A Comparative Study between the EU-GDPR and the US-CCPA

Angela Djerf

Master's Thesis in European and International Trade Law

HARN63

Spring Semester 2023

LUND UNIVERSITY

SCHOOL OF ECONOMICS AND MANAGEMENT

Table of Contents

Abstract

The development of the Internet is the most significant reason as to why Regulation (EU) 2016/679 (General Data Protection Regulation / EU GDPR) with its improvements, applicable since 25th May 2018, is replacing the Directive (Dir.) 95/46/EC. Outside the EU, American California Consumer Privacy Act (CCPA) of 2018 was adopted. The choice of the topic was influenced, inter alia, by the fact that the United States (U.S.) is an important economic and trading partner to the EU.

The purpose was to compare the two legislations with assistance from the *comparative legal method* and the research question ”What are the *principal* similarities and/or differences between the GDPR and the CCPA?”

The main similarity between the two frameworks is the purpose and the content aiming at the data protection of a data subject (GDPR) and a consumer (CCPA). The main difference is the choice of the term - ”data subject” is broader comparing to ”consumer”. The GDPR contains a slightly better structure with its eleven chapters organised by themes, while the CCPA is lacking this feature. Overall, both frameworks are quite ”strong” due to the usage of the word ”shall” in the provisions.

Keywords: CCPA, GDPR, personal data, data subject, consumer

Foreword

I would like to thank my family for supporting me during this thesis and my supervisor, Jonas Ledendal, for providing me with practical advice throughout the whole research period.

Angela Djerf

Malmö, 26th May 2023

Abbreviations

Art.	Article
CCPA	California Consumer Privacy Act
CFR	The Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Dir.	Directive
ECHR	European Convention on Human Rights (ECHR)
EDPB	European Data Protection Board
EU	European Union
GDPR	The General Data Protection Regulation
IMY	Integritetsskyddsmyndigheten (Swedish Authority for Privacy Protection)
OECD	Organisation for Economic Co-operation and Development
TEU	Treaty on European Union
TFEU	The Treaty on the Functioning of the European Union
U.S.	United States

1. Introduction

1.1 Background

The rapid technological development and the digitalisation era have together resulted in the adjustment of various legal frameworks, both on the national and on the international level. After several years of negotiations, the Organisation for Economic Co-operation and Development (OECD) adopted in 1980 guidelines concerning the protection of privacy and the cross-border transfer of personal data. On 28th January 1981, the legally binding treaty "Council of Europe Convention No. 108 on data protection", was established by the Council of Europe.[1] The European Commission was concerned over the significant differences between the different member states' legislation on personal data on the national level and its negative impact on the establishment of the single market. This resulted in negotiations concerning a directive aiming at harmonised legislation during the first half of the 1990s. The outcome was Data Protection Directive, officially Directive (Dir.) 95/46/EC, regulating the processing of personal data within the European Union (EU) and the free movement of such data, which was ratified on 24th October 1995.[2]

The development of the Internet is the most significant reason as to why Regulation (EU) 2016/679 (General Data Protection Regulation / EU GDPR) with its improvements, which has been applicable since 25th May 2018, is replacing the Dir. 95/46/EC.[3] Outside the EU, American California Consumer Privacy Act (CCPA) of 2018 was adopted. The choice of the topic was influenced, inter alia, by the fact that the United States (U.S.) is an important economic and trading partner to the EU[4], therefore the CCPA is worth to be studied. The CCPA was inspired by the GDPR and was put into effect on 1st January 2020, although the two legal

[1] David Frydlinger, Tobias Edvardsson, Caroline Olstedt Carlström, Sandra Beyer – "GDPR – Juridik, organisation och säkerhet enligt dataskyddsförordningen". Norstedts Juridik AB, 2018. P. 23.

[2] Ibid, p. 24.

[3] "The History of the General Data Protection Regulation". The official website of the European Union.

[4] The Official website of the European Union: "United States: EU trade relations with the Unites States. Facts, figures and latest developments.".

frameworks differ one from another, e.g., one can observe divergent definitions.[5] This thesis aims at examining and comparing the two legislations.

1.2 Purpose and research question

As mentioned in Section 1.1, the CCPA and the GDPR are two different legal frameworks, even though the CCPA builds on the GDPR-model. The purpose of this thesis is to examine the similarities and the differences between the two legal frameworks. Both regulations came into force almost in parallel with one another. Following research question will be guiding the study:

> What are the *principal* similarities and/or differences between the GDPR and the CCPA?

1.3 Delimitations

Due to time constraints and space limitations, the most prominent parts of both legislations have been studied. As regards to the GDPR, chapters 1 to 3 have been highlighted, with the data subject in focus. This means that chapters 4 to 11, dealing with controller and processor, remedies, liability and penalties, inter alia, have been left out. When studying the CCPA, the consumer has been the main target and once again, parts treating, inter alia, remedies, liability and penalties have been *excluded*.

1.4 Method and materials

This study focuses mainly on the GDPR and the CCPA as such, but other relevant material, e.g., case law and guidelines, have also been used. The main applicable method for this paper is the *comparative legal methodology*. According to Calboli, the general definition of comparative law is "comparison of different legal systems of the world". In other words, a comparative legal analysis is the method applied by scholars or other legal experts, when performing a comparison. These definitions are based on the observation that a comparative legal analysis requires "a comparison between the laws, judicial decisions, or legal practices of two or more different legal systems". With regard to the method, when one is going to conduct a comparative law study, any specific legal topic or set of issues can be compared

[5] Californian Compliance blog "Truevault".

– from constitutional law to criminal law to intellectual property, and so forth. One or more foreign legal systems will be studied first, followed by a "joint" analysis.[6]

The national systems are often to be included in the comparison, but scholars are allowed to contrast two or more foreign systems without referring to their national jurisdictions. Author provides an example of law areas which have undergone, or are undergoing, international or regional harmonisation, e.g., the field of intellectual property or European Union ("EU") law.[7] Calboli highlights an important fact that no agreement has been settled – and perhaps never will – "over whether comparative law has developed into an independent substantive field of law or simply constitutes a 'legal method' for comparing the laws of different countries".[8] However, scholars seem to agree on following objectives of comparative law: (1) to investigate the historical, philosophical, economic, and social aspects linked to national laws; (2) to use this information for a better understanding of different national or regional legal systems; (3) a better understanding of different legal systems, in order to improve national laws, regional and international laws as well as international relations.[9]

According to professor Merryman, there are several alternatives to rule-comparison and a variety of different ways of thinking about law. Professor finds them being more "complicated", by highlighting the "very comfortable" side of a rule-comparison. In this situation, you analyse two texts and "you do not have to get up from your chair". Merryman encourages one to leave "our chairs" and seek other types of organised information. This will facilitate to do more remarkable kinds of comparative research. He draws the attention to the fact that for a lawyer, a rule-comparison is of an important matter and it is logic that he/she will have to compare foreign rules with those on his/her national level. However, one should keep in mind other professions for which this comparison may not suffice.[10]

---

[6] Irene Calboli: "A call for Strengthening the Role of Comparative Legal Analysis in the United States". St. John's Law Review. Volume 90, Fall 2016, Number 3 – Article 5. P. 614.

[7] Ibid.

[8] Ibid, p. 615.

[9] Ibid, p. 616.

[10] Pierre Legrand: "John Henry Merryman and Comparative Legal Studies: A Dialogue." – *The American Journal of Comparative Law*, Winter, 1999, Vol. 47, No. 1, pp. 3-66. Oxford Journals. Oxford University Press. P. 4-5.

Similarly, EU legal method has been utilised in this thesis, but in order to facilitate the understanding for the reader, both the EU legal system and the American legal system have been explained more in detail in chapter 2.

1.5 Structure

Chapter 2 This chapter presents the EU legal system and the American legal system. The placement was considered in order to facilitate the reading.

Chapter 3 EU General Data Protection Regulation (GDPR) is being analysed here.

Chapter 4 This chapter has been dedicated to the American legal framework "California Consumer Privacy Act" (CCPA).

Chapter 5 This chapter highlights the principal similarities and/or differences between the above-mentioned legislations and contains summary and conclusions.

2. An overview of the EU Legal System and the American Legal System

2.1 Introduction

In Section 1.4 the comparative legal method has been explained in detail. This chapter presents an overview to the EU legal system and the American legal system.

2.2 EU Law (Legal System) and EU Legal Method

Most European Union (EU) nations, including Germany and France with civil law as origin, excluding Cyprus, are all examples of jurisdictions that use the civil law system. (Before Brexit, United Kingdom and Ireland were exceptions to the civil law system in line with Cyprus.)[11] In civil law countries (which may not have jury trials), in which the judge can have a more significative impact (exceptions exist, though), juries and oral arguments by lawyers often have a lesser value comparing to common law countries.[12] In civil law countries, statutes and other similar legal sources usually rank higher than case law.[13]

EU law is divided into primary law based on the founding treaties and the Charter of Fundamental Rights (CFR),[14] and into secondary law consisting of regulations, directives, decisions, recommendations, and opinions.[15] Primary law, binding secondary law, international agreements, general legal principles, and rulings issued by Court of Justice of the European Union (CJEU)[16], are all binding legal sources. *Non-binding* secondary law, preparatory works, the advocate general's opinions, the EU legal doctrine and economic theories are all examples of guidance

[11] Toni M. Fine: "American Legal Systems", chapter 2 *The American Legal System Made Easy*, p. 12. Anderson Publishing, a member of the LexisNexis Group, 1997.

[12] Ibid, p. 11.

[13] Ibid, p. 12.

[14] Jörgen Hettne & Ida Otken Eriksson: "EU-rättslig metod", p. 40. Norstedts Juridik AB. 2011.

[15] European Commission's website: "Primary versus secondary law".

[16] See further Art. 19(1) of the Treaty on European Union (TEU).

and are thus *non-binding*.[17] As regards the CJEU, the latter applies the teleological method[18] of interpretation for the most part. However, the Court highlights the fact that one should not only interpret a provision's wording, but also take into consideration its context and the purposes behind. This leads to other interpretation methods, such as: literal interpretation, autonomous interpretation, analogical interpretation and so forth.[19] Third chapter of this thesis is dedicated to the examination of the GDPR, but secondary sources in relation to the Regulation has also been included.

2.3 The American Legal System

The American law is built on common law from the United Kingdom and follows the principle of stare decisis (Latin, meaning "stand by your decision"). Stare decisis is a legal principle asserting that prior court decisions (e.g., holdings, conclusions, rulings) must be asserted as precedent case law. If a case is considered being a precedent case, then lower courts are obliged to rule in line with the precedent case. However, this requirement is applicable only if the precedent case is binding or mandatory. Among other sources, one can find the U.S. Constitution, statutes, restatements, decrees, treatises, and various other rules and sources that are applicable.[20]

As described, in common law countries, juries and oral arguments by lawyers often have a greater value comparing to civil law countries (which may not have jury trials), in which the judge can have a more significant impact (exceptions exist, though).[21] United Kingdom except Scotland, United States except Louisiana and Ireland are examples of common law jurisdictions. As mentioned, in civil law countries, statutes and other similar legal sources usually rank higher than case law. As the author states: "Under civil law, neither precedent cases nor stare decisis exist.".[22] Most European Union nations, except for Cyprus, are all examples of

[17] Hettne & Eriksson, 2011, p. 40.

[18] Subjective teleological interpretation aims at interpreting the legal framework in the light of the legislator's purpose, whereas the objective teleological interpretation aims at interpreting a provision in the light of "its function in the society."

[19] Hettne & Eriksson, 2011, p. 159.

[20] M. Fine, chapter 2, 1997, p. 11.

[21] Ibid.

[22] Ibid, p. 12.

jurisdictions that use the civil law system.[23] In line with the EU law, the American law contains two main types of legal sources: primary and secondary.

1. Primary legal sources include the following:
    - U.S. Constitution
    - Statutes
    - Rules, regulations, and orders
    - Executive orders and proclamations
    - Case law

2. Secondary legal sources include the following:

    - Treatises[24]
    - Restatements
    - Law review journals
    - *American Law Reports*[25]
    - (Hornbooks)[26]
    - Legal encyclopedias[27]

Similarly, there is a hierarchy where federal legal sources, such as U.S. Constitution, Federal statutes and treaties, federal rules and regulations, federal cases, are more prominent than state legal sources such as state constitutions, state statutes, state rules and regulations, state law cases.[28] Even though the United States is one country, from a legal perspective, a certain level of discretion is attributed to each individual state. The intent behind this dualistic system was to avoid one overly powerful central source of authority.[29] Like in the case with legal sources, a similar dual system can be observed as regards to federal-state court systems, where federal courts play a more significant role in the judicial court hierarchy, comparing

[23] Ibid.

[24] A treatise is a formal piece of writing examining a particular subject and should not be confused with a treaty, a ratified agreement between states.

[25] Marked in *italics* in the original source.

[26] According to Jerome Hall Law Library – Maurer School of Law's website, Hornbooks supply a detailed and straightforward analysis of a legal subject. These can be used by students or be useful to anyone requiring an overview of e legal subject. Therefore, it has been marked in parenthesis in this paper.

[27] M. Fine, 1997, p. 13.

[28] Ibid, p. 13-14.

[29] Ibid, p. 14.

to state courts. Hereby follows the federal court hierarchy (from highest to lowest): U.S. Supreme Court (USSC), Circuit courts, District courts.[30] Many cases that start at the state court level, are, if necessary, appealed to the federal level. Most state court systems are based on the federal court system. In some states there are three levels of hierarchy, while other states have chosen two levels of hierarchy. Each state court follows its own rules of procedure and set of practices. A three-level state court system ranks the courts from highest to lowest: State Supreme Court, State court of appeals, State trial court.[31]

As regards the American judicial system, there exists three branches of government: (1) the legislative branch (the Congress, which is composed of the Senate and House of Representatives); (2) the executive branch (including the U.S. President), and (3) the judicial branch (including the USSC and other courts). The idea is based on the separation of power in government[32], so no branch becomes too powerful comparing to the other two branches.[33]

2.4 Summary and conclusions

The civil law system dominates in most EU countries. The American law builds on common law system from the United Kingdom and is followed by the principle of stare decisis, which means "stand by your decision" in Latin. This legal principle means that prior court decisions such as, inter alia, rulings, must be declared as precedent law. Under civil law, neither precedent cases nor stare decisis exist. Statutes and other similar legal sources usually rank higher than case law. In common law countries, juries and oral arguments by lawyers often have a greater value comparing to civil law countries (which may not have jury trials), in which the judge can have a more significative impact (exceptions exist, though).

[30] Ibid, p. 15.

[31] Ibid, p. 16.

[32] In the U.S. government the term "the concept of checks and balances" is often used to describe the separation of power in the government.

[33] M. Fine, 1997, p. 17.

3. The General Data Protection Regulation

3.1 Introduction

This chapter describes the structure and the most significant content of the General Data Protection Regulation. Section 3.4 contains a summary of the most prominent articles and recitals. A shorter analysis has been included in the *end* of each *subsection*. Additionally, a few words have been mentioned straight after some GDPR-articles in relation to the CCPA, where relevant. As stated in Section 1.5, a similar description of the CCPA is provided in Chapter 4. Finally, both privacy frameworks are compared to one another in Chapter 5.

3.2 The structure of the GDPR

The Regulation is comprised of 99 articles and 173 recitals. There are eleven chapters. Chapter 1 covers the general provisions such as the scope of the Regulation, Chapter 2 defines the various principles relating to processing of personal data and Chapter 3 regulates the rights of the data subject such as transparency of the personal data. Chapter 4 describes the responsibilities of the controller and the processor, Chapter 5 handles the transfer of personal data to third countries or international organisations, Chapter 6 is dedicated to independent supervisory authorities and in Chapter 7 one can find provisions relating to the cooperation between the lead supervisory authority and the other supervisory authorities concerned. Chapters 8-11 deal with remedies, liability, penalties and so forth.

3.3 The purposes and scope of the GDPR

One of the purposes of the GDPR is the protection of individuals' fundamental rights and freedoms, especially their right to protection of their personal data. Integritetsskyddsmyndigheten (IMY), Swedish Authority for Privacy Protection refers on its website to the right to one's private life according to Art. 8 of the European Convention on Human Rights (ECHR). A reference is also provided to

Articles 7 and 8 of the EU Treaty on Fundamental Rights, covering the same rights as per Art. 8 ECHR.[34]

Regarding the scope of the GDPR, the Regulation is generally applicable in all situations where automated personal data processing takes place, and in some cases also manual processing of personal data. Any information referring to an identified or identifiable natural person is defined in the GDPR as personal data.

The purposes can be found in Art. 1 GDPR, which has been developed further in the next section and the recitals of the GDPR, which are partly presented in relation to the summarised articles, have likewise been presented in the next section.

3.4 The legal provisions and the recitals of the GDPR

3.4.1 Chapter 1 – "Subject-matter and objectives"

General provisions can be found in chapter 1, which contains four articles.

Article 1 "Subject-matter and objectives"

Art. 1(1) GDPR precises that the Regulation establishes the rules relating to the processing of personal data and rules relating to the free movement of personal data. Art. 1(2) draws the attention to the Regulation protecting fundamental rights ("fundamental privacy rights" are briefly mentioned in point (c) of the Section 1798.199.40 in the CCPA, but due to the space limitation, this Section has not been summarised in this paper) and freedoms of natural persons, in particular their right to the protection of personal data. Art. 1(3) GDPR clarifies that the protection of natural persons related to the processing of personal data shall *not* hinder the free movement of personal data within the Union.

Art. 1 refers to, inter alia, following recitals: **Recital 1** highlighting the fundamental right concerning the protection of the natural persons in relation to the processing of personal data, where a reference is made to the Article (Art.) 8(1) of the Charter

[34] The official website of Integritetsskyddsmyndigheten (IMY), Swedish Authority for Privacy Protection's website.

of Fundamental Rights of the European Union (the 'Charter' / CFR) and Art. 16(1) of the Treaty on the Functioning of the European Union (TFEU) covering the right of Fundamental Rights of the European Union (the 'Charter' / CFR) and Art. 16(1) of the Treaty on the Functioning of the European Union (TFEU) covering the right to the protection of personal data concerning him or her; **Recital 2** stating that the principles of, and rules on the protection of natural persons with regard to the processing of their personal data, should respect their fundamental rights and freedoms. It has been highlighted that all the natural persons should be treated in the same manner, no matter their nationality or residence; with help from **Recital 3** a link is established between the GDPR and the former Directive 95/46/EC, which both underline the importance of the harmonisation, but also the significance of protecting the fundamental rights and freedoms of natural persons when processing activities and to guarantee the free flow of personal data between Member States. However, **Recital 4** states that the right to the protection of personal data is *not* an absolute right. This means that in each situation it will depend on the context where this right will be balanced against other fundamental rights, based on the principle of proportionality.

Article 2 "Material scope"

Art. 2 covers four parts and describes situations when the Regulation is to be applied. According to Art. 2(1) it aims at circumstances where the processing of personal data occurs wholly or partly by automated means as well as "other than by automated means". Art. 2(2) lists situations of exceptions, where the Regulation is *not* covering. One example is where a natural person is processing personal data within a personal context or in relation to a household activity (Art. 2(2)(c) GDPR). Art. 2(3) precises the applicability of Regulation (EC) No 45/2001 when the processing of personal data is handled by the Union institutions, bodies, offices and agencies. However, the principles and rules in Art. 98 of the GDPR should still be respected. Art. 2(4) refers to the Directive 2000/31/EC, stating that the Regulation shall respect particularly Articles 12 to 15.

In relation to Art. 2, following recitals, inter alia, are mentioned: **Recital 14** explains that the Regulation is *not* applicable to legal persons. In **Recital 15** it is stated that the protection of natural persons "should be technologically neutral and should not

depend on the techniques used". In **Recital 18** one can find the information about the Regulation *not* being applicable to situations where the processing of personal data by a natural person occurs *outside* of a professional or a commercial activity, such as "purely personal or household activity".

The material scope is not detailed in the provisions of the CCPA, but this might be due to the reason of the title "California Consumer Privacy Act", which takes aim at consumers in California.

Case C-101/01 – Lindqvist (2003)

In relation to Art. 2(2)(c), case C-101/01 – Lindqvist from 2003 should be highlighted, where the CJEU concluded that Mrs. Lindqvist's "mainly charitable and religious activities" were *not* considered as an exception in accordance with Art. 3(2) in the Dir. 95/46/EC (today the provision is to be found in Art. 2(2)(c) GDPR).[35] This means that Lindqvist's activity did not count as "purely personal or as a household activity". The case illustrates how a context impacts the interpretation of a certain article. One should be aware of this crucial aspect.

Article 3 "Territorial scope"

Art. 3(1) GDPR states that the Regulation applies when processing of personal data is observed in the context of the activities of an establishment of a controller or a processor in the Union, even if the processing occurs outside the Union. According to Art. 3(2), the processing of personal data is covered by the GDPR, when a data subject is in Union, but, e.g., is offered goods or services by a controller or processor not established in the Union. Art. 3(3) states that the Regulation is applicable to the data processing by a controller not established in the Union, "but in a place where Member State law applies by virtue of public international law".

In relation to Art. 3, following recitals, inter alia, are mentioned: **Recital 22** arguing that Regulation covers any processing of personal data by the controller or by the processor, whether the process takes place within the Union or not; **Recital 23** specifying that the targeted data subjects within the Union are protected by the Regulation, whether the processing of personal data of data subjects is issued by a

[35] C-101/01 – Lindqvist (2003), paras 45-47. CJEU.

controller or a processor not established in the Union. This recital aims at processing of data related to offering goods and/or services.

In comparison to the GDPR, the CCPA does not cover the territorial scope, but this might be due to the reason of the title "California Consumer Privacy Act", which is already pointing at consumers in California. There is no legal provision specifying the protection of a consumer's personal data, when the processing occurs outside California or when a controller is not established in California, but still is processing the data. However, Section 1798.199.40 "The agency shall perform the following functions" (not included in this thesis) touches vaguely on the territorial aspect in its point (i) stating following: "Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections."

Article 4 "Definitions"

Art. 4 GDPR contains 26 definitions. One of these is to be found in Art. 4(1), which defines "personal data". It is "…any information relating to an identified or identifiable natural person ("data subject")…" and so forth.

Section 1798.140 in the CCPA (not included in this thesis) is a corresponding provision to the GDPR's Art. 4. Instead of "personal data", one can find a definition of "advertising and marketing" already in the beginning. The list of the definitions in the CCPA could have been a little bit shorter and could have been placed earlier in the framework, e.g., already in the beginning.

As one can observe that the first four articles of the GDPR are covering subject-matter, objectives, the material scope, the territorial scope and definitions. The legislator has used relatively short and concise sentences and it has therefore facilitated the reading of each provision. A preference for a "strong" wording such as "shall" instead of "may" has been applied several times, e.g., in Articles 1(3) and 2(4), which strengthens the position. "Data subject", "processing", "personal data" are the most encountered words in the first chapter.

3.4.2 Chapter 2 – "Principles"

Chapter 2 lays down principles that should be respected when the personal data is being processed and consists of seven articles.

Article 5 "Principles relating to processing of personal data"

Art. 5 GDPR contains two paragraphs, with the precision "personal data shall be". One should observe the "strong" wording "shall" and not "may" or "might". Art. 5(1)(a) provides for the "lawfulness, fairness and transparency", meaning that the processing of the personal data related to the data subject should be lawful, fair and transparent. Art. 5(1)(b) highlights the necessity of the personal data being collected for "specified, explicit and legitimate purposes" ('purpose limitation'). Any further processing of personal data should be compatible with those purposes. Archiving purposes are considered as exception and therefore compatible with the initial purposes. Further examples are provided in the Art. 89(1) of the same Regulation, which Art. 5(1)(b) refers to. According to Art. 5(1)(c) personal data shall be 'adequate, relevant and limited'. The principle of the 'data minimisation' requires the necessity to limit the personal data as much as possible. Art. 5(1)(d) precises the accuracy and updated personal data ('accuracy'). Inaccurate information should be erased or rectified without delay. Art. 5(1)(e) requires 'storage limitation', meaning that the personal data shall be kept in a form permitting identification of data subjects only during the time the situation of data processing requires so. However, archiving purposes in the public interest, inter alia, are permitted to store the data for longer periods. Once again, a reference is provided to Art. 89(1) of the same Regulation. Art. 5(1)(f) aims at the security of the personal data in relation to its processing, such as accidental loss ('integrity and confidentiality'). Art. 5(2) calls out for the responsibility of the controller and the ability to prove the obedience with paragraph 1 ('accountability').

Art. 5 refers to **Recital 39**, which presents the principles of data processing. Considering the fact of the principles of lawfulness and fairness being brought forth already in the first sentence, one may assume the two being the most prominent ones. Similarly, the principle of transparency should be respected, requiring any information relating to the processing of the natural persons' personal data, be accessible and formulated in a clear and concise manner. The identity of the

controller and the purposes of the processing should be included. Natural persons should get informed about risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. A reference is also made in Art. 5 to **Recital 74,** covering responsibility and liability of the controller.

Article 6 "Lawfulness of processing"

Art. 6(1) GDPR precises that the processing of personal data shall be lawful only if one of the conditions set out in paragraph 1 are respected. Art. 6(1)(a) brings forth the provided consent by the data subject. Art. 6(1)(b) aims at the necessity of the processing in order to fulfil a contract to which the data subject is party. Art. 6(1)(c) allows the processing in situations where the data controller is required to respect a legal obligation. Art. 6(1)(d) identifies a situation where a processing is perceived as lawful, related to the protection of the vital interests of the data subject or another natural person. Further on, Art. 6(1)(e) allows the processing if it is e.g., in the public interest. Finally, Art. 6(1)(f) covers situations where the purposes of the legitimate interests pursued by the controller or by a third party, require the processing of data. However, an exception is made, inter alia, where the personal data belongs to a child. Point (f) is *not* applicable "to processing carried out by public authorities in the performance of their tasks". Art. (6)(2) allows the Member States to regulate the rules of the Regulation on the national level, in relation to points (c) and (e) in the first paragraph.

Art. 6 refers to, inter alia, **Recital 39** covering principles of data processing (already mentioned in relation to Art. 5), and **Recital 40** stating that the processing of personal data is considered being lawful if it is built on the basis of the consent of the data subject, or if another legitimate reason could be justified by law.

Article 7 "Conditions for consent"

Art. 7(1) GDPR requires the data controller to demonstrate that the consent has been provided by the data subject, in situations where the data processing is based on consent. Art. 7(2) precises the importance of the request for consent being presented in a clearly distinguishable way from other matters, if the data subject's consent is provided in the context of a written declaration involving other matters.

If a part of such a declaration constitutes an infringement of the Regulation, that part shall not be binding. According to Art. 7(3) the data subject shall have the right to withdraw his or her consent at any time. It is also important to make it easy for a data subject to withdraw as to give consent. Art. 7(4) precises that when it comes to evaluating whether consent is freely given, it is mainly important to consider, inter alia, whether the performance of a contract, including the provision of a service, is depending on consent to the processing of personal data that is not necessary for the fulfilment of that contract.

Article 8 "Conditions applicable to child's consent in relation to information society services"

Art. 8(1) GDPR makes a reference to point (a) of Art. 6(1), where the offer of information society services is directed to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. If a child is below the age of 16 years, the processing is considered being lawful only if consent is given or authorised by the holder of parental responsibility over the child. It is also possible for Member States to regulate a lower age, but as far as it is not below 13 years.

In comparison to the GDPR, there is no provision dedicated separately to a child in the CCPA, but the importance of a consent in relation to a child, figures in Section 1798.120 (cf. Section 4.3.3).

Article 9 "Processing of special categories of personal data"

The most important parts of Art. 9 have been summarised below.

Art. 9(1) GDPR states that processing of personal data revealing, inter alia, racial or ethnic origin, political opinions, genetic data, shall be prohibited. Art. 9(2) lists situations with help from points (a) to (j) where paragraph 1 should *not* be applicable. A description of the most prominent ones has been provided below. Point (a) covers situations when the data subject has provided explicit consent to the processing of those personal data for one or more specified purposes, except "where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject". Point (b) aims at situations where the obligations and exercising specific rights of the controller or of the data subject

in the field of employment and social security and social protection law, require the data processing for the purposes. However, it should be authorised, e.g., by Union or Member State law. Safeguards for the fundamental rights and the interests of the data subject are extremely important.

Sensitive data can be found in the CCPA's Section 1798.100 (cf. Subsection 4.3.2).

Article 10 "Processing of personal data relating to criminal convictions and offences"

Art. 10 GDPR explains that processing of personal data relating to criminal convictions and offences or related security measures according to Art. 6(1) shall be performed in the power of official authority or if the processing is authorised by Union or Member State law. Safeguards for the rights and freedoms of data subjects are highlighted as well.

Article 11 "Processing which does not require identification"

Art. 11(1) GDPR states that if the purposes for which a controller treats personal data "do no longer require the identification of a data subject by the controller", no additional information in order to identify the data subject needs to be processed only for the sole purpose of complying with the Regulation. Art. 11(2) states that if the controller is not able to prove that he/she is not capable to identify the data subject, in cases referred to in paragraph 1 of Art. 11, the controller shall inform the data subject consequently, if possible. In such cases, Articles 15 to 20 shall *not* be applicable, except in situations where the data subject, "for the purpose of exercising his or her rights under those Articles, provides additional information enabling his or her identification."

The division in seven articles facilitates the navigation of the Chapter 2. Each heading is clear enough to grasp the idea of its content. In line with the first chapter, the word "shall" can be observed in e.g., Art. 5, which strengthens the position of the provision. Art. 9 aiming at sensitive personal data is important, but its content could have been shortened down a little bit. Overall, the text is not hard to read. Points (a) to (j) in, e.g., Art. 9, are helping the reader out to follow the different exceptions, instead of letting these "melt" together as one single paragraph.

The CCPA is lacking a detailed provision/chapter over the principles. Section 1798.100 contains both the purposes for which personal data is collected, but also the duty of the controller to notify the consumer about his/her collection of personal data. In the GDPR, as one could read above, the purposes are stated in Art. 5(1)(b) and the obligation of the controller to inform the data subject is covered by Articles 13 and 14 (cf. Section 1798.100 in the Subsection 4.3.2 below).

3.4.3 Chapter 3 – "Rights of the data subject": Section 1 – "Transparency and modalities"

Chapter 3 aims at the rights of the data subject and contains five sections with its 23 articles, which are presented separately in each subsection below.

Section 1 is comprised solely of one article.

Article 12 "Transparent information, communication and modalities for the exercise of the rights of the data subject"

Art. 12(1) GDPR highlights the controller's responsibility to take appropriate measures to provide any information according to Articles 13 and 14 of the Regulation (also Articles 15 to 22 and 34 are referred to in this context) to the data subject. The information should be presented in a concise and transparent manner, especially when the data subject is a child, in written form and, where appropriate, by electronic means. Art. 12(2) states that the controller shall simplify the exercise of data subject rights under Articles 15 to 22. Art. 12(3) encourages the controller to provide information on action taken following a request as per Articles 15 to 22 "to the data subject without undue delay in any event within one month of receipt of the request". If necessary (e.g., due to the complexity and number of requests), the period may be extended by two further months.

Section 1 of the Chapter 3 in the GDPR takes aim at the rights of the data subject, the transparency and modalities as its headline states, but one could also see this section describing the relationship between the data subject and the data processor together with the latter's obligations towards the data subject. The same criticism could be provided in relation to Art. 12 as to Art. 9 in Chapter 2 – the content could have been a little bit shorter or divided into two articles instead.

3.4.4 Chapter 3 – "Rights of the data subject": Section 2 – "Information and access to personal data"

Section 2 comprises three articles.

Article 13 "Information to be provided where personal data are collected from the data subject"

Art. 13(1) GDPR reads: "Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:", and contains points (a) to (f), which have been partly summarised below. Point (a) aims at the identity and the contact details of the controller, but also of the controller's representative, if necessary. Point (b) mentions the contact details of the data protection officer, if applicable. Point (c) indicates the purposes of the processing and its legal basis. Point (d) refers to Art. 6(1) stating situations where the processing is based in point (f) in the same article, and the legitimate interests are pursued by the controller or by a third part. Art. 13(2) aims at the fairness and transparency and indicates that additional information referred to in paragraph 1 of the same article, should be provided to the data subject at the time when personal data are obtained. Art. 13(3) clarifies that if further process of the personal data is required for a purpose other than that for which the personal data were collected, the controller shall provide the data subject with information prior to that further processing. According to Art. 13(4) paragraphs 1, 2 and 3 are *not* applicable to situations where the data subject already has the information.

Article 14 "Information to be provided where personal data have not been obtained from the data subject"

The first paragraph of Art. 14 GDPR consists of points (a) to (f) and lists the same type of information as in Art. 13. The rest of paragraphs are almost identical with those in Art. 13 and have therefore not been included in this paper.

Art. 13 of the GDPR corresponds to Section 1798.100 of the CCPA (cf. Subsection 4.3.2).

Article 15 "Right of access by the data subject"

Art. 15(1) GDPR reads: "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:", and covers points (a) to (h) including the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipient to whom the personal data have been or will be disclosed, especially in circumstances where a transfer might occur to third countries or international organisations and the envisaged period for which the personal data will be stored. Art. 15(2) describes the right of the data subject to be informed of the appropriate safeguards as per Art. 46, when personal data are transferred to a third country or to international organisation. Art. 15(3) clarifies that the controller shall provide the data subject a copy of the personal data undergoing processing. The controller may charge a reasonable fee in situations where the data subject requests additional copies. Art. 15(4) highlights that the right to obtain a copy as per Art. 15(3) "shall not adversely affect the rights and freedoms of others".

Section 2 of the Chapter 3 captures a very important nuance. The legislator has indeed thought through its content. It is crucial distinguishing a situation where the personal data has been collected directly from a data subject as per Art. 13, and a situation where the personal data have *not* been obtained from the data subject as per Art. 14. Art. 15 is very important in the sense that it contains other recipients of personal data, beyond the "first" data controller.

An equivalent provision of Art. 15 GDPR can be found in Section 1798.110 of the CCPA (cf. Subsection 4.3.3). Overall, section 2 in the chapter 3 of the GDPR aiming at data subjects' rights has a lot in common with the provisions covering consumers' rights in the CCPA.

3.4.5 Secondary sources in relation to Article 15 GDPR

One recent case and guidelines provided by the European Data Protection Board's (EDPB) in relation to Art. 15 are presented below.

Case C-154/21 – RW vs. Österreichische Post AG (2023)

A citizen of Austria had requested, in accordance with Art. 15 of the GDPR, information from Österreichische Post AG, whether his personal data concerning him was being or had been stored. If the data had been transferred to third parties, the data subject had sought information about the recipients of the data.[36]

Österreichische Post AG replied that the data would only be processed in accordance with law and referred to a website for further information and supplementary data processing purposes. The data subject brought an action before the Austrian courts and insisted on receiving the information about the recipients of his personal data. The case went up to the Austrian Supreme Court (OGH), which consulted the CJEU about the interpretation of Art. 15(1)(c) GDPR, by addressing following questions:

A) Are the data controllers obliged to disclose the specific identities of the recipients of personal data to data subjects upon request or else?
B) Does the provision leave it up to the controller whether to communicate the specific identities of the recipients or only the categories of recipients?

In this case, the CJEU followed the recommendations of the Advocate General, Giovanni Pitruzella's opinion of 9 June 2022, that the interpretation in favour of the data subjects is also established by Art. 19 GDPR. The first sentence aims at the controller's obligation to notify any recipients of personal data of any rectifications or erasure. The second sentence states that the controller has to inform the data subjects of the recipients upon request. The CJEU continued: "The data subject therefore has the right, within the framework of the controller's duty to inform, to receive information about the specific recipients in order to be able to exercise the rights under Articles 16, 17 and 18 of the GDPR. In this respect, an interpretation in favour of the data subjects, as set out above, is correct in order to comply with the transparency requirement." However, the CJEU also stated that in certain circumstances, data controllers are *not* obliged to provide detailed information on specific recipients. In such cases, it may be sufficient to provide categories of recipients.

[36] Case C-154/21 – RW vs. Österreichische Post AG. CJEU.

European Data Protection Board's (EDPB) guidelines are pointing out, inter alia, the circumstances when data controllers have the possibility to avoid providing detailed information on specific recipients. Art. 15(4) of the GDPR states that the right to obtain a copy "shall not adversely affect the rights and freedoms of others". According to the EDPB, these rights must be taken into consideration also in situations when access to data is possible "on-site" (and not only when providing a copy). It is the responsibility of the controller to demonstrate that the rights or freedoms of others would be negatively impacted in the concrete situation. When applying Art. 15(4), one should keep in mind the non-possibility of refusing the data subject's request altogether. Only those parts with potential negative impact are allowed to be left out.[37]

Another reason to when controllers are allowed to, in accordance with Art. 12(5) GDPR, dismiss requests, is when these are "manifestly unfounded or excessive". An alternative would be to charge a reasonable fee for this kind of requests. According to the EDPB, these concepts have to be interpreted narrowly. The specifics of the controller's business activity determines whether a request should be considered excessive or not. The controller may agree on charging a fee from the data subject instead of refusing access. It is the controller's obligation to prove that a request is being manifestly unfounded or excessive. In the same manner, Member States' national law may restrict the right of access, according to Art. 23 GDPR).[38]

3.4.6 Chapter 3 – "Rights of the data subject": Section 3 – "Rectification and erasure"

Section 3 contains five Articles.

Article 16 "Right to rectification"

Art. 16 GDPR consists of one single paragraph stating that the data subject shall have the right to a rectification by the controller of inaccurate personal data concerning him or her, without undue delay.

[37] European Data Protection Board's webpage, "Guidelines 01/2022 on data subject rights – Right of access", p. 5. Version 2.0. Adopted on 28 March 2023.

[38] Ibid.

The CCPA provides for an equivalent possibility in its Section 1978.106 (cf. Subsection 4.3.3).

Article 17 "Right to erasure" ("Right to be forgotten")

Art. 17(1) GDPR aims at the data subject and his/her right to acquire from the controller the erasure of personal data. The grounds are presented in points (a) to (f) covering situations where the personal data are no longer necessary for the processing, the data subject's withdrawal of the consent, the data subject's objection to the processing, if the personal data have been unlawfully processed, the personal data have to be erased due to compliance with a legal obligation in Union or Member State law to which the controller is subject, the personal data have been gathered based on the offer of information society services as per Art. 8(1). Art. 17(2) sets out the controller's obligation to inform other controllers which are processing the personal data that the data subject has requested the erasure by such controllers. This situation aims at situations where "the controller has made the personal data public and is obliged to erase the personal data according to paragraph 1. Art. 17(3) mentions exceptions and reads following: "Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:". The five exceptions that are being cited in points (a) to (e), meaning that the erasure of personal data is *not* obliged, are, inter alia, following: in situations where the right of freedom of expression and information applies; when compliance with a legal obligation requires processing by Union or Member State law to which the controller is subject, and so forth.

Case C-131/12 – Google vs. Spain (2014)

In this context, case C-131/12 – Google vs. Spain should be highlighted. The CJEU ruled that European citizens have a right to request commercial search firms, such as Google, collecting personal information for profit, to remove links to private information in circumstances where the latter is no longer required.[39] The case refers to Articles 2, 4, 12 and 14 in the Dir. 95/46/EC, but today the right to be forgotten is to be found in Art. 17 GDPR.

[39] Case C-312/12 – Google vs. Spain (2014). CJEU.

Similarly, the right to delete information is covered by Section 1798.105 of the CCPA (cf. Subsection 4.3.3).

Article 18 "Right to restriction of processing"

Art. 18(1) GDPR states that the data subject shall have the right to acquire restriction of processing from the controller and lists with help of points (a) to (d) the applicable situations: where the accuracy of the personal data is opposed by the data subject; when the processing is unlawful and the data subject requests the restriction of their personal data instead of the erasure; when the controller no longer requires the personal data for the purposes of the processing; when the data subject has objected to processing in relation to Art. 21(1). Art 18(2) states that if processing has been restricted under paragraph 1, such personal data shall only be processed with the data subject's consent (or e.g., for the establishment). Storage of data is allowed as an exception, though. Art. 18(3) indicates that a data subject who has acquired restriction of processing according to paragraph 1, shall be informed by the controller "before the restriction of processing is lifted".

Article 19 "Notification obligation regarding rectification or erasure of personal data or restriction of processing"

Art. 19 GDPR states the controller's obligation to inform each recipient to whom the personal data have been disclosed, about any rectification or erasure of personal data or restriction of processing according to Art. 16, Art. 17(1) and Art. 18.

Article 20 "Right to data portability"

Art. 20(1) GDPR allows the data subject to receive the personal data concerning him or her in a machine-readable format and the data subject has the right to transfer those data to another controller. According to Art. 20(2), there is a possibility for the data subject, following paragraph 1, to request the transfer of the personal data from one controller to another, where technically feasible. Art. 20(3) states that "the exercise of the right referred to in paragraph 1 of this Article should be without prejudice to Art. 17". Art. 20(4) highlights that paragraph 1 shall not affect the rights and freedoms of others in a negative manner.

Section 3 of the Chapter 3 in the GDPR highlights a data subject's right to, inter alia, an erasure of personal information as per Art. 17, which is a very important right. The presented case Google vs. Spain demonstrates the significance of this possibility. For some individuals, it might be crucial especially if an access to their data risks putting them in danger due to political persecution and so forth.

3.4.7 Chapter 3 – "Rights of the data subject": Section 4 – "Right to object and automated individual decision-making"

Section 4 contains two articles, which have been summarised below.

Article 21 "Right to object"

Art. 21(1) GDPR indicates the data subject's right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, according to point (e) or (f) of Art. 6(1). Art. 21(2) aims at the data subject's right to an objection of the processing of personal data, including profiling, related to direct marketing. Art. 21(3) states that the personal data shall no longer be processed for direct marketing purposes once the data subject has objected to the latter. Art. 21(4) precises the importance of the data subject receiving the information regarding the right as per paragraphs 1 and 2 "at the latest at the time of the first communication with the data subject". Art. 21(5) precises the data subject's right to object by automated means and refers to the context of the use of information society services and the Directive 2002/58/EC. Art. 21(6) GDPR treats an exception of processing personal data for scientific or historical research purposes or statistical purposes as per Art. 89(1) of the same Regulation. In case of the data subject's objection, the personal data may still be processed for reasons of public interest.

Article 22 "Automated individual decision-making, including profiling"

Art. 22(1) GDPR precises that the data subject "shall have the right not to be subject to a decision based solely on automated processing, including profiling…". Art. 22(2) states that paragraph 1 shall not apply if the decision: (a) is necessary for entering, or fulfilment of, a contract between a data controller and the data subject;

(b) “is authorised by Union or Member State law to which the controller is subject…”, or; (c) “is based on the data subject’s explicit consent”. Art. 22(3) precises that in cases as per points (a) and (c) of paragraph 2, the data controller is obliged to implement “suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests…”. Art. 22(4) states that decisions mentioned in paragraph 2 shall *not* be based on special categories of personal data as per Art. 9(1), except for situations where point (a) or (g) of Art. 9(2) applies and appropriate measures to safeguard the data subject’s rights and freedoms and legitimate interests are established.

Section 4 of the Chapter 3 in the GDPR provides, inter alia, a data subject’s right not to be subject to a decision, based exclusively on automated processing, including profiling as per Art. 22. The importance of this right can be observed in situations where a government or a municipality applies an automated processing when treating significant matters such as determining about an individual’s residence permit in a country. This kind of subjects should always be verified by a human as it is not very “safe” to rely on an automated processing. If a human is able committing a mistake, a robot has a greater risk of doing so.

Even though “automated individual decision-making, including profiling” is missing in the CCPA, the right to object can be found in Section 1798.120 (cf. Section 4.3.3 below).

3.4.8 Chapter 3 – “Rights of the data subject”: Section 5 – “Restrictions”

Section 5 consists of one single article – Article 23 “Restrictions” with its two paragraphs.

Article 23 “Restrictions”

Art. 23(1) indicates the possibility for a “Union or Member State law to which the data controller or processor is subject”, to restrict the extent of the obligations and rights provided in, inter alia, Articles 12 to 22, with help from a legislative measure. Such a restriction has to respect the essence of the fundamental rights and freedoms and has to be a necessary and proportionate measure in a democratic society to safeguard following as per points (a) to (j) set out in Art. 23(1): national security;

defence; public security; the prevention, investigation, detection or prosecution of criminal offences; other important objectives of general public interest of the Union or of a Member State; the protection of judicial independence and judicial proceedings; the prevention, investigation and prosecution of breaches of ethics for regulated professions; a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); the protection of the data subject or the rights and freedoms of others; the enforcement of civil law claims. Art. 23(2) highlights that any legislative measure as per paragraph 1, shall contain specific provisions, at least, where relevant, as regards to the following listed in points (a) to (h): the purposes of the processing or categories of processing; the categories of personal data; the scope of the restrictions introduced; the safeguards to prevent abuse or unlawful access or transfer, and so forth.

Section 5 of Chapter 5 in the GDPR allows a restriction of data subjects' rights. The legislator has thought it through indeed, as a balance is required. In some situations, a data subject's right may collide with the interests of the state and in this case, it is important having the access to a legal provision allowing exceptions.

"Restrictions" as such are missing in the CCPA. The word appears in several provisions of the legal framework, but these do not cover other states' law and are mainly observed together with words such as "contractor". This is probably, due to the fact, that the CCPA covers one state, California, but the EU GDPR covers more than one country.

3.5 Summary and conclusions

The GDPR contains 173 recitals and eleven chapters with its 99 articles. The recitals are on one hand, describing the reasons behind the legislation, on the other hand – developing further the content of the legal provisions. E.g., **Recital 15** aims at the technology neutrality. This means that personal data linked to natural persons "should be technologically neutral and should not depend on the techniques used". This is very important information in addition to, inter alia, **Articles 2** and **3** bringing forth the applicability of the GDPR to the processing of personal data, but with the word combination "technology neutrality" being absent. The sentences encountered both in recitals and in articles are easy to follow.

The legal framework's division in eleven chapters with its clear headlines, where Chapter 1 aims at subject-matter and objectives, Chapter 8 (not analysed in this thesis, but is worth to be mentioned) – remedies, liability and penalties, and so forth, facilitates the navigation when studying the provisions.

The cited case law together with guidelines demonstrate that the interpretation of a legal provision often is based on the context.

4. The California Consumer Privacy Act

4.1 The CCPA

4.1.1 Introduction

First of all, it is important to mention the California Consumer Privacy Act (CCPA), which came into effect on 1st January 2020. The purpose of this legal framework was to set up rules for businesses regarding the collection and sale of California consumers' personal information.[40]

The California Privacy Rights Act (CPRA), also titled as Proposition 24, amended the CCPA. Sometimes this Act is being referred to as "CCPA 2.0". The CPRA took effect on 16th December 2020, but became "operative" first on 1st January 2023.[41] New regulations went into effect on 29th March 2023. While the CCPA provides Californian consumers to exercise more control over the personal information businesses collect about them, the CPRA added supplementary consumer privacy rights. An agency was established with responsibilities such as the enforcement of the law and enlightening the public on their rights under the law. One of the new

[40] Bloomberg Law's webpage.

[41] Ibid.

features in the CCPA, is the consumer's right to delete personal information businesses have collected form them (subject to some exceptions).[42]

4.2 The structure, the purpose and the scope of the CCPA

The CCPA contains 45 sections in total. These have not been arranged and placed in chapters, comparing to the GDPR-model. Recitals in the CCPA are completely absent. Therefore, the historical background of the CCPA and its purposes have been introduced below with help from "The California Privacy Rights and Enforcement Act of 2020", explaining in a very clear manner why the CCPA has been adopted. The most prominent parts of the CCPA have been summarised in Section 4.3. A direct link to the CCPA has been included as a footnote for the reader.

4.2.1 Section 2 – "Findings and Declarations"

Section 2 consists of paragraphs A to H, which describe the proposition to the amendment of "The California Consumer Privacy Act of 2018". Due to the limited space of this paper, the most prominent parts will be summarized and presented herein. Paragraph A takes one back to 1972, when California voters contributed to the inclusion of the right of privacy among the "inalienable" rights of all people, in the California Constitution. The cause was the escalating intrusion into personal freedom and security due to the increased data collection and usage in contemporary society. The amendment meant a legal and enforceable constitutional right of privacy for every Californian. The crucial part of this right of privacy is the individuals' control over the usage of their personal information, including its sale. The rest of the paragraphs develop the background further. After the approval of the constitutional right of privacy, the California Legislature has adopted specific mechanisms to safeguard Californians' privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light. However, the consumers had no right to acquire a knowledge

[42] The California Privacy Protection Agency's webpage.

of what personal information a business had collected about them or how they used it. Similarly, they had no possibility to impact businesses not to sell the consumer's personal information.

A change could be observed in 2018, when more than 629,000 California voters signed petitions, which led to the Legislature enacting the California Consumer Privacy Act of 2018 (CCPA) into law. The CCPA permits California consumers to learn what information a business has collected about them, to delete their personal information, to stop businesses from selling their personal information or use it for cross-context behavioural advertising. California consumers were also attributed the right to make businesses accountable if they do not take appropriate measures to safeguard their personal information. Even before the CCPA had come into effect, businesses made an attempt to weaken the law. More than a dozen bills to amend the CCPA were proposed to be modified by the members of the Legislature. The amendment was therefore important in order to impose restrictions on businesses' use of personal information and how long they can keep it, allowing consumers to hinder the use of their sensitive personal information for advertising and marketing and to impose on businesses a correction of inaccurate information about consumers.

Due to scandals regarding data security breaches and the use of personal information for political intentions had illustrated that California law required an amendment. In situations where a business uses a consumer's personal information for the benefit of its own political interests, the business should be obliged to disclose that information to the consumer and should also disclose such use to the state. Similarly, business should be held responsible for data security breaches and inform consumers in cases where consumers' "most sensitive information" has been made vulnerable. An independent watchdog's obligation should comprise the protection of consumer privacy and making sure that businesses and consumers are well-informed about their rights and obligations. The watchdog should also strongly enforce the law against businesses in cases of violation of consumers' privacy rights.

4.2.2 Section 3 – "Purpose and Intent"

Section 3 aims at the principles lying behind the implementation of the Act and is divided into point A "Consumer Rights", point B "The Responsibilities of Businesses" and point C "Implementation of the Law".

Point A "Consumer Rights"

Point A is divided into seven subpoints: consumers' right to know who is collecting their personal information, how it is being used, and to whom it is disclosed; consumers' right to the control of their personal information, including their sensitive personal information, and meaningful options over how it is collected, used, and disclosed; consumers' right to have access to their personal information and consumers should be given the possibility to correct it, delete it, and take it with them from one business to another; consumers' and their approved agents' authorisation to exercise these rights through easily accessible self-serve tools; consumers' right to exercise these rights without being penalised for doing so; consumers' right to hold businesses responsible for failing to take appropriate measures to protect their most sensitive personal information from hackers and security breaches; consumers' right to benefit from businesses' use of their personal information.

Point B "The Responsibilities of Businesses"

Point B consists of eight subpoints. The first subpoint requires businesses to inform consumers in a clear manner about how they collect and use personal information and how they can exercise their rights and choices. Businesses should *not* assemble the personal information of children without consent. The second subpoint aims at businesses' obligation to collect consumers' personal information for specific, explicit, and legitimate purposes. Further collection, usage, disclosure of consumers' personal information should only be aligned with those purposes. Subpoint three obliges businesses to collect consumers' personal information only to the extent that it is relevant and limited to what is necessary in connection with the purposes for which it is being collected, used, and shared. Fourth subpoint indicates that businesses should provide consumers or their authorised agents "with

easily accessible self-serve tools that allow consumers to obtain their personal information, delete it, or correct it, and to opt-out of the sale of their personal information, including for cross-context behavioural advertising, and the use of their sensitive personal information for advertising and marketing". Subpoint five aims at prohibiting businesses to penalize consumers for exercising these rights. Subpoint six obliges businesses to disclose whenever consumers' personal information is used in order to advance their own political purposes. Seventh subpoint states that businesses should take appropriate measures to protect consumers' personal information from a security breach. Subpoint eight takes aim at the businesses' responsibility in case of violation consumers' privacy rights, highlighting the fact that penalties should be higher when the violation influences children.

Point C "Implementation of the Law"

Point C consists of four subpoints. The first subpoint indicates that the rights of consumers and the responsibilities of businesses should be implemented with the goal of maximising consumer privacy. Second subpoint states that businesses and consumers should be informed about their responsibilities and rights in a clear manner. Third subpoint highlights the importance of the law adapting to technological changes. Fourth subpoint states following: "Businesses should be held accountable for violating the law through vigorous administrative and civil enforcement".

4.3 The legal provisions of the CCPA

4.3.1 Introduction

Following subsections are dedicated to the sections (the legal framework uses this word instead of "articles" encountered in the GDPR).[43]

[43] The California Consumer Privacy Act (the CCPA): https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (Accessed on 25th May 2023).

4.3.2 General Duties and Obligations of Businesses

Section 1798.100. "General Duties of Businesses that Collect Personal Information"

Section 1798.100 consists of points (a) to (f). Point (a) reads: "A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following:" and contains three points. The first one aims at the categories of personal information to be collected or uses and the purposes for which these are being collected. (A corresponding provision can be found in the Art. 5(1)(b) of the GDPR). The information should also contain whether that personal information is sold or shared. Second point treats the collection of sensitive personal information. In case the business collects sensitive personal information (Art. 9 of the GDPR covers sensitive data), the categories of the latter and the purposes for which the categories of sensitive personal information are collected or used, should be communicated to the consumer (the communication about the collection of the personal data regarding a data subject, should be provided in a like manner in accordance with Articles 14-15 of the GDPR). Like in the first point, it is required to precise whether that information is sold or shared. Both points indicate the prohibition of treating the personal information for "additional purposes that are incompatible with the disclosed purpose…". Third point indicates the length of time the business plans to hold on to each category of personal information, including sensitive personal information. A business shall not store a consumer's personal information or sensitive personal information for longer than it is reasonably necessary for the disclosed purpose.

Point (b) indicates that a business that is acting as a third party and manages the collection of personal information about a consumer, may live up to the conditions set out in subdivision (a), by bringing forth the required information notably on the homepage of its internet website.

Point (c) aims at the proportionality: a business shall collect, use, store and share a consumer's personal information only if necessary and proportionate in relation to the purposes for which the personal information was collected or processed (the same principle is to be found in Art. 5(1) c) of the GDPR).

Point (d) indicates the necessity of an agreement between a business and a third party in situations where a business, e.g., sells a consumer's personal information to a third party or discloses it to a service provider. The contract should include following: (1) a specification whether the personal information is sold or disclosed by the business, but only for a limited and specified purposes; (2) an obligation of the third party, service provider, or contractor to comply with relevant requirements and to provide "the same level of privacy protection as is required…"; (3) an allowance of the business rights to ensure that the third party, service provider, or contractor uses the personal information transferred in accordance with the business' obligations; (4) a requirement of the third party, service provider, or contractor to inform the business in case where it can no longer comply with its obligations; (5) the business' right, upon notice, including under paragraph (4), to act in a suitable manner in order to stop unauthorised use of personal information.

Point (e) lays down an obligation on businesses to implement "reasonable security procedures and practices" when collecting a consumer's personal information, in order to protect the latter from, inter alia, unauthorised or illegal access. A reference is made to Section 1798.81.5. (f) and to paragraph (3) of subdivision (a) of Section 1798.185.

Point (f) states: "Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185."[44]

Section 1798.135. "Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Information"

Section 1798.135 contains subdivisions (a) to (g). Due to the long article and to the space limitation[45], a summary with the most prominent parts has been provided below.

[44] Amended November 3, 2020, by initiative Proposition 24, Sec. 4. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.

[45] In this section, the sentences containing phrases "sale of personal information" and "share of personal information", also include "use of personal information" and "use of sensitive information", but have been left out due to the space limitation.

Subdivision (a) aims at businesses' obligation to, inter alia, (1) provide a clear and visible link on the business's internet homepage, titled "Do Not Sell or Share My Personal Information", to an internet web page permitting a consumer, or a person authorised by the consumer, to opt-out of the sale or sharing of the consumer's personal information, when a business that sells or shares consumers' personal information or uses or disclosed consumers' sensitive personal information for other purposes than those stated in subdivision (a) of Section 1798.121. The rest of Section 1798.135 indicates also that a business should facilitate for a consumer or a person authorised by the consumer, to revoke the consent via the web page. The consent web page shall comply with technical specifications according to paragraph (20) of subdivision (a) of Section 1798.185.

A business shall *not* demand a consumer to create an account or bring forth additional information "beyond what is necessary…". A business shall also provide a description of a consumer's rights in accordance with Sections 1798.120 and 1798.121, together with a separate link to the "Do Not Sell or Share My Personal Information" internet web page and a separate link to the "Limit the Use of My Sensitive Personal Information" internet web page. It is a business's responsibility to secure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance, are aware of the requirements as per, inter alia, Sections 1798.120 and 1798.121. If a consumer exercise his/her right to opt-out of the sale or sharing of their personal information, the business shall withhold from selling or sharing the consumer's personal information and wait for a minimum of 12 months before seeking an authorisation of the sale or sharing of the consumer's personal information again.

There is a possibility for a consumer to authorise another person to opt-out of the sale or sharing of the consumer's personal information on his/her behalf. If a business informs a person authorised by the business to collect personal information, about a consumer's opt-out request, the person is only allowed to thereafter, to use the consumer's personal information for a business purpose specified by the business, or as otherwise permitted by the latter, and shall therefore be forbidden to, inter alia, selling or sharing the personal information. If a business informs a person authorised by the business to collect personal information, about a consumer's opt-out request, the business shall *not* be liable if the person receiving

the request violates the restrictions and the business, at the time of communicating the opt-out request, did not have actual knowledge, or reason to suspect, that the person plans to commit such a violation.[46]

In comparison to the GDPR, a data controller's obligation to communicate to a data subject / consumer and the treatment of sensitive data, inter alia, have been placed much earlier in the CCPA. Overall, a data controller's obligations are very similar in both legal frameworks.

4.3.3 Consumers' Rights

Section 1798.105. "Consumers' Right to Delete Personal Information"

Section 1798.105 consists of points (a) to (d), where point (a) aims at a consumer's right to request a business to delete any personal information about the consumer. (A corresponding provision can be found in the Art. 17 of the GDPR.) Point (b) refers to Section 1798.130, stating a business' obligation to inform the consumer about his/her rights to request the deletion of the consumer's personal information.

Point (c) contains three subdivisions. Subdivision (1) states that if a business receives a verifiable consumer request from a consumer to erase the consumer's personal information according to subdivision (a), shall delete the consumer's personal information from its database and inform any service providers or contractors to delete the consumer's personal information. (The corresponding provision is the Art. 19 of the GDPR.) All the third parties to whom the business has sold or shared the personal information, should also erase the consumer's personal data. Subdivision (2) indicates the business' possibility to keep a confidential record of deletion requests solely based on the purpose of precluding the personal information of a consumer who has put forward a deletion request from being sold, e.g., for compliance with laws. Subdivision (3) aims at a service

[46] Amended November 3, 2020, by initiative Proposition 24, Sec. 13. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.

provider's or contractor's obligation to cooperate with the business and, inter alia, shall delete personal information about the consumer, at the direction of the business, according to a verifiable consumer request.

Point (d) allows a business, or a service provider or contractor to keep the consumer's personal information even if the latter has required a deletion of his/her personal data and provides eight exceptions. (The corresponding exceptions can be found in the Art. 17(3) of the GDPR.)

Subdivisions (1) to (8) are covering, inter alia, the completion of a transaction for which the personal information was collected, or fulfil a contract between the business and the consumer; help to ensure security and integrity; identification and repairing errors; exercising free speech, ensure the right of another consumer to exercise that consumer's right of free speech; compliance with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code; engaging in public or peer-reviewed, inter alia, scientific research, conforming to all other applicable ethics and privacy laws; enabling solely necessary internal uses; compliance with a legal obligation.[47]

Section 1978.106. "Consumers' Right to Correct Inaccurate Personal Information"

Section 1978.106 consists of points (a) to (c). (A corresponding provision is to be found in Art. 16 of the GDPR.) Point (a) indicates a consumer's right to request a business to rectify the consumer's inaccurate personal information. Point (b) covers a business' obligation to inform the consumers about their right to request correction of inaccurate personal information, according to Section 1798.130. Point (c) states that a business receiving a verifiable consumer request to correct inaccurate personal information, shall use commercially reasonable efforts to correct the information. A reference to Section 1978.130 and regulations adopted pursuant to paragraph (8) of subdivision (a) of Section 1798.185.[48]

[47]Amended November 3, 2020, by initiative Proposition 24, Sec. 5. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.
[48]Added November 3, 2020, by initiative Proposition 24, Sec. 6. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.

Section 1798.110. "Consumer's Right to Know What Personal Information is Being Collected. Right to Access Personal Information"

Section 1798.110 contains points (a) to (c). (Cf. Art. 15 of the GDPR.) Point (a) states a consumer's right to request that a business collecting personal information about the consumer inform the latter the following: (1) the categories of personal information it has collected about that consumer; (2) the categories of sources from which the personal information is collected; (3) the business or commercial purpose for collecting, selling, or sharing personal information; (4) the categories of third parties to whom the business discloses personal information; (5) the specific pieces of personal information it has collected about that consumer.

Point (b) states, inter alia, that a business that collects personal information about a consumer shall disclose to the consumer, according to subparagraph (B) of paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer…". Point (c) refers to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130 and states that a business collecting personal information about consumers shall disclose following: (1) the categories of personal information it has collected about consumers; (2) the categories of sources from which the personal information is collected; (3) the business or commercial purpose for collecting, selling or sharing personal information; (4) the categories of third parties to whom the business discloses personal information; (5) that a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.[49]

Section 1798.115. "Consumers' Right to Know What Personal Information is Sold or Shared and to Whom"

Section 1798.115 consists of subdivisions (a) to (d). Subdivision (a) states that a consumer has a right to request a disclosure when a business sells or shares the consumer's personal information. Points (1) to (3) describe the type of information that should be disclosed: (1) the categories of personal information that the business collected about the consumer; (2) the categories of personal information that the

[49] Amended November 3, 2020, by initiative Proposition 24, Sec. 7. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.

business sold or shared about the consumer and the categories of third parties to whom the personal information was sold or shared; (3) "the categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.". Subdivision (b) precises a business' obligation to disclose the information to the consumer upon receipt of a verifiable consumer request from the consumer, in situations where that business sells or shares personal information about that consumer for a business purpose. A reference is provided to paragraph (4) of subdivision (a) of Section 1798.130. Point (c) contains the same information as point (b), but the difference consists in the fact that "a verifiable consumer request" is missing in the point (c) and a reference is made to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130 instead. Point (d) states that a third party that a consumer's personal information has been sold to, or shared with, shall not sell, or share the information without explicitly notifying the consumer and providing a possibility to "exercise the right to opt-out" according to Section 1798.120.[50]

Section 1798.120. "Consumers' Right to Opt-Out of Sale or Sharing of Personal Information"

Section 1798.120 consists of subdivisions (a) to (d). (A corresponding provision is to be found in Articles 7(3) and 21 of the GDPR.) Point (a) indicates a consumer's right to opt-out of sale or sharing. In other words, a consumer has a right to stop a business from selling or sharing the consumer's personal information to third parties. Point (b) states a business' obligation to inform the consumers when their personal information may be sold or shared with third parties and that consumers have the right "right to opt-out" of the sale or sharing their personal information. A reference is provided to subdivision (a) of Section 1798.135. According to the point (c), in spite of subdivision (a), a business is prohibited to sell or share the personal information of consumers if the business is aware of that the consumer is less than 16 years old. An exception is allowed, "in the case of consumers at least 13 years old and less than 16 years old, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorised the sale

[50] Amended November 3, 2020, by initiative Proposition 24, Sec. 8. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.

or sharing of the consumer's personal information." Point (d) states that in situations where a consumer indicates to a business not to sell or share the consumer's personal information, or if a consent has not been provided, the business shall be prohibited to sell or share the latter, as per paragraph (4) of subdivision (c) of Section 1798.135.

The rights of data subjects and consumers are almost identical in the CCPA and in the GDPR. A striking difference is that the GDPR uses a broader term. A data subject may be a consumer, but a consumer can only be a consumer. Another difference is that the GDPR is using a "broader" term - "right to object to the *data processing*" or similar, while the CCPA mostly applies the "*sale* of the personal data" and "*the use* of personal information" in relation to consumers.

4.3.4 Case law in relation to the "Do Not Sell My Personal Information" link in the CCPA

One of the "CCPA Enforcement Case Examples" published on the State of California Department of Justice's webpage, takes aim at non-compliant opt-out process and verification procedures, presented below.[51]

People Search Company Updated its Opt-Out and Other CCPA Processes
Industry: Data Broker. Issue: Non-compliant Opt-Out Process and Verification Procedures.

A company responsible for a people search website had a "Do Not Sell My Personal Information" link that worked only on certain browsers, which resulted in consumers landing on a confusing webpage which demanded several additional steps to agree on CCPA requests. The consumers had to agree to terms of service and the privacy policy in the same manner. Whether the consumer was obliged to create an account in order to complete their requests or not, was also unclear. The company had not disclosed CCPA metrics for the previous calendar year either. The notification of alleged non-compliance resulted in, inter alia, the business updating the website so the "Do Not Sell My Personal Information"-link worked on all browsers, updated its California Privacy Page to facilitate the processes of submitting CCPA requests, brought forth alternate methods to submit CCPA requests including simplified alternatives which did not oblige consumers to agree

[51] State of California Department of Justice's webpage.

to terms of service and the privacy policy. The company also clarified on the webpage that consumers are not required to create an account.[52]

Online Dating Platform Added Do Not Sell My Personal Information Link and Sales Disclosures
Industry: Online Dating. Issue: No “Do Not Sell My Personal Information” Link; Non-Compliant Privacy Policy

Another relevant case involves a business, an online dating platform. The company sold personal information but did not have a “Do Not Sell My Personal Information” link on its homepage and did not provide the information in its privacy policy about what personal information it sold. According to the business, when a user clicked on the button “accept sharing” when creating a new account, it was sufficient as consent to sell personal information. The business got notified of alleged non-compliance, which led to the business creating a clear “Do Not Sell My Personal Information” link and, to updating its privacy policy with compliant sales disclosures.[53]

4.4 Summary and conclusions

In comparison to the GDPR, one should have more time to read through the CCPA, at least the first time. The lack of a clear structure and a division into, e.g., two or three chapters, makes it harder to follow the content of the provisions. Some of the sections are too long and could have been divided in two parts as well. Except for some nuances, the content of the CCPA is similar to the one provided in the GDPR. As regards to the wording, the CCPA applies the term “consumer” instead of “data subject” encountered in the GDPR. Further on, the CCPA uses very often “sale of personal information” and “use of personal information" in comparison to “the processing of personal data” as per GDPR. Most of the time, the text of the provisions in the CCPA is easy to grasp. However, some sections could have been written more “smoothly”. Case law shows that some businesses are not compliant with the CCPA.

[52] Ibid.
[53] Ibid.

5. Summary and conclusions

After having studied in detail the GDPR and the CCPA, one realises how both frameworks are similar one to another and yet, different, at the same time. This chapter is providing the answer to the question that has been leading the research:

What are the principal similarities and/or differences between the GDPR and the CCPA?

The structure

In terms of *structure*, the GDPR is to be preferred. With its 173 recitals and 99 articles organised in eleven chapters, the legislation permits the navigation in a very smooth manner. Headings of the chapters and those of the legal provisions have been formulated in a short and concise manner, capturing very well its core. The main *difference* between the frameworks is the absence of recitals in the CCPA, containing solely articles (the "sections") with no division into chapters. However, the headings of the legal provisions are clear enough to grasp the idea of its content. This is the main *similarity* between the two frameworks. The CCPA consists of 45 sections (corresponding to articles in the GDPR). Both frameworks are using points (a) to (d) and so forth within the legal provisions, in order to avoid too long paragraphs. Articles 12 and 15 of the GDPR are examples of provisions, that could have been divided in two articles, as they are too long. In the CCPA, Sections 1798.130, 1798.140, 1798.145 (not summarised in this thesis) are examples of provisions that could have been improved as well.

The content and its main purpose

The main purpose of the two legislations is quite similar one to another in terms of protecting a data subject (GDPR) and a consumer (CCPA) when his or her personal information/data is either "processed" and "collected" (GDPR and CCPA) or when the information/data is being "sold" and/or "used" (CCPA). The content in the CCPA is mainly addressed to a business, comparing to the GDPR which takes aim at a "data controller" and a "data processor", both being broader terms.

The language

Some of the legal provisions in the CCPA could have been written in a more "smooth" manner, with shorter sentences (or by adding commas). However, most of the time the text is easy to follow. Similarly, the legislator of the GDPR has also made a great job when formulating its provisions, but there are a couple of articles, where an improvement could have been made.

The wording

Both frameworks use the word "shall" to a great extension, which strengthens a provision's position. "Natural person" and "collecting personal information" are encountered in both legislations (although, in GDPR one can find "personal data" instead of "personal information"). While the GDPR is using the term "data subject", the CCPA has preferred making a reference to "consumer". Furthermore, "processing", "collecting" are both terms encountered in the CCPA and in the GDPR. Instead of the broad terms "data controller" and "data processor", the legislator of the CCPA has chosen the word "business". In comparison to the GDPR lacking the term "sale of personal data", the CCPA contains the wording "sale of personal information" in many of its provisions.

Overall, the main purpose is shared by both legislations. One is covering "a data subject's personal data", the other one – "a consumer's personal information", but the aim is the same – the protection. There are a lot of similarities and a lot of minor differences between the frameworks. However, the GDPR gives a slightly better overview of its content, mainly due to its structure.

Reference list / Bibliography

Official Publications

Sweden

The official website of Integritetsskyddsmyndigheten (IMY), Swedish Authority for Privacy Protection. “The purposes and scope of GDPR”: https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/the-purposes-and-scope-of-gdpr/ (Accessed on 22nd May 2023).

European Union

Court of Justice of the European Union: https://curia.europa.eu/jcms/jcms/j_6/en/ (Accessed on 24th May 2023).

The Official website of the European Union:

”The History of the General Data Protection Regulation” https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (Accessed on 6th April 2023).

“United States: EU trade relations with the Unites States. Facts, figures and latest developments.” https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en (Accessed on 6th April 2023).

European Commission’s website: “Primary versus secondary law”. https://commission.europa.eu/law/law-making-process/types-eu-law_en (Accessed on 7th April 2023).

European Data Protection Board’s webpage, “Guidelines 01/2022 on data subject rights – Right of access”, p. 5. Version 2.0. Adopted on 28 March 2023. https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (Accessed on 18th May 2023).

Unites States

Bloomberg Law: https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra/ (Accessed 3rd May 2023).

State of California Department of Justice's webpage: https://oag.ca.gov/privacy/ccpa/enforcement (Accessed on 17th May 2023).

The California Privacy Protection Agency's webpage: https://cppa.ca.gov/faq.html (Accessed on 10th May 2023).

Literature

Calboli, Irene: A call for Strengthening the Role of Comparative Legal Analysis in the United States, p. 614. St. John's Law Review. Volume 90, Fall 2016, Number 3 – Article 5.

Frydlinger, David, Edvardsson Tobias, Olstedt Carlström Caroline, Beyer, Sandra: "GDPR – Juridik, organisation och säkerhet enligt dataskyddsförordningen". Norstedts Juridik AB, 2018.

Hettne, Jörgen, Otken Eriksson, Ida: "EU-rättslig metod – Teori och Genomslag I Svensk Rättstillämpning". Norsteds Juridik AB, 2011.

Legrand, Pierre: "John Henry Merryman and Comparative Legal Studies: A Dialogue." The American Journal of Comparative Law, Winter, 1999, Vol. 47, No. 1 Oxford Journals. Oxford University Press. https://www.jstor.org/stable/840997 (Accessed on 20th May 2023).

M. Fine, Toni: "American Legal Systems", chapter 2 *The American Legal System Made Easy*, p. 13. Anderson Publishing, a member of the LexisNexis Group 1997. https://www.americanbar.org/content/dam/aba-cms-dotorg/products/inv/book/131991070/Chapter%202.pdf (Accessed on 11th May 2023).

Online sources

Californian Compliance blog "Truevault". https://www.truevault.com/learn/ccpa/what-is-the-ccpa (Accessed on 10th May 2023).

Dictionary Cambridge: https://dictionary.cambridge.org/dictionary/english/treatise (Accessed on 25th May 2023).

Jerome Hall Law Library – Maurer School of Law https://law.indiana.libguides.com/c.php?g=19799&p=112316 (Accessed on 25th May 2023).

"Lagtolkning" / "Judicial interpretation": https://lagen.nu/begrepp/Lagtolkning (Accessed on 6th April 2023).

Cases

European Union

Court of Justice of the European Union

Case C-101/01 – Lindqvist (2003)

Case C-131/12 – Google vs. Spain (2014)

Case C-154/21 – RW vs. Österreichischische Post AG (2023)

United States

Online Dating Platform Added Do Not Sell My Personal Information Link and Sales Disclosures
Industry: Online Dating. Issue: No "Do Not Sell My Personal Information" Link; Non-Compliant Privacy Policy

People Search Company Updated its Opt-Out and Other CCPA Processes Industry: Data Broker. Issue: Non-compliant Opt-Out Process and Verification Procedures.