and selling concepts regulated in the CCPA. In both regulations, we can find important exclusions. On the other hand, the GDPR excludes from its application the processing of personal data by individuals for purely personal or household purposes. In other words, it excludes any kind of data processing that has no connection to a professional or commercial activity. On the other hand, the CCPA stipulates that the rights afforded and the obligations imposed on businesses do not apply if they are related to the non-commercial activities of a person. Another similarity is that neither of these two regulations is applicable in the law enforcement and national security areas, although they may apply to businesses providing services to law enforcement or national security agencies.

However, there are certain aspects in which the GDPR and the CCPA differ in terms of their material scope of applicability. The GDPR applies to the processing of personal data regardless of the type of processing operation. In the case of the CCPA, it creates requirements for businesses that share or sell information, and to some extent, it includes some requirements for collection (for example, in the CCPA the right to opt-out is only available in the case of selling or sharing personal information). Another

[56] Cal. Civ. Code § 1798.140 (t)(2)(A).
[57] Cal. Civ. Code § 1798.145 (m).

difference is that while the GDPR does not exclude specific categories of personal data from its scope of application, the CCPA specifically excludes from its scope of application the collecting and sharing of some categories of personal information (as explained in section 2.2). Finally, it can be observed that even if both regulations exclude certain processing activities, they are substantively different in terms of what is excluded. In the case of the GDPR, if the processing is conducted through non-automated means that are not part of a filling system, or if the processing is conducted by a natural person for a purely personal or household activity, then they would be out of the scope of the GDPR. In the case of the CCPA, it excludes several specific processing activities from the definition of selling (e.g. sharing with third parties an identifier that signals a consumer opted out from selling data).

Notwithstanding there are certain dissimilarities, the likeness of the key provisions regards this subject, makes it possible to observe that these two regulations are fairly consistent with each other.

3.2 Territorial Scope.

3.2.1 GDPR.

Article 3[58] defines the GDPR's scope in a geographical sense. This provision specifies which sorts of communication with the EU's territory will trigger the GDPR's application and it does so in a way that is both territoriality-dependent and territoriality-independent. These concepts will be explained in the following lines.

The first two paragraphs of Article 3[59] explain the regulation's geographical scope in terms of two key concepts: the "establishment" of a controller or processor in the EU and the "targeting" of data subjects located in the EU. If any of these two conditions are met, the GDPR will apply to personal data processing. The third paragraph states that the GDPR applies to the processing of personal data by a controller who is not based in the EU but is located in a place where Member State Law applies due to public international law.

The GDPR does not define establishment for the purpose of Article 3[60]. However, according to Recital 22[61] 'establishment' implies the effective and real exercise of activity

[58] Article 3 GDPR.
[59] Ibid.
[60] Ibid.
[61] Recital 22 GDPR

through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.[62] The EDPB has pointed out that this concept is coincident with the one found in Recital 19 of DPD, to which the CJEU has reportedly agreed in its interpretation. In synthesis, any controller or processor established outside the EU, that exercises a real and effective activity, through a stable arrangement within the territory of a Member State, will be considered to have an establishment in that Member State.

The second requisite from Article 3(1)[63] is that the processing of personal data is carried out "in the context of the activities" of an establishment in the EU[64]. The CJEU has taken a broad interpretation in this matter. For example, in the *Wirtschaftsakademie case*[65], the CJEU stated (about DPD) that processing carried out in the context of the activities of the controller's establishment "cannot be interpreted restrictively" and that processing "does not require that such processing be carried out 'by' the establishment concerned itself, but only that it be carried out 'in the context of the activities of the establishment"[66].

The EDPB Guidelines 3/2018 on the territorial scope of the GDPR, suggest taking into consideration two factors as key elements in determining whether processing occurs in the context of an establishment in the EU[67]. First, the relationship between a data controller or processor outside the EU and a local establishment in the EU[68]. If a case-by-case analysis of the facts reveals that there is an "inextricable link" between the processing of personal data by a non-EU controller or processor and the activities of his EU facility, EU law will apply to that process[69]. The second factor is revenue-raising in the EU concerning whether or not the local establishment in the EU contributes to the revenues of the non-EU entity[70].

As has been stated before, the location of the processing itself is irrelevant to determining the geographical scope of the GDPR. The geographical location is only

[62] *Zanfir-Fortuna*, in Kuner, Bygrave, Docksey, The EU General Data Protection Regulation (GDPR): A Commentary, Article 3, p. 19 (Oxford University Press 2020).
[63] Article 3(1) GDPR.
[64] C-210/16 - Wirtschaftsakademie v Schleswig-Holstein, CJEU [2018]
[65] Ibid.
[66] Ibid. margin numbers 56-57
[67] EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', 12 November 2019 (Version 2.1), 6
[68] Ibid.
[69] Ibid. 7
[70] Ibid.7

relevant to answering whether a controller or processor is established in or outside the EU and whether a non-EU controller or processor has an establishment in the EU[71].

If neither the controller nor the processor is established in the EU, the GDPR is still applicable if the personal data of individuals located in the EU is being processed. In light of Recital 14[72] and the EDPB guidelines, the GDPR will be applicable anytime that the personal data of a natural person located in the EU is processed as described in Article 3(2)(a) and (b)[73]. So the requirement that the data subject is located in the EU must be assessed at the moment in time when the relevant trigger activity takes place, such as the moment when goods or services are offered, or the moment when the behavior of the data subject is being monitored[74]. In this regard, Recital 14[75] is explicit that the protection is neither limited by residence nor nationality. The processing activities related to data subjects in the EU must have taken place intentionally, rather than inadvertently or incidentally[76].

Finally, the GDPR applies to the processing of personal data by a controller not established in the EU if the Member State's legislation applies by public international law. For example, processing that takes place in a Member State's diplomatic mission or consular post[77].

3.2.2 CCPA.

When examining the territorial scope of application of the CCPA, in a broad sense it can be concluded that this regulation applies to all businesses that do business in California (territorial reach), and, it can be inferred that applies to a business established outside of California if they collect or sell California consumers personal information while conducting businesses in California (extraterritorial reach).

To understand the territorial reach of the CCPA and determine if it is applicable, first it has to be determined if an organization does or does not do business in the State of California. However, the CCPA does not give a precise definition of what it specifically

[71] Ibid. 8
[72] Recital 14 GDPR.
[73] Article 3(2)(a) and (b) GDPR.
[74] Gdpr hub, 'Article 3' (GDPR Hub, 2 march 2022) <https://gdprhub.eu/index.php?title=Article_3_GDPR> accessed 25 July 2022.
[75] Recital 14 GDPR.
[76] EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', 12 November 2019 (Version 2.1), pp. 14-15 (available here).
[77] Recital 25 GDPR.

means to "do business in the State of California". Nevertheless, this concept has been built through relevant case law which guides its applicability[78].

First, a company should review if it is subject to court jurisdiction in the state of California. Under well-established law, one question a court considers before exercising jurisdiction over an out-of-state entity is whether it is purposely availing itself of the privilege of doing business in the state[79]. Typically, an incorporated business entity will be subject to the general personal jurisdiction of its home state. This is generally considered to be the state of incorporation, and/or the place of principal business (i.e. its headquarters)[80]. Many organizations will be subject at the same time to the general jurisdiction of two states as a result of this. For example, if a company is established in Delaware but has its headquarters in California, the company will be subject to both jurisdictions. Independently of this duality of applicable jurisdictions, to establish that a company does business in California according to the rulings reviewed, if a company is either incorporated or has a physical presence in California, it will certainly be subject to the jurisdiction of this state.

The question of the CCPA's extraterritoriality is whether California, as a sovereign state, can apply its laws and regulations to companies established outside the state but operating inside it[81]. These situations are often complex, and critical distinctions in a case can rely on individual factual circumstances. When delimiting the scope of the applicability of the CCPA to companies operating out of the boundaries of the State of California, the question arises, what if a business is not operating within the physical confines of the state but maintains a limited amount of business connections with California consumers? How many connections with California consumers are necessary for a California law to apply to an organization based in another state?[82]

When US courts fail to establish general jurisdiction, they then look to specific jurisdiction. Specific jurisdiction relates to the number of contacts that a defendant has with a state[83]. Based on the actions of the defendant -either by working within the state or dealing with residents – a sufficient level of contact is established to grant the local

[78] Bukaty, P. (2019) *The California Consumer Privacy Act (CCPA): An implementation guide*. Ely: ITGP. Chapter 1.
[79] United States Court of Appeals, Ninth Circuit, BOSCHETTO v. D. HANSING and others, No. 06-16595, August 20, 2008.
[80] US Supreme Court, Daimler AG. v. Bauman et al., 571 U.S. 2014.
[81] Ibid. 75
[82] Ibid. 75
[83] Ibid. 75

court jurisdiction over the out-of-state defendant. The U.S. Supreme Court answered what is a sufficient level of contact in the *Bristol-Myers Squibb Co. v. Superior Court (Anderson) case*[84]. In this case, the Court stated that the mere fact that other plaintiffs were prescribed, obtained, and ingested Plavix in California—and allegedly sustained the same injuries as did the non-residents—does not allow the State to assert specific jurisdiction over the nonresidents' claims[85].

The Court explicitly noted that there must be "a connection between the forum and the specific claims at issue."[86] In this case, the relevant plaintiffs were non-California residents: "all the conduct giving rise to the nonresidents' claims occurred elsewhere," and the plaintiffs did not "claim to have suffered harm in that State. […] It follows that the California courts cannot claim specific jurisdiction."[87]

Taking into consideration the United States Supreme Court ruling, it may be interpreted that California laws will apply to an organization established outside the state based on specific personal jurisdiction if the plaintiffs at issue are California residents who claim to have suffered harm in the state[88]. That is if the claims at issue arise from the defendant's activities in the state. Of course, the laws will also apply if the organization is established in California (i.e. general jurisdiction by physical presence). Therefore, whether a business is "doing business in the state of California" – and consequently whether the CCPA applies to an organization – hinges on whether the organization maintains a physical presence in the State or the degree to which California residents suffer harm in the State.

Finally, it is important to note that the CCPA does not prevent an organization from collecting or selling a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California[89].

3.2.3 Compared Analysis.

When contrasting the territorial scope of the GDPR and CCPA, it can be stated that both of them are fairly inconsistent. The most relevant similarity between these regulations is that both of them have an extraterritorial factor. However, the way they are

[84] Bristol-Myers Squibb Co. v. Superior Court of California, 582 U.S. [2017].
[85] Walden, 571 U. S., (slip op., at 8)
[86] Ibid 81, 8.
[87] Ibid.
[88] Ibid 75.
[89] Cal. Civ. Code § 1798.145 (a)(6).

regulated differs. In the case of the GDPR, is regulated that it applies to organizations that do not have any presence in the EU, but that offer goods, and services or monitor the behavior of persons in the EU. In the case of the CCPA, as reviewed the concept of extraterritoriality applies with a narrower scope, for those organizations "doing business in California".

Another difference is that the obligations imposed on businesses by the CCPA do not restrict a business's ability to "*collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California [...] Commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California was sold*[90]. There is no provision similar to this concept in the GDPR.

[90] Cal. Civ. Code § 1798.145 (a)(6).

4. LEGAL BASIS.

4.1 GDPR.

Article 6[91] regulates the lawfulness of the processing. The 'processing' is defined in the GDPR as operation(s) which are performed on personal data or on sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[92]. Independently of the way the personal data is processed, to be considered lawful under the GDPR, it has to fall upon any of the six limited categories described in Article 6(1)(a) to (f)[93] which are the following:

(i) The data subject has given consent to the processing of his or her personal data for one or more specific purposes. Under the GDPR, consent must satisfy different requirements to be legally binding. According to Article 4(11)[94], consent must be freely given, specific, informed, and unambiguous. Furthermore, under Article 7[95], consent must be requested in an intelligible and easily accessible form, using clear and plain language[96]. It is also an essential condition of consent that it is withdrawable at any time[97]. In the case of children (16 years or below that age) Article 8[98] regulates specific conditions applicable for them to give lawful consent.

(ii) Processing is necessary for the performance of a contract. For this case, the processing will be considered lawful if two conditions are met: (a) the contract between the data subject and controller is valid, and (b) the specific processing is necessary for the performance of the contract[99].

[91] Article 6 GDPR.
[92] Ibid.
[93] Ibid (a) to (f) GDPR.
[94] Article 4(11) GDPR.
[95] Article 7 GDPR.
[96] Article 7(2) GDPR
[97] Article 7(3) GDPR
[98] Article 8 GDPR. GDPR Hub,
[99] Gdpr hub, 'Article 6 ' (GDPR Hub, 25 april 2022) <https://gdprhub.eu/index.php?title=Article_6_GDPR> accessed 28 july 2022

(iii) Processing is necessary for compliance with legal obligations to which the controller is subject. The legal obligation to which the controller is subject must originate directly from the law and not from a contractual arrangement[100].

(iv) Processing is necessary to protect the vital interests of the data subject or another natural person. Recital 46[101] clarifies that a vital interest is "essential for the life" of the data subject[102].

(v) Processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller[103].

(vi) Processing is necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The GDPR provides data subjects with a right to withdraw consent at any time as well as a right to object if their personal data is processed based on a legitimate interest or performing a task in the public interest.

A notable case that permits us to have a clearer view of how the CJEU interprets what is valid consent, is the Orange Romania case[104]. Orange România is a provider of mobile telecommunication services in the Romanian market. The Romanian National Data Protection Authority has charged Orange România with administrative sanctions under Article 32 of the Romanian Data Protection Act on the grounds that copies of customer identification documents were obtained and stored without their express consent. The DPA also instructed the administrator to destroy any existing copies of her IDs.[105] Moreover, Orange România asked its customers for their consent to this data processing and allowed them to decline their consent in written form. Some mobile service agreements included a pre-checkbox indicating consent to retain a copy of the ID card, while others did not. Customers were required to complete an additional form before signing the contract to indicate that they did not agree to keep a copy of their ID card.

[100] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN, 9 April 2014, 19.
[101] Recital 46 GDPR
[102] Ibid.
[103] Ibid.
[104] Case C-61/19, Orange România SA v ANSPDCP, CJEU [2020]
[105] Gdpr hub, 'CJEU - C-61/19 - Orange Romania' (*GDPR Hub*, 26 november 2020) <https://gdprhub.eu/index.php?title=CJEU_-_C-61/19_-_Orange_Romania> accessed 31 July 2022

Orange România appealed against the Romanian National Data Protection Authority's decision before the Regional Court of Bucharest, which then requested the CJEU's preliminary ruling on the following two questions:

'(1) *For the purposes of Article [2](h) of Directive 95/46, what conditions must be fulfilled in order for an indication of wishes to be regarded as specific and informed?*

(2) For the purposes of Article 2(h) of Directive 95/46, what conditions must be fulfilled in order for an indication of wishes to be regarded as freely given?'[106]

The CJEU ruled that "*Article 2(h) DPD must be interpreted as meaning that it is for the data controller to demonstrate that the data subject has, by active behavior, given his or her consent to the processing of his or her personal data and that he or she has obtained. Moreover, it stated that a contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent, as provided for in those provisions, to that collection and storage, where: (i) the box referring to that clause has been ticked by the data controller before the contract was signed; or (ii) where the terms of that contract are capable of misleading the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data; (iii) or where the freedom to choose to object to that collection and storage is unduly affected by that controller, in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal*[107].

4.2 CCPA.

The CCPA does not set a list of legal grounds to which businesses must adhere before collecting, selling, and disclosing personal information, and only provides for a *posteriori* mechanism, which allows customers to opt-out to the sale and disclosure of

[106] Ibid 101
[107] Ibid 101

their personal information or to ask for the erasure of their information. The right to opt out of the sale or sharing of personal information is regulated in section 1798.120[108].

Under the CCPA rules, once a business has received direction from a consumer not to sell or share his/her personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, it is prohibited for this business to sell or share the consumer's personal information[109]. It is important to point out two things in this regard: (i) in the case a consumer opts out the business will only be able to sell, share or disclose personal information if the consumer gives their explicit permission; and, (ii) that the consent requirement is only mandatory in the CCPA for the selling of the minor's personal information, and not for the collecting of such information.

'Consent' under the CCPA means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, agrees to the processing of personal information relating to the consumer[110]. It does not constitute consent to the acceptance of (i) general or broad terms of use; (ii) hovering over, muting, pausing, or closing a given piece of content does not constitute consent; or, (iii) any kind of agreement obtained through use of dark patterns.

4.3 Compared analysis.

From the descriptions given before, it can be stated that the way the legal basis of the processing is regulated in the GDPR and CCPA is inconsistent. Between the few similarities, it can be noted that they have somehow regulated alike the right to withdraw and the right to object (GDPR) to the right to opt out (CCPA). Also, both regulations permit under special conditions the processing of children's information.

However, the fact that the GDPR states that data controllers can only process personal data when there is a legal ground for it (limited list of grounds, see 4.2) and that the CCPA does not list the legal grounds based on which businesses can collect and sell personal information, it makes them inconsistent in the way they regulate the legal basis for processing in each regulation.

[108] Cal. Civ. Code § 1798.120.
[109] Ibid(d).
[110] Cal. Civ. Code § 1798.140(h).

5. RIGHTS OF USERS.

5.1 Right of erasure – Right to deletion.

5.1.1 GDPR.

Article 17(1)[111] together with Recitals 65[112] and 66[113] establish that data subjects have the right to request the data controllers to have their personal data erased in certain circumstances without undue delay, and that data controllers have the obligation to erase this information upon this request. This is known as the right to erasure, or the "right to be forgotten", and is regarded as one of the particular novelties introduced by this regulation from its predecessor the DPD. The inclusion of this right for the data subjects "*recognizes its increased importance in today's society, in which personal data is generated, made public, and shared on a massive scale, as an instrument for the data subject to retain a certain control over personal data*."[114]

A major precedent that informed the GDPR's right to erasure was the interpretation of Articles 12(b) and 14(1)(a) of the DPD by the CJEU in its landmark judgment G*oogle Spain*[115]. In this ruling, one of the key components of the right to erasure was established: the "right to request delisting". The CJEU ordered the removal of possible any links between documents and information relating to the names of data subjects from search results. This means, the Court recognized that data subjects may ask search engines to remove certain URLs from their search results if the online information is "inadequate, irrelevant or irrelevant or excessive" [116]. As a direct result of this case, in 2020, the EDPB adopted the "Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR" [117] to define the content and scope of the "Right to Request Removal".

[111] Article 17(1) GDPR
[112] Recital 65 GDPR.
[113] Recital 66 GDPR.
[114] Zanfir-Fortuna, in Kuner Bygrave, Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Article 17 GDPR, (Oxford University Press 2020) 477.
[115]Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos, CJEU [2014].
[116] Ibid, margin numbers 93-94.
[117] EDPB, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)', 7 July 2020

In order data subjects may exercise the right to erasure, at least one of the following legal grounds has to apply, which in in turn gives rise to a correlated obligation on the data controller:

(i) The data is no longer necessary for its original purpose and has no new lawful purpose:

The legal basis for this is Article 5(1)(b) and (e) respectively. Article 6(4) provides that certain factors are necessary for the controller to determine whether the further processing is consistent with the purposes for which the personal data were originally collected. In order for this new processing to be considered lawful, it must be taken into account[118];

(ii) The legal basis for processing is the consent of the data subject. If the data subject withdraws this consent, there are no other possible legal grounds. According to Article 7(3), the data subject can withdraw their consent at any time and withdrawing this consent must be as simple as giving consent. Further processing of personal data after withdrawal of consent renders this processing operation unlawful and requires the data controller to delete the personal data upon request[119];

(iii) The data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing. The data subject may request erasure in the event of an objection pursuant to Article 21(1). This establishes the right of objection arising from the particular situation of the data subject where the processing is necessary for the performance of the tasks specified in Article 21(1). In either case, the data controller bears the burden of proving whether compelling legitimate grounds exist. However, the data subject must prove the circumstances that led to the change of interest[120].

(iv) The data has been processed unlawfully; or

(v) Erasure is necessary for compliance with EU law or the national law of the relevant member state.

The GDPR provides as a general rule that data subjects should be able to exercise the right of erasure free of charge[121]. However, there are certain exemptions to this rule where data subjects do have to pay some fees (for example, when the requests are unfounded, excessive, or have a repetitive character). In this regard, data controllers must

[118] Gdpr hub, 'Article 17' (*GDPR Hub*, 21 october 2021) <https://gdprhub.eu/Article_17_GDPR> accessed 6 june 2022
[119] Ibid.
[120] Ibid.
[121] GDPR Recital 59 and Article 12(5).

have in place mechanisms to ensure that the request is made by the data subject whose personal data is to be deleted. For example, the controller should provide data subjects with means for requests to be made electronically, especially where personal data has been processed in this form.

The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month. In case they do not intend to comply with the data subjects' requests, in this same communication they should give reasons for why they do not intend to do so.

When the controller has made the personal data public, the controller is obliged to take reasonable steps to inform others processing the personal data that the data subject has requested the deletion of its personal data[122].

Finally, there are certain exceptions to the right of erasure considered in the GDPR. These exceptions are the following: a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation that requires processing by EU or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health; (d) for certain research purposes or statistical purposes; or (e) for the establishment, exercise or defense of legal claims[123].

5.1.2 CCPA.

In the CCPA, the right to deletion is regulated as the right that consumers have towards businesses to request them to delete any personal information they have collected from them[124]. In this regard, businesses have a series of obligations when collecting the personal information of consumers. First and most important is that when they collect personal information about the consumers, they are obliged to disclose to consumers that they have the right to request the deletion of their personal information if needed or wanted[125]. Another obligation that businesses have, is that upon the reception of a verifiable consumer request to delete his personal information, the business not only has to delete the consumer's personal information from its records but also has to notify any

[122] Article 17(2) GDPR.
[123] Article 17 GDPR.
[124] Cal. Civ. Code § 1798.105 (a)
[125] Cal. Civ. Code § 1798.105 (b)

service providers, contractors, or third parties to whom the business has sold or share the personal information in order they delete the consumer's personal information from their records too[126].

It is important to note that the right to deletion is not an absolute one, as the organization can continue to hold a consumer's personal information if it is necessary for several purposes. The CCPA recognizes there may be situations where organizations cannot realistically delete data. In resume, the exceptions are the following: (i) neither a business nor a service provider needs to comply with a request for deletion if the information is needed to complete a transaction, provide a good or service, or otherwise perform a contract between the business and the consumer; (ii) detected security incidents or the information is needed to protect against malicious, deceptive, fraudulent, or illegal activity; (iii) debug to identify and repair errors that impair existing intended functionality; (iv) exercise free speech; engage in scientific, historical, or statistical research in the public interest; (v) comply with a legal obligation; (vi) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the businesses; and/or, (vii) to use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information[127].

The CCPA does not limit the scope of this right to specific situations, categories of personal information, or purposes. The right to deletion generally applies to personal information that a business has collected from the consumer and it seems that the consumer does not have to justify his or her request. The CCPA establishes that businesses have to provide at least two different methods to consumers for submitting requests to delete their personal data[128]. Bylaw, as a minimum all businesses have to provide a toll-free telephone number that the consumers may call; and if the businesses maintain an internet website, a website address.

Finally, once a consumer has requested a business to delete its personal information, the deadline to answer this request is of 45 days from the receipt of the

[126] Cal. Civ. Code § 1798.105 (c)
[127] Cal. Civ. Code § 1798.105(d)(1)-(9)
[128] Cal. Civ. Code § 1798.130

consumer's request. The deadline can be extended an additional 45 days when reasonably necessary if the consumer is informed within the first 45 days[129].

5.1.3 Compared Analysis.

Like the GDPR, the CCPA confer individuals the right to request the deletion of their personal information, unless exceptions apply. Under the CCPA, the right applies to personal information that has been "collected" from the consumer. The core of this right is quite similar in both pieces of legislation, however, its scope, applicability, and exemptions vary. It is worth noting that some exceptions are the same under both laws, for example, freedom of speech, and processing of personal data for research purposes if the erasure of that data would impair the objectives of the research and establishing or exercising legal claim. Because of the proximity between how both rules regulate the right to be forgotten, it can be established that these two provisions are fairly consistent.

As to their most important commonalities, it can be pointed out: (i) that the scope of this right is not limited to the data controller/business that collects personal data, but also impacts third parties who may also have to comply with the erasure requests; (ii) a general rule, this right can be exercised free of charge for data subjects/consumers. Both regulations also agree that certain fees should apply to the data subject/consumer when the requests are unfounded, excessive, or have a repetitive character; (iii) the GDPR and the CCPA impose data controllers/businesses the obligation to have mechanisms to ensure that the request is made by the data subject/consumer who's personal information is to be deleted; and, (iv) lastly, both have provided as exceptions to the right of erasure the freedom of expression, processing for research purposes and if the deletion of the personal data would impair the objectives of the research, the establishment exercise or protection against illegal activities, and lastly, both contemplate the exception of complying with a legal obligation.

When it comes to differences between the two regulations, the main ones to point out in this section are the following: (i) the right to erasure in the GDPR only applies if any of the following grounds apply, in contrast, the CCPA does not limit the scope of this right to specific situations, categories of personal information or purposes; (ii) the period that the GDPR and CCPA contemplate for a response to the data subject/consumer once they have request their data is deleted is different. In the case of the GDPR, the data

[129] Cal. Civ. Code § 1798.130 (a).

subject must receive an answer within 1 month from the receipt of the request, as the CCCP gives 45 days as the time of response; (iv) within the exemptions, both regulations have certain rules that cannot be found in the other one. For example, in the GDPR, a data controller is exempted to comply with the erasure request for reasons of public interest in the area of public health, the CCPA does not have any rule like this. In the case of the CCPA, businesses are not required to comply in cases such as performing a contract between a business and the consumer, data security incidents, and debugging to identify and repair errors that impair existing intended functionality, among others.

5.2 Right to be informed.

5.2.1 GDPR

In the GDPR, transparency is envisaged as an overarching concept that governs several other data protection rights and obligations[130], including Articles 13 to 15[131] on information and access to personal data. There is a need for transparency regarding the gathering and use of data to allow EU citizens to exercise their right to the protection of personal data. Therefore, the GDPR gives individuals a right to be informed about the collection and use of their personal data, which leads to a variety of information obligations by the controller[132].

The law differentiates between two cases: on the one hand, if personal data is directly obtained from the data subject (Article 13[133]) and, on the other hand, if this is not the case (Article 14[134]). In any case, data controllers cannot collect and process personal data for purposes other than the ones about which the consumer was informed unless they provide them with further information.

When data is obtained directly from the data subjects, the person must be immediately informed at the time the data has been obtained. In terms of content, and to ensure a uniform and sufficient level of information for the data subjects, the GDPR lists the data controller's obligations to inform. Usually, this information is provided by controllers to data subjects as an online data protection notice, which is commonly referred to as a privacy policy or privacy notice. Regardless of the format of the notice or

[130] Article 5(1)(a) GDPR
[131] Article 13 to 15 GDPR.
[132] Intersoft consulting, 'Right to be Informed' (*GENERAL DATA PROTECTION REGULATION (GDPR)*, 08 June 2020) <https://gdpr-info.eu/issues/right-to-be-informed/> accessed 17 October 2022
[133] Article 13 GDPR
[134] Article 14 GDPR.

the method of transmission, Article 13(1)[135] provides that the information should be provided "at the time when personal data are obtained"[136]. The attention of the data subject should be drawn to the existence of the notice, and the latter must be easily accessible and distinguishable from other information, such as the terms of use of a website or the clauses of a contract[137]. What remains essential in any case is for the information to be accessible to the data subjects before the moment the personal data has been obtained.

With respect to content, the right to information includes the identity of the processor, the contact details of the data protection officer (where available), the purposes and legal basis of the processing, the legitimate interests pursued and the recipients of the transfer. This includes the processor's obligation to provide information about of personal data and the intention to transfer personal data to third countries. In addition, this right includes information on retention periods, data subject rights, possibility to withdraw consent, right to lodge a complaint with authorities and whether the provision of personal data is obliged by law or contract. Also, data subjects must be informed of all automated decision-making activities, including profiling. Only if the data subject is already aware of the above information does not need to be provided[138].

If personal data is not collected from the data subject, he must be notified within a month. If the information collected is used to contact the data subject directly, he/she has the right to be notified immediately upon contact. In terms of content, the officer must provide the same specific information as if the personal data were collected directly from the data subject. The only exception to this is information regarding the obligation to provide personal data. Because in this case, the controller has no decision-making authority. Furthermore, the responsible party is obliged to communicate the origin of the personal data and whether they were publicly accessible. Data subjects have the right to be informed in a format that is precise, transparent, comprehensible, and easily accessible form. Information obligations can be fulfilled in written or electronic form[139].

[135] Article 13(1) GDPR.
[136] 'Guidelines on Transparency under Regulation 2016/679', 18
[137] *Zanfir-Fortuna*, in Kuner, Bygrave, Docksey, The EU General Data Protection Regulation (GDPR): A Commentary, Article 13, p. 427 (Oxford University Press 2020).
[138] Intersoft consulting, 'Right to be Informed' (*GENERAL DATA PROTECTION REGULATION (GDPR)*, 01 January 2019) <https://gdpr-info.eu/issues/right-to-be-informed/> accessed 8 june 2022
[139] Ibid.

In resume, in the case of Article 13[140] and Article 14[141], the GDPR states that information must be provided to individuals concerning: (i) the categories of personal data processed; (ii) the purposes of the processing; and (iii) the existence of data subject's rights and the contact details of the DPO.

5.2.2 CCPA.

The right to notice at collection means that businesses are required to give consumers certain information about the categories of personal information they collect about them and the purpose for which they use the different categories of information. Businesses must also provide a link to the businesses' privacy policy which describes the businesses' privacy practices and consumer privacy rights.

According to section 100 of the CCP, it is a requirement that any business that collects consumers' personal information must inform them at the time of the collection of the different categories of personal information that have been collected, and the purposes for which the information will be used. According to the CCPA, the data privacy policy or data processing notices must include the following: (i) a description of consumer rights, under sections 1798.110, 1798.115, and, 1798.125[142]; (ii) a description of the method for submitting verifiable consumer requests; (iii) a list of categories of information and the purpose for which those categories will be used[143]; a list of categories of information that may be sold or disclosed for a business purpose[144].

Moreover, data privacy policies or data processing notices should explain the following: (i) the categories of sources from which personal information is collected[145]; (ii) the categories of third parties with whom the business shares personal information[146]; and, the business or commercial purpose for collecting or selling personal information[147].

Finally, the CCPA contemplates a specific requirement, which is that consumers must receive explicit notice when a third party intends to sell personal information about them[148].

---

[140] Article 13 GDPR.
[141] Article 14 GDPR.
[142] Cal. Civ. Code 1798.130(a)(5)(A)
[143] Cal. Civ. Code 1798.100(b)
[144] Cal. Civ. Code 1798.130(a)(5)(C)
[145] Cal. Civ. Code 1798.100(a)(2)
[146] Cal. Civ. Code 1798.100(a)(4)
[147] Cal. Civ. Code 1798.100(a)(3)
[148] Cal. Civ. Code 1798.115(d)

5.2.3 Compared analysis.

The scope of disclosures required by the GDPR is broader and extends beyond the ones required by the CCPA, as most of the types of information required to be disclosed by the CCPA are also required to be disclosed under the GDPR. Both regulations prescribe when information must be given to the individuals and what they must be informed of. In general, the similarities between these two regulations can be seen in various aspects of how they regulate the transparency rights of information for individuals, it can be said that both regulations are fairly consistent. More specifically, both legislations state that information regarding the categories of personal data, the purposes of the processing, and the existence of the data subject's rights must be provided to the individuals. Also, both regulations set a common standard which is that the information must be given to the individuals at the moment data is obtained or collected. Finally, another similarity found in both laws is the prohibition for data controllers and businesses respectively to collect and process data for other purposes than the ones informed, unless they provide further information to the individuals.

However, there are some subtle differences between the GDPR and CCPA. For example: (i) while the GDPR undoubtedly requires disclosure if personal data is being sold, it does not include very prescriptive obligations of the kind reflected by the CCPA; (ii) the CCPA requires some disclosures only in respect of the previous 12 months, whereas the GDPR has no such limitation; and (iii) while both the GDPR and the CCPA require the disclosure of the rights available to applicable individuals, the rights themselves are also not identical.

5.3 Right of access.

5.3.1 GDPR.

The right to access plays a central role in the GDPR. First, only this right allows the data subject to exercise further rights such as rectification and erasure. Second, due that an omitted or incomplete disclosure is subject to fines.

The right of access under Article 15(1)[149] includes three components: (i) the right to obtain confirmation from the controller as to whether data concerning them are being processed; (ii) the right to obtain access to the personal data undergoing processing; and, (iii) the right to obtain information on certain aspects of the processing as outlined in the

[149] Article 15(1) GDPR.

list under Article 15(1)(a-h)[150]. It is important to note, the GDPR does not impose any requirements regarding the form of the request by which the data subject or their authorized representative exercises the right of access[151].

The data subject may define the scope of their request and does not need to outline the reasons behind it. Even if they did, the controller does not have the jurisdiction to assess their reasons[152]. However, if the request is unclear and a large amount of data is being processed, the controller may ask the data subject to specify what processing activities the request relates to (Recital 63[153]). If the data subject nonetheless requests access to all their personal data, the controller has to provide this information[154], as confirmed by the EDPB[155] and national courts[156].

The answer to a right of access request includes two components. The first one consists of the right of the data subject to receive a confirmation about whether his/her personal data has been processed. The search for personal data should be performed on all the paper and computer records where personal data has been processed, including the controller's backup systems[157]. The controller should respond with a confirmation even if no personal data has been processed. For this purpose, the controller should check whether the personal data of the person seeking information is being processed. If the processor's answer is affirmative, the second step may include information about the purposes of the processing, the categories of personal data to be processed, the recipients or categories of recipients, the intended retention period or its criteria, etc., which includes a full range of information. Information about the data subject's rights, such as definitions, information about rectification, deletion or restriction of processing, right to object, right to lodge a complaint with an authority, information about the origin of the data[158].

---

[150] Article 15(1)(a-h) GDPR.
[151] EDPB, 'Guidelines 01/2022 on data subject rights - Right of access', 18 January 2022 (Version 1.0), 21
[152] Gdpr hub, 'Right of access by the data subject' (*Article 15 GDPR*, 08 December 2021) <https://gdprhub.eu/Article_15_GDPR#cite_ref-6> accessed 22 October 2022
[153] Recital 63 GDPR.
[154] *Zanfir-Fortuna*, in Kuner, Bygrave, Docksey, The EU General Data Protection Regulation (GDPR): A Commentary, Article 15 GDPR, p. 465 (Oxford University Press, Oxford, 2020).
[155] Ibid. 148
[156] Rechtbank Noord-Holland, 18 June 2021, AWB - 20 _ 4638
[157] EDPB, 'Guidelines 01/2022 on data subject rights - Right of access', 18 January 2022 (Version 1.0), p. 35
[158] Intersoft consulting, 'Right of Access' (*GENERAL DATA PROTECTION REGULATION (GDPR)*, 01 January 2019) <https://gdpr-info.eu/issues/right-of-access/> accessed 8 June 2022

The second component of the right of access is the right to receive a copy of all personal data undergoing processing[159]. The scope of the provision reflects the definition of personal data provided for in Article 4(1)[160]. According to the EDPB, this includes, inter alia, special categories of personal data[161]; personal data relating to criminal convictions and offenses[162]; data knowingly and actively provided by the data subject (e.g. account data submitted via forms, answers to a questionnaire); observed data or raw data provided by the data subject by their use of the service or device (e.g. data processed by connected objects, transactional history); data derived from other data, rather than directly provided by the data subject (e.g. credit score, country of residence derived from postcode); data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules); and pseudonymized data as opposed to anonymized data[163].

Finally, the GDPR has set several limits to the right of access. For example, this right is constrained by Article 15(4)[164] (rights and freedoms of others) and Article 12(5)[165] (manifestly unfounded or excessive requests). Furthermore, EU or Member State law may restrict the right of access by Article 23[166]. Derogations regarding the processing of personal data for scientific, historical research, statistical or archiving purposes in the public interest can be based on Articles 89(2)[167] and 89(3)[168] accordingly, as well as for processing carried out for journalistic purposes and academic artistic or literary expression on Article 85(2)[169].

5.3.2 CCPA

This right is reiterated in a few places throughout the CCPA. The first is in section 100[170]: "*a consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific*

[159] Article 15(3) GDPR.
[160] Article 4(1) GDPR.
[161] Article 9 GDPR.
[162] Article 10 GDPR.
[163] EDPB, 'Guidelines 01/2022 on data subject rights - Right of access', 18 January 2022 (Version 1.0), 31
[164] Article 15(4) GDPR.
[165]Article 12(5) GDPR.
[166] Article 23 GDPR.
[167] Article 89(2) GDPR.
[168] Article 89(3) GDPR.
[169] Article 85(2) GDPR.
[170] Cal. Civ. Code § 1798.100

pieces of personal information the business has collected."[171] A consumer shall have the right to request that a business that collects personal information discloses the following: *(i) the categories of personal information it has collected about that consumer; (ii) the categories of sources from which the personal information is collected; (iii) the business or commercial purpose for collecting or selling personal information; (iv) the categories of third parties with whom the business shares personal information; (v) the specific pieces of personal information it has collected about that consumer*[172]. This information must be disclosed to the consumer upon receipt of a verifiable consumer request.

In addition to responding to requests, any business that collects consumer personal information is required to inform consumers at the time of collection as to the categories of personal information to be collected and the purposes for which the information will be used[173]. Additional information cannot be used without providing consistent, similar notice.

When an organization sells consumers' personal information, they have specific requirements that can be found in section 115[174]. In this case, upon receipt of a verifiable consumer request, a business that sells personal information must disclose to the consumer[175]: (i) the categories of personal information that the business collected about the consumer; (ii) the categories of personal information that the business sold about the consumer; (iii) the categories of third parties to whom the personal information was sold (by category of personal information for each third party); and (iv) the categories of personal information that the business disclosed about the consumer for a business purpose. As can be seen, the requirements for organizations that sell personal information are substantially similar to those in sections 100[176] and 110[177], which detail the information that must be provided by organizations that simply collect personal information. In either case, organizations processing personal information should be prepared to respond to requests for information relating to the types of information listed above.

[171] Cal. Civ. Code § 1798.100(a)
[172] Bukaty P, *The California Consumer Privacy Act (CCPA): An Implementation Guide* (ITGP 2019), chapter 5.
[173] Cal. Civ. Code § 1798.100(b)
[174] Cal. Civ. Code § 1798.115
[175] Cal. Civ. Code § 1798.115(a), (1)-(5)
[176] Cal. Civ. Code § 1798.100
[177] Cal. Civ. Code § 1798.110

Any organization that collects or sells personal information will have to comply with section 130[178] concerning the response to "right of access" requests. This section requires two things:

(i) that the organization provides at least two designated methods that allow consumers to submit requests for information, "including, at a minimum, a toll-free telephone number, and if the business maintains an internet website, the website address. [179]"; and

(ii) that the organization provides the required information to the consumer free of charge within 45 days of receiving the request[180]. Although the organization is required to "promptly take steps to determine whether the request is a verifiable consumer request," this does not affect the 45-day window[181]. Ultimately, the total time to respond is 45 days after receipt. This period may be extended once, by an additional 45 days, provided the consumer is given notice of the extension within the first 45-day period[182].

Organizations only have to provide information related to the past 12 months[183]. The response is to be made in writing and delivered through either the consumer's account or at the consumer's option (again a compelling reason to consider creating a consumer account portal were requests for information can be collectively tracked and stored, although it should be noted that organizations cannot require a consumer to make an account to make a verifiable consumer request[184]). Organizations are also not obligated to reply to the same consumer request more than twice in 12 months[185].

The CCPA requires responses to verifiable consumer requests to be provided "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance."[186] Considering this requirement applies to both categories and specific pieces of information, organizations must be able to respond completely to consumer requests, which means that they must be able to identify and gather the necessary information, and provide it to the consumer in the appropriate format.

[178] Cal. Civ. Code § 1798.130
[179] Cal. Civ. Code § 1798.130(a)(1)
[180] Cal. Civ. Code § 1798.130(a)(2)
[181] Ibid.
[182] Ibid.
[183] Cal. Civ. Code § 1798.130(a)(2)
[184] Ibid.
[185] Cal. Civ. Code § 1798.130(b)
[186] Cal. Civ. Code § 1798.130(a)(2)

On March 10, 2022, in its first formal opinion interpreting the CCPA compliance obligations, the California Attorney General answered the question addressed to him:

> *"does a consumer's right to know the specific pieces of personal information that a business has collected about that consumer apply to internally generated inferences the business holds about the consumer from either internal or external information sources?*[187]

In summary, the CA AG concluded that "*internally generated inferences that a business holds about a consumer is personal information within the meaning of the CCPA, and must be disclosed to the consumer on request. A business that withholds inferences on the ground that they are protected trade secrets bears the ultimate burden of demonstrating that such inferences are indeed trade secrets under the applicable law*"[188].

5.3.3 Compared analysis.

As observed the GDPR and the CCPA establish a right of access that allows individuals to have full visibility of the data an organization holds about them. Under both laws, they can obtain details about the data which has been processed, but also copies of the data items themselves. The core of this right is fairly consistent between the two regulations.

The first similarity is how data controllers/businesses have to respond to an access request. In the case of the GDPR, a data controller must indicate the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipients to whom personal data have been disclosed; and any sources from which data was collected. The GDPR specifies that individuals also have the right to receive a copy of the personal data processed about them. This is pretty similar to the CCPA, as a business must indicate the categories of personal information collected/sold; the categories of sources from which the personal information is collected; the business or commercial purpose for collecting or selling personal information; and the categories of third parties with whom the business has shared personal information.

---

[187] Rob Bonta, Opinion of Attorney General, *REPORTS OFFICE OF THE ATTORNEY GENERAL State of California*, 10 March 2022, 1
[188] Ibid, 15.

Both regulations provide that data subjects must have a variety of means through which they can make their request. Also, both of them specify that data controllers/businesses must have mechanisms to ensure that the request is made by the data subject/consumer whose personal data is requested access to. Finally, both laws state that data subjects/consumers can exercise this right free of charge, and both regulate specific exceptions to this rule.

The most notable differences are the following: (i) the scope of application in the GDPR is wider than in the CCPA. Under the GDPR, the right applies to all the personal data collected and processed about the data subject making the request; in the CCPA the right applies only to personal information collected in the 12 months before the request; (ii) in the GDPR, data controllers can refuse to act on a request when it is manifestly unfounded, excessive or has a repetitive character, in the CCPA businesses are not required to provide access to personal information more than twice in 12 months; (iii) in the GDPR, data subjects' requests must be complied without undue delay and in any event within 1 month from the receipt of the request, and the deadline can be extended for an additional of 2 months. In the CCPA, the deadline to respond to such a right is 45 days of receipt of the consumer's request, with the possibility to be extended an additional 45 days; and, (iv) the GDPR has a distinct right to data portability, as the CCPA states that when businesses provide data electronically to the consumer this data should be sent in a portable and readily usable format that allows for the transmission of this data to third parties.

6. ENFORCEMENT.

6.1 Monetary Penalties.

6.1.1 GDPR.

The GDPR provides for the possibility of imposing administrative fines in the form of monetary penalties in different cases of non-compliance. According to Article 83[189], these monetary penalties shall be imposed by supervisor authorities, who shall decide in each individual case whether an administrative fine is to be imposed and the amount that should be awarded. These fines should be effective, proportionate, and dissuasive[190]. The GDPR establishes that for all those jurisdictions that do not provide administrative fines, the fine may be imposed by a competent national court as long as those legal remedies are effective and have an equivalent effect on the administrative fines[191].

Article 83(2) provides that depending on the circumstances of each individual case, fines should be imposed in addition to, or instead of the corrective powers that each supervisory authority has according to Article 58(2). Moreover, supervisor authorities when deciding whether to impose an administrative fine and deciding on the amount must consider different elements such as the nature, gravity, and duration of the infringement, the intentional or negligent character of the infringement, if any actions were taken to mitigate damages, the degree of responsibility of the controller and processors, between others.

Depending if the violation occurred is considered less or more severe, the amount awarded as penalties will vary. If the infringement is less severe, meaning it was upon any of the provisions of the GDPR listed in Article 83(4) letters (a) to (c), administrative fines can reach up to 10,000,000 Euros, or in the case of an undertaking, up to 2% of the total worldwide turnover of the proceeding financial year, whichever is higher. Now, if the infringement is more severe, meaning it was upon any of the provisions of the GDPR listed in Article 83(5) letters (a) to (e), administrative fines can reach up to 20,000,000 Euros, or in the case of an undertaking, up to 4% of the total worldwide turnover of the proceeding financial year, whichever is higher. If a controller or processor breaches several provisions of the GDPR, either intentionally or negligently, in the same or related

[189] Article 83 GDPR.
[190] Recital 151 paragraph 4; and Recital 152 paragraph 1 GDPR.
[191] Article 83(9) GDPR.

processing operations, the aggregate amount of the penalty shall be set for the most serious breach of the same provisions[192].

Within the category of administrative fines, the GDPR leaves to the Member States the possibility to create rules on whether and to what extent administrative fines should apply to public authorities and bodies established in that Member State.

Finally, it is important to note that in Article 84[193] the GDPR requires Member States to adopt by national law specific provisions for breaches of the GDPR not subject to the discipline of Article 83[194]. Such penalties must also be effective, proportionate, and dissuasive.

6.1.2 CCPA.

Under section 1798.155[195], any business, service provider, or individual that violates the conditions of this regulation will be subject to fines and penalties[196]. According to section 1798.155(b), a business shall be in violation if it fails to cure any alleged violation within 30 days after being notified of the alleged noncompliance. The penalties for statutory violations are limited to 2,500 USD for each violation or 7,500 USD for each intentional violation. The injunction is also available as a remedy[197]. These penalties must be awarded in a lawsuit brought by the California Attorney General who has been exclusively authorized under the CCPA to bring forth civil actions on behalf of the people of the State of California to enforce the law.

Violations that can make businesses liable to pay the civil penalties are failing to maintain a CCPA-compliant privacy policy, to respond to consumers' requests under the CCPA rights, to provide adequate notice when collecting personal information, selling consumers' personal information without providing an opt-out, discriminating against consumers who exercise their CCPA rights, between others[198]. Businesses have 30 days to take action and remedy the violation. They can provide the California Attorney General or the offended consumer with a statement confirming that the violation has been

[192] Zanfir-Fortuna, in Kuner, Bygrave, Docksey., *The EU General Data Protection Regulation (GDPR),* Article 83 GDPR, p. 1189 (Oxford University Press 2020)
[193] Article 84 GDPR.
[194] Article 83 GDPR
[195] Cal. Civ. Code § 1798.155
[196] Securiti, 'Fines & Penalties for Non-Compliance with the CCPA' (*CCPA*, 7 July 2022) <https://securiti.ai/blog/ccpa-fines/> accessed 23 August 2022
[197] Bukaty P, *The California Consumer Privacy Act (CCPA): An Implementation Guide* (ITGP 2019), chapter 7
[198] Securiti, 'Fines & Penalties for Non-Compliance with the CCPA' (*CCPA*, 7 July 2022) <https://securiti.ai/blog/ccpa-fines/> accessed 23 August 2022

remedied to avoid statutory civil penalties. In the event a business does not take action to remedy a breach within 30 days of receiving notice, this omission could be considered a piece of pretty strong evidence that the breach was intentional, which would make applicable the higher fees considered for intentional violations (7,500 USD instead of 2,500 USD for each violation).[199] Moreover, as the CCPA does not provide for a maximum amount that can result in the imposition of several penalties for each violation, businesses' liabilities can vary tremendously depending if the penalties awarded are for intentional or non-intentional violations of the CCPA.

In recent case law related to the topic reviewed in this section, California Attorney General Rob Bonta ("CA AG") announced a 1.2 million dollar settlement with Sephora, Inc. ("Sephora"), marking the first announced enforcement action under the CCPA. After conducting an enforcement sweep of online retailers, the Attorney General alleged that Sephora failed to (i) disclose to consumers that it was selling their personal information; (ii) that it failed to process user requests to opt-out of sale via user-enabled global privacy controls in violation of the CCPA; and, (iii) that it did not cure these violations within the 30 days period currently allowed by the CCPA[200].

In Sephora's case, the third parties could create profiles about consumers by tracking whether a consumer is using a MacBook or a Dell, the brand of eyeliner or the prenatal vitamins that a consumer puts in their "shopping cart," and even a consumer's precise location. Retailers like Sephora benefit in kind from these arrangements, which allow them to more effectively target potential customers. Sephora's arrangement with these companies constituted a sale of consumer information under the CCPA, and it triggered certain basic obligations, such as telling consumers that they are selling their information and allowing consumers to opt-out of the sale of their information. Sephora did neither[201].

The settlement also imposes injunctive obligations on Sephora in addition to the monetary fine of 1.2 USD million. For example, Sephora must: provide mechanisms for

[199] Clarip, 'California Consumer Privacy Act (CCPA) Fines and Consumer Damages' (*Data Privacy*, 08 january 2022) <https://www.clarip.com/data-privacy/california-consumer-privacy-act-fines/#:~:text=Potential%20Government%20Fines,violations%20is%20%242500%20per%20violation.> accessed 01 September 2022

[200] Attorney general Bonta, 'Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act' (*State of California Department of Justice*, 24 August 2022) <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement> accessed 10 October 2022

[201] Ibid.

consumers to opt out of the sale of personal information, and Provide reports to the Attorney General relating to its sale of personal information, among others[202].

6.1.3 Compared analysis.

The only similarity between the GDPR and the CCPA in this topic is that both provide for the possibility for monetary penalties to be issued in cases of non-compliance. Also as reviewed in the Sephora case, companies are subject to big penalties which can traduce in severe liabilities for them. The low amount of commonalities and all the differences that will be pointed out in the next paragraph, make it possible to conclude that these two regulations are inconsistent.

Among the several differences, the most important ones are who issues the penalties, the amounts and maximum possible associated with this kind of penalties, and finally the possibility in the case of the EU Member States to create rules on the application of administrative fines, which in the case of the CCPA has no similar nor related provision. As to who can issue the penalties in cases of non-compliance, the GDPR is to be issued by the supervisory authority, while the CCPA is issued by the Court. Also, the approach to calculating the fines differs. In the GDPR depending on the violation penalties may be diverse, the maximum possible administrative fine would be 4% of global annual turnover with no limits on an undertaking. As for the CCPA, the approach is different, as it will charge either 2,500 USD or 7,500 USD for each violation with no maximum amount to be fined, it will ultimately depend on the number of violations committed. As it can be observed, in both regulations violations may potentially result in significant economic liability for companies. Last, under the GDPR the Member States of the EU may create rules on the application of administrative fines to public bodies and authorities, and under the CCPA this is certainly not possible under no circumstance.

6.2 Civil remedies.

6.2.1 GDPR.

A personal data breach is defined in the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed[203]. With an ever-

[202] Ibid.
[203] Article 4(12) GDPR.

increasing use of technological means, breaches of security of data protection have increased, especially in service-based sectors with direct public interactions. Mobile operators, software companies, retailers, and banks have been in the spotlight over the past few years due to data breaches.

The right of compensation for damages caused as a result of an infringement of the GDPR is regulated in Article 82[204]. This provision contains all of the conditions for a damage claim under the GDPR, which as with any other European Regulation has to be interpreted by EU law. It is important to note that Article 82[205] is directly applicable in all Member States without any act of implementation. In virtue of the principle of the primacy of EU Law, any local law of any Member State which deviates from the scope and purpose of Article 82[206], will remain inapplicable. In this regard, it should also be pointed out that this provision should be construed only in accordance with EU law, not the law of Member States.

The person entitled to compensation is regulated in Article 82(1)[207], according to which any person who has suffered material (i.e. actual loss of money) or non-material damage (i.e. distress and emotional suffering) as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. It is important to note here the wording of the article, as "any person" and not only a "data subject" are entitled to bring an action for damages. Recital 146[208] states the controller or the processor should compensate for any damage which a person may suffer as a result of processing that infringes this Regulation. In resume, any person and not only data subjects can bring a claim for damages if the rest of the conditions set in the GDPR are fulfilled. Article 82(2)[209] regulates the person liable for compensation. According to this provision, only controllers (meaning of Article 4(7)[210]) or processors (meaning of Article 4(8)[211]) can be liable for compensation. Different liability requirements exist for the controllers or processors. Independently if it's a controller or processor the infringer, there must exist causality between breach and damage. Article 82(2)[212] sets specific liability requirements for processors being liable,

[204] Article 82 GDPR.
[205] Ibid.
[206] Ibid.
[207] Article 82(1) GDPR.
[208] Recital 146 GDPR
[209] Article 82(2) GDPR.
[210] Article 4(7) GDPR.
[211] Article 4(8) GDPR.
[212] Article 82(2) GDPR.

namely: (i) it had not complied with obligations of the GDPR specifically directed to processors; and (ii) it had acted outside or contrary to lawful instructions of the controller.

A claim for damages requires several conditions to be met. The first one is that a provision of the GDPR has been infringed. There is no specific catalog of infringements that would justify compensation. However, Recital 75[213] gives a comprehensive list of situations of data processing that could lead to physical, material, or non-material damage. The second requirement is that material or immaterial damage is suffered. The term "damage" has to be interpreted in harmony with the EU Law.

The GDPR has no minimum or maximum amounts for a damages claim. Recital 146[214] establishes about the amount for damages, that "*the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation*". Article 82(3)[215] introduces a specific rule for the burden of proof, exempting from liability the controller or processor if they can prove that they are in any way responsible for the event giving rise to the damage.

Article 82(3)[216] establishes a prerequisite of responsibility for the claim for damages, and Article 82(4)[217] contains a special rule of liability in the case of multiple damaging parties (joint liability). Article 82(5)[218] gives the right for internal compensation between the other controllers or processors when one of them has been considered liable for the entire damage in an external relationship. This article then provides that all the parties involved should "*compensate the other party corresponding to their part of the responsibility for the damage"*. Finally, Article 82(6)[219] regulates the court proceedings and the competent court. In this regard, Recital 147[220] clarifies *lex specialis* relationship to other provisions governing jurisdiction, especially concerning claims for damages

Damage claims are a controversial and very important part of the GDPR. Since its implementation, local courts have been dealing with how to interpret this provision by EU Law. However, there are still many questions to be answered.

[213] Recital 75 GDPR.
[214] Recital 146 GDPR.
[215] Article 82(3) GDPR.
[216] Ibid.
[217] Article 82(4) GDPR.
[218] Article 82(5) GDPR.
[219] Article 82(6) GDPR.
[220] Recital 147 GDPR

For example, in *Case C-300/21*[221], dealing with a civil action for non-material damages under Article 82(1) GDPR, the Supreme Court of Justice of the Republic of Austria referred some questions to the CJEU for further clarification over Non-material damages resulting from unlawful processing of data and upon which conditions the right to compensation should be awarded.

The facts of this pending case can be resumed as follows: from 2017 onwards, the Austrian Postal Service (Österreichische Post AG) collected the personal data of the Austrian population (name, addresses, and date of birth) and with the assistance of an algorithm, it defined the affinity of this person towards the different political parties. The plaintiff, an Austrian attorney to whom the Austrian Postal Service carried out an extrapolation, and to whom the algorithm defined he had a high affinity with the right-wing Austrian Freedom Party (FPÖ). It is important to note that the plaintiff had not consented to the processing of his personal data to the Austrian Post Service, and he was outraged by the storage of information about his party affinity data and offended by the affinity with the FPÖ. The plaintiff claimed compensation of EUR 1 000 in respect of non-material damage (inner discomfort). The first-instance court and the appellate court dismissed the plaintiff's claim for compensation. An appeal against the judgment of the appellate court was lodged with the Supreme Court of Austria, which referred the following questions to the CJEU for a preliminary ruling:

(1) Does the award of compensation under Article 82 also require, in addition to the infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?

(2) Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?

(3) Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence of the infringement of at least some weight that goes beyond the upset caused by that infringement?'[222]

[221] Case C-300/21, UI v Österreichische Post AG, CJEU [2021], ongoing.
[222] Ibid.

On 6 October 2022, Advocate General Campos Sánchez-Bordona ("AG") delivered his opinion in this case and gave well-founded arguments of how these three questions should be resolved by the CJEU[223].

Regards the first question, he considers there is no compensation right for a "mere" GDPR infringement[224], and he sustains this by following closely the wording of Article 82[225] which entitles a person with the right to compensation when he/she has actually "*suffered material or non-material damage*". Moreover, the AG rejects the arguments that there is an irrefutable presumption of damage once a GDPR violation has occurred – particularly that an infringement results in a "*loss of control*" over data which is compensable damage under Article 82[226]. The wording of the GDPR does not support this presumption and, instead, the recitals name loss of control over data as simply one possible damage that can occur. Finally, the AG concludes that Article 82 does not allow for punitive damages.

In connection to the second question, the AG concludes in its vaguest answer that neither the principle of equivalence nor the principle of effectiveness play an important role in this case and does not propose an answer to this question.

Lastly, the AG's response to the third question is that mere "annoyance" or "upset" is not sufficient to award compensation. He argues that as a criterion for eligibility for compensation, the request for a preliminary ruling refers to the intensity of the data subject's experience. It does not ask, however (at least not directly), whether certain emotions or feelings of the data subject are relevant or irrelevant to Article 82(1)[227] by their nature[228]. The AG concludes that he "does not believe that it is possible to infer from the principle of compensation for non-material damage which exists in EU law, that all non-material damage, regardless of how serious it is, are eligible for compensation."[229]

6.2.2 CCPA.

[223] Case C-300/21, UI v Österreichische Post AG, CJEU [2021], Opinion Advocate General Campos Sánchez-Bordona
[224] Ibid.
[225] Ibid.
[226] Martin bär, 'U – Advocate General opinion suggests strict limits on GDPR compensation claims' (*Linklaters*, 11 October 2022) <https://www.linklaters.com/en/insights/blogs/digilinks/2022/october/eu---advocate-general-opinion-suggests-strict-limits-on-gdpr-compensation-claims> accessed 28 October 2022
[227] Article 82(1) GDPR.
[228] Ibid 224, paragraph 96
[229] Ibid 224, paragraph 117

As pointed out at the beginning of this paper, California has the most comprehensive data privacy law in the United States and regulates any business that does business in California. The CCPA regulates damages for personal security data breaches in Section 1798.150[230]. According to this provision, individuals have a private right of action to any consumer whose nonencrypted and nonredacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: (i) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; (ii) Injunctive or declaratory relief; or (iii) Any other relief the court deems proper.

It is important to note that the term "personal information" in Section 1798.150(a)[231] has a narrower definition -for purposes of a private right of action- than in the rest of the CCPA. The definition of personal information for Section 1798.150(a)[232] is the one of Section 1798.81.5(d)(1)(A)[233] from California's Customer Records Act, which means an individual's name in combination with another listed data element, such as social security number, driver's license or another identification number, account number or credit or debit card number with access code or password, medical information, Health insurance information, unique biometric data generated from measurements or technical analysis of human body characteristics or genetic data[234].

When reviewing Section 1798.150(a)[235], it is possible to see that the damages available for a private right of action, include: (i) a statutory amount of between $100 and $750 per consumer per incident or actual damages, whichever is greater; (ii) injunctive or declaratory relief; and (iii) a catch-all for any other relief the court deems proper. Section 1798.150(b)[236], limits the private right of action. Under this provision, when a consumer is seeking statutory damages before initiating any action against a business, it first has to allow the business to "cure" the alleged violation by sending a written notice.

[230] Cal. Civ. Code § 1798.150
[231] Cal. Civ. Code § 1798.150(a)
[232] Ibid.
[233] Cal. Civ. Code § 1798.155
[234] Cathy Cosgrove , 'CCPA litigation: Shaping the contours of the private right of action' (*IAPP*, 08 June 2020) <https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action/> accessed 15 October 2022.
[235] Ibid.
[236] Cal. Civ. Code § 1798.150(b)

In this regard, this prior written notice appears as a mandatory condition to be fulfilled to file a lawsuit in the latter. Moreover, "*if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business*"[237].

Finally, Section 1798.150(c)[238] states the private right of action only applies to violations defined in Section 1798.150(a)[239] and "*shall not be based on violations of any other section of this title*".

The courts of California have ruled that Section 1798.150[240] has a limited private right of action and that it does not apply retroactively. "*In the case McCoy v. Alphabet, No. 20-cv-05427 (N.D. Cal. Feb. 2, 2021), the court dismissed a CCPA cause of action because there were no allegations of a data security breach. The allegations were that Google had collected personal information without complying with the CCPA's notice and consent requirements. The court reasoned that "nothing in [section 1798.150] shall be interpreted to serve as the basis for a private right of action under any other law." Accordingly, the court held that the CCPA's private right of action does not extend to non-data breach violations (e.g., CCPA notice violations). In Gardiner v. Walmart, No. 20-cv-04618 (N.D. Cal. July 28, 2021), the court ruled that the CCPA did not apply retroactively. Plaintiff alleged that he found his data for sale on the dark web in 2019 and that the data was still available on the dark web in 2021. The court found this argument unavailing, stating that the security breach must have "occurred on or after January 1, 2020," the effective date of the CCPA."*[241]

6.2.3 Compared analysis.

When comparing Article 82[242] with Section 1798.150[243], it is possible to see both provisions have few similarities and substantial differences, especially in the rationale, scope, and application. For this reason, it is possible to conclude that both regulations are inconsistent with each other.

---

[237] Cal. Civ. Code § 1798.150(b)
[238] Cal. Civ. Code § 1798.150(c)
[239] Cal. Civ. Code § 1798.150(a)
[240] Cal. Civ. Code § 1798.150
[241] Perkins Coie LLP, *California Consumer Privacy Act Litigation 2021 YEAR IN REVIEW*, April 2022 pg. 8
[242] Article 82 GDPR.
[243] Cal. Civ. Code § 1798.150

What they have in common, is that both rules entitle individuals to seek damages for violation of data privacy laws in two events: (i) when security measures violations have occurred; and/or (ii) data breaches have happened.

When it comes to the differences between them, the most important ones are the following: (i) in the GDPR, any person who has suffered material or non-material damages as a result of a violation of such regulation can claim judicial remedies. In the case of the CCPA, the scope is more narrow, as the remedy is only allowed when non-encrypted and non-redacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of security obligations. (ii) to seek damages under Article 82[244], there is no need to do any preemptive measure to initiate legal actions against the processor or controller. In the case of the CCPA, according to Section 1798.150(b)[245], when an individual wants to claim statutory damages, before initiating any action against a business, it first has to allow the business the opportunity to cure the alleged violation using an ending written notice, upon which business is given a 30-day term to cure the violation. In the event the business successfully cures the violation, then the individual cannot pursue further legal action against the business for statutory damages or class-wide statutory damages. (iii) The GDPR does not provide any figure for potential damages. On the other hand, Section 1798.150(a)(1)(A)[246] establishes that "damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater".

6.3 Representation of data subjects or consumers.

This section is dedicated to one of the many provisions found in the GDPR which do not have a direct homologous in the CCPA, to expose one of the many examples that make the GDPR a way more comprehensive data privacy regulation than the CCPA.

6.3.1. GDPR.

Article 80[247] contains rules related to the right of data subjects to be represented by not-for-profit entities (NPOs) active in the field of the protection of data subjects' rights and freedoms about the GDPR. The first paragraph of this article grants data subjects a subjective right to mandate NPOs to file complaints under Article 77[248], file

[244] Article 82 GDPR.
[245] Cal. Civ. Code § 1798.150(b)
[246] Cal. Civ. Code § 1798.150(a)(1)(A)
[247] Article 80 GDPR.
[248] Article 77 GDPR.

judicial remedies under Articles 78[249] and 79[250] as well as claim damages under Article 82[251] on their behalf. The second paragraph, Article 80(2),[252] provides that Member States may enable NPOs to (i) file complaints under Article 77[253], (ii) bring legal proceedings under Article 78[254] against a supervisor authority; and (iii) bring legal proceedings against controllers or processors under Article 79[255], independently of the data subjects mandate if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing. About this second paragraph, Recital 142[256] clarifies this does not extend to the filing of damage claims.

Article 80 is one of the great innovations introduced by the GDPR, and has changed the data privacy landscape in the EU. One example of this is the *Meta Platforms Ireland Limited case*[257]. Meta Platforms' decision is revolutionary in the field of data protection. This is a guide for consumer organizations working in this area to provide consumers with effective remedies, and how CJEU interprets the scope of Article 80(2). By this broad interpretation of the CJEU, consumer associations have the right to file the action without a specific mandate from the data subject or the subjective identification of individual data subjects. Even more, The CJEU held the presence of consumer protection associations strengthens the rights of data subjects, and a representative action might be better than several persons individually exercising their rights.

The facts of the case are resumed. "*Meta Platforms Ireland supplies services from the social network Facebook and is the controller of the personal data of users of that social network in the European Union. The Facebook internet platform contains, at the internet address www.facebook.de, an area called 'App-Zentrum' ('App Center') on which Meta Platforms Ireland makes available to users free games provided by third parties. When viewing some of those games, the user is informed that the use of the application concerned enables the gaming company to obtain a certain amount of personal data and gives it permission to publish data on behalf of that user. By using that*

[249] Article 78 GDPR.
[250] Article 79 GDPR.
[251] Article 82 GDPR.
[252] Article 82(2) GDPR.
[253] Article 77 GDPR.
[254] Article 78 GDPR.
[255] Article 79 GDPR.
[256] Recital 142 GDPR.
[257] Case C-319/20, Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände, CJEU [2022].

application, the user accepts its general terms and conditions and data protection policy. In addition, in the case of a specific game, the user is informed that the application has permission to post photos and other information on his or her behalf.

The German Federal Union of Consumer Organisations and Associations (1) considered that the information provided by the games concerned in the App Center was unfair. Therefore, as a body with standing to bring proceedings seeking to end infringements of consumer protection legislation, (2) the Federal Union brought an action for an injunction against Meta Platforms Ireland. That action was brought independently of a specific infringement of the right to data protection of a data subject and without a mandate from a data subject. The decision upholding that action was the subject of an appeal brought by Meta Platforms Ireland which, after that appeal was dismissed, then brought a further appeal before the Bundesgerichtshof (Federal Court of Justice, Germany). Since it had doubts as to the admissibility of the action brought by the Federal Union, and in particular as to its standing to bring proceedings against Meta Platforms Ireland, that court referred the matter to the Court of Justice" and asked the following question:[258]

> *'Does Article 80(1) and (2) and Article 84(1), preclude national rules which – alongside the powers of intervention of the supervisory authorities responsible for monitoring and enforcing the Regulation and the options for legal redress for data subjects – empower, on the one hand, competitors and, on the other, associations, entities and chambers entitled under national law, to bring proceedings for breaches of [the GDPR], independently of the infringement of specific rights of individual data subjects and without being mandated to do so by a data subject, against [the person responsible for that infringement] before the civil courts based on the prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions?*[259]'

The CJEU ruled: "*in the light of all the foregoing considerations, the answer to the question referred is that Article 80(2) of the GDPR must be interpreted as not precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the*

[258] Ibid.
[259] Ibid.

person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation"[260].

Besides the representation of data subjects in the terms just described, data subjects under the GDPR can designate a third party to request on their behalf. This may apply to, among others, acting through a proxy or legal guardians on behalf of minors, as well as acting through other entities via online portals. In some circumstances, the identity of the person authorized to exercise the right of access as well as authorization to act on behalf of the data subject may require verification, where it is suitable and proportionate. It should be recalled that making personal data available to someone who is not entitled to access it can amount to a personal data breach. As the GDPR does not regulate directly the requisites for valid powers of attorney, they are governed by national laws, which may impose specific requirements for demonstrating authorization to make a request on behalf of the data subject.

6.3.2 CCPA.

First of all, it is important to make clear that the CCPA does not regulate the possibility that consumers are represented in any way by a third party unless they have been designated someone as an authorized agent or they have been granted power of attorney. With this in mind, this chapter will review the requirements and regulations of the authorized agent, as it is the only legal figure in the CCPA and its Regulations that permits consumers to be represented for issues related to the enforcement of their rights.

As said, consumers may enlist a third person named the 'authorized agent' to act on their behalf to exercise their rights to submit data requests on their behalf.

'Authorized agent' means a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf[261]. When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer do the following: (i) provide the authorized agent signed permission to do so; (ii) verify their own identity

[260] Ibid paragraph 83.
[261] Final Text of Proposed Regulations Title 11. Law division 1. Attorney General Chapter 20. California Consumer Privacy Act Regulations, § 999.301. (c)

directly with the business; (iii) directly confirm with the business that they provided the authorized agent permission to submit the request[262]. These requirements would not apply when the consumer has provided the agent with power of attorney.

According to the before mentioned, under the CCPA consumers for example may use an authorized agent to submit a request to opt-out on their behalf, as long as they can provide proof that they have authorized such agent by means of written permission duly signed them. A business may deny a request from an authorized agent if the agent cannot provide the business with the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf[263].

6.3.3 Compared Analysis.

As is evident in this section, the regulation of the representation of data subjects in the GDPR and the authorized agents in the CCPA is absolutely divergent. There is absolutely no common ground between these two figures. Both laws permit data subjects or consumers to be represented by third parties as long as they have delegated powers of attorney. This is not a surprise as it's a general rule that applies to almost every matter in the legal field in every jurisdiction.

However, the GDPR went beyond the traditional figures of legal representation and allowed the possibility that third parties act on behalf of a data subject in their best interest even without consent. As resumed in Recital 142[264], a Member State may provide for NPOs to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation[265].

The ruling in the Meta Platforms case is a clear win for effective consumer protection. The fact that the CJEU resolved that consumer protection associations may bring representative actions against infringements of personal data protection and then added that such an action may be brought independently of the specific infringement of a data subject's right to the protection of their personal data and in the absence of a mandate to that effect, will set a new standard in this matter.

---

[262] Ibid.
[263] Bukaty P, *The California Consumer Privacy Act (CCPA): An Implementation Guide* (ITGP 2019), chapter 5
[264] Recital 142 GDPR.
[265] Ibid.

7. CONCLUSION.

As it has been reviewed throughout this thesis, the legal regimes for the protection of privacy in the EU and California have undergone radical changes in the last years since the GDPR and CCPA entered into effect. It is notable that with a difference of fewer than two years (2018-2020) these data protection regulations became applicable in two of the most relevant markets in the world. Both laws have raised the general standard of protection and landmark rulings in California and the EU confirm this tendency of protecting the privacy rights of people. Also, both of them have heavily captured the attention outside their jurisdictional borders, for the market relevance and the extraterritorial effect, covering businesses not incorporated in their respective territories.

At the beginning of this thesis, it was announced that the CCPA had been modeled after the GDPR. While there are substantive similarities between both of them, and even in certain aspects, it can be concluded they are fairly consistent, as reviewed from chapters 2 to 6 it is clear that both legislation have significant differences, with consequences for businesses' compliance efforts. These differences manifest themselves in many ways and can be understood partly as differences in the legal culture in their home jurisdictions.

When reviewing the key definitions and the material and territorial scope it was possible to see in detail why these legislations differ in elemental aspects that make them inconsistent between them. The most notable differences to point out are (i) the GDPR protects data subjects, who may or not be EU residents or citizens, and they may be located either in or out of the EU, while the CCPA's personal scope is more restrictive, as it only protects consumers who must be California residents; and (ii) the concept of data controller opposed to businesses also proves that the GDPR has a far ample reach than the CCPA, as data controllers may be natural or legal persons, for and non-for-profit entities, while businesses to qualify as such must fulfill specific thresholds and they must be for-profit entities. When reviewing the material scope, it is evident that the GDPR intends to have a broader scope of application than the CCPA, as both concepts of processing and personal data start their definitions in the GDPR with the wording "any", to have the amplest reach possible, as opposed to the more restrictive concepts of collecting and personal information in the CCPA.

In chapter four when reviewing the legal basis of each legislation, the greatest difference between the GDPR and CCPA in this regard is that the first one states that data controllers can only process personal data when there is a legal ground for it (consent or

processing is necessary for certain taxative reasons), while the second one not even lists the legal grounds based on which businesses can collect and sell personal information.

Chapter five, related to some of the most important rights of users regulated in the GDPR and CCPA corroborates that this is one of the aspects where these regulations are more consistent. Both of them regulate key rights of users, for example (i) the right to know about the data that has been collected from the data subjects and what data controllers/businesses do with it; (ii) the right to access by entitling users to access their personal data, including the possibility to ask for copies of their personal information; and (iii) the right to erasure also known as the right to be forgotten, and give individuals the right to request the deletion of their personal data that an organization has collected or stored.

The last chapter related to enforcement under both regulations is yet another demonstration of why the GDPR and the CCPA have profound differences, making these two legal texts inconsistent with each other. Both regulations provide monetary penalties for non-compliance, which in both cases may lead to significant liabilities for companies or entities managing personal data, having to pay fines of millions of euros or dollars. Which competent authority issues the fine, the maximum amounts awarded for this concept, and who can bring action towards the competent authority are all divergent topics between the GDPR and CCPA. In regards to the civil remedies for individuals, the GDPR set a way higher standard of protection for data subjects by establishing that any violation of the GDPR can trigger the claim for judicial remedies, no matter if the violation consists of material and no-materials damages, and that there are no maximum amounts that courts can award for a damages claim. In the case of the CCPA, the remedy is only allowed when non-encrypted or non-redacted personal information is subject to unauthorized access as a result of the business violation of security obligations. Finally, another great difference is that the GDPR gives the possibility to data subjects for giving a mandate to non-for-profits organizations to protect their rights, and even these entities may act in certain cases without a mandate to protect data subjects' rights (as reviewed in Meta Platforms Ireland case). The CCPA, on the other hand, does not have any provision like this and permits businesses to cure the alleged violations before any action against them is initiated for statutory damages. All of these topics make it possible once more, to make evident the great differences between these two laws.

In summary, there is no doubt that first the GDPR and then the CCPA have contributed tremendously to people's protection of their privacy rights, and they have

impacted the ways companies can model their businesses when dealing with personal data. As we face the fifth industrial revolution which is changing the world in unforeseeable ways as we increasingly rely on new technologies including artificial intelligence, big data, the internet of things, digital platforms, and augmented and virtual reality, the regulation of data privacy will become one of the most important legal topics in the century ahead and will have an impact on our daily lives.

8. BIBLIOGRAPHY.

8.1 Legislation.

1. Assembly Bill No. 375 of 28 June 2018, the California Consumer Privacy Act of 2018, codified in Title 1.81.5 Part 4 of Division 3 of the Civil Code of California, published on 29 June 2018 (Cal. Civ. Code § 1798.100)
2. California Code of Regulations, Title 18.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 2 281/31.
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1 [2016].
5. Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU).

8.2 Cases.

1. Case C-25/17, *Tietosuojavaltuutettu v Jehovan todistajat* [2018] CJEU.
2. Case C-212/13, *Ryneš v Úřad pro ochranu osobních údajů*, CJEU [2014]
3. Case C-210/16 - *Wirtschaftsakademie v Schleswig-Holstein*, CJEU [2018]
4. Case C-61/19, *Orange România SA v ANSPDCP*, CJEU [2020]
5. Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos*, CJEU [2014].
6. Case C-300/21, *UI v Österreichische Post AG*, CJEU [2021],
7. Opinion Advocate General Campos Sánchez-Bordona in Case C-300/21, *UI v Österreichische Post AG, CJEU* [2021],
8. Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems*, judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559) ('Schrems II')
9. Case C-319/20, *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände*, CJEU [2022].

10. Case C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, judgment of 24 September 2019 (Grand Chamber) (ECLI:EU:C:2019:772).
11. Case C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, judgment of 1 October 2019 (Grand Chamber) (ECLI:EU:C:2019:801)
12. Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, judgment of 4 May 2017 (ECLI:EU:C:2017:336)
13. Case *Rechtbank Noord-Holland v. Minister van Financiën*, ECLI:NL:RBNHO:2021:6040, [2021]
14. United States Court of Appeals, Ninth Circuit, *Boschetto v. D. Hansing* and others, No. 06-16595, August 20, 2008.
15. Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems*, judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559) ('Schrems II').
16. US Supreme Court, Daimler AG. v. Bauman et al., 571 U.S. 2014.
17. Bristol-Myers Squibb Co. v. Superior Court of California, 582 U.S. [2017].
18. Walden v. Fiore :: 571 U.S. 277 (2014)

8.3 Recommendations and Guidelines.

1. EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', 12 November 2019 (Version 2.1)
2. EDPB, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)', 7 July 2020
3. EDPB, 'Guidelines 01/2021 on Examples regarding Personal Data Breach Notification', 3 January 2022
4. EDPB, 'Guidelines 01/2022 on data subject rights - Right of access', 18 January 2022
5. EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, 12 may 2022
6. EDPB, 'Guidelines 9/2022 on personal data breach notification under GDPR', 10 october 2022
7. 'Guidelines on Transparency under Regulation 2016/679', Working Party, Article 29, 22 august 2018

8.4 Academic Sources.

1. Bukaty, P. *The California Consumer Privacy Act (CCPA): An implementation guide*. Ely: ITGP, 2019.
2. Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The Eu General Data Protection Regulation (Gdpr): A Commentary*, Oxford University Press, 2020.
3. David A Zetoony, *The Desk Reference Companion to the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA),* ABA Book Publishing, 2021.
4. IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*, ITGP, 2020.

8.5 Other Documents and Web Sources.

1. Albert Molins Renter, 'Primera ley de privacidad en línea de EE.UU. entra en vigor en California' (La Vanguardia, 5 January 2020) < https://www.lavanguardia.com/vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html> accessed on 20 June 2022.
2. Attorney general Bonta, 'Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act' (*State of California Department of Justice*, 24 August 2022) <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement> accessed 10 October 2022
3. Cathy Cosgrove , 'CCPA litigation: Shaping the contours of the private right of action' (*IAPP*, 08 June 2020) <https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action/> accessed 15 October 2022.
4. Clarip, 'California Consumer Privacy Act (CCPA) Fines and Consumer Damages' (*Data Privacy*, 08 january 2022) <https://www.clarip.com/data-privacy/california-consumer-privacy-act-fines/#:~:text=Potential%20Government%20Fines,violations%20is%20%242500%20per%20violation.> accessed 01 September 2022
5. Data Guidance One Trust, *Comparing privacy laws: GDPR v. CCPA, 2018, 6 https://fpf.org/blog/comparing-privacy-laws-gdpr-v-ccpa/* accessed on July 29 2022
6. Gdpr Hub, 'Article 2' (*GDPR Hub*, 4 july 2022) <https://gdprhub.eu/Article_2_GDPR#cite_ref-2 > accessed 10 July 2022.

7. Gdpr Hub, 'CJEU - C-61/19 - Orange Romania' (*GDPR Hub*, 26 november 2020) <https://gdprhub.eu/index.php?title=CJEU_-_C-61/19_-_Orange_Romania> accessed 31 may 2022
8. Gdpr hub, 'Article 3' (GDPR Hub, 2 march 2022) <https://gdprhub.eu/index.php?title=Article_3_GDPR> accessed 25 July 2022.
9. Gdpr hub, 'Article 6 ' (GDPR Hub, 25 april 2022) <https://gdprhub.eu/index.php?title=Article_6_GDPR> accessed 28 may 2022
10. Gdpr hub, 'Article 17' (*GDPR Hub*, 21 october 2021) <https://gdprhub.eu/Article_17_GDPR> accessed 6 june 2022
11. Intersoft consulting, 'Right to be Informed' (*GENERAL DATA PROTECTION REGULATION (GDPR)*, 08 June 2020) <https://gdpr-info.eu/issues/right-to-be-informed/> accessed 17 October 2022
12. Securiti, 'Fines & Penalties for Non-Compliance with the CCPA' (*CCPA*, 7 July 2022) <https://securiti.ai/blog/ccpa-fines/> accessed 23 August 2022
13. Martin bär, *'U – Advocate General opinion suggests strict limits on GDPR compensation claims'* (*Linklaters*,11October022) <https://www.linklaters.com/en/insights/blogs/digilinks/2022/october/eu---advocate-general-opinion-suggests-strict-limits-on-gdpr-compensation-claims> accessed 28 October 2022
14. Perkins Coie, *California Consumer Privacy Act ("CCPA") White Paper*, October 1, 2018 <https://www.perkinscoie.com/images/content/2/3/232754/CCPA-WHITE-PAPER-APRIL-13-2020.pdf> accessed 16 October 2022