BRATISLAVA LAW REVIEW

PUBLISHED BY
THE FACULTY OF LAW,
COMENIUS UNIVERSITY
IN BRATISLAVA

ISSN (print): 2585-7088
ISSN (electronic): 2644-6359

APPLY OR NOT TO APPLY? A COMPARATIVE VIEW ON TERRITORIAL APPLICATION OF CCPA AND GDPR /

Matúš Mesarčík

JUDr. Matúš Mesarčík, PhD., LL.M; Comenius University in Bratislava, Faculty of Law, Institute of Information Technology Law and Intellectual Property Law; Šafárikovo nám. 6; 810 00 Bratislava; Slovakia; matus.mesarcik@flaw.uniba.sk. ORCID: 0000-0003-3311-5333.

The article was drafted with the support from the project Jean Monet Module n. 611579-EPP-1-2019-1SK-EPPJMO-MODULE "Digital Single Market as a New Dimension of EU Law."

Abstract: *A new era of data protection laws arises after the adoption of the General Data Protection Regulation (GDPR) in the European Union. One of the newly adopted regulations of processing of personal data is Californian Consumer Privacy Act commonly referred to as CCPA. The article aims to fill the gap considering a deep analysis of the territorial scope of both acts and practical consequences of the application. The article starts with a brief overview of privacy regulation in the EU and USA. Introduction to GDPR and CCPA follows focusing on the territorial scope of respective legislation. Three scenarios of applicability are derived in the following part including practical examples.*

Key words: *data protection; privacy; GDPR; CCPA; territorial scope*

Submitted: 21 March 2020
Accepted: 15 November 2020
Published: 31 December 2020

Suggested citation:
Mesarčík, M. (2020). Apply or not to Apply? A Comparative View on Territorial Application of CCPA and GDPR. *Bratislava Law Review*, 4(2), 81-94. https://doi.org/10.46282/blr.2020.4.2.171

1. INTRODUCTION

The area of data protection is one of the most discussed subjects in the current public debate. Traditional conservatism of law is slowly adapting to a new technological reality. Impact of technology on privacy may be enormous, therefore new legislation is needed to regulate and reflect the latest development (Andraško, 2017). New laws attempting to regulate the area of data have been adopted on both sides of the Atlantic Ocean and although the approach to legal protection of privacy is different, the fundamentals are similar.

The article examines two core legislative developments within the European Union and the United States of America considering the protection of privacy (or informational privacy) in regards to territorial scope. The emphasis is put on General Data Protection Regulation (GDPR) and California Consumer Protection Act (CCPA). The questions discussed in the article are of essential importance as cross-border commerce is one of the fundamental pillars of the world economy. The controllers in the EU and the USA shall carefully assess if data protection legislation is applicable especially in regards to territorial scope of laws. The in-depth research on the specific issue of the territorial applicability is generally absent (see Kessler, 2019 or Umhoefer, 2019). The second part

of the article is focused on the comparison of different backgrounds and approaches to the regulation of informational privacy in the EU and the USA. The third part deals with analysis of respective provisions of GDPR and CCPA related to territorial scope. The fourth part provides a brief overview of practical examples when laws are applicable or non-applicable to companies based on their residence.

2. FOUNDATIONS OF EU & US PRIVACY LAWS

It is of the essence to outline different background of EU and US privacy protection. First of all, each model of protection of privacy should be founded on several basic principles drafted by the Organisation for Economic Co-operation and Development (OECD). The principles are stated in OECD Guidelines[1] and include collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle and accountability principle. Each party of the OECD (including most of the member states of the EU and USA) shall implement the principles into their privacy regulations.[2] It is therefore important to emphasize that many systems of protection of privacy are governed by same or similar principles although the approach itself may vary. These principles are implemented into different models of protection of privacy.

Kuner (2013) differentiates among four models of protection of privacy: complex, sectoral, self-regulating model and co-regulating model. Complex model represents a system with general regulation applicable to private and public sector with independent data protection authority responsible for ensuring compliance with data protection rules in the territory of the state. General regulation is often supplemented by specific sectoral regulation. An example of this approach is the European Union's GDPR and specific regulations (e.g. ePrivacy directive).[3] The second model of implementation is sectoral model. General regulation is absent, and each sector is regulated by specific tailor-made legislation. This is the case of the USA where many acts regulating privacy or data protection exist for different sectors (e.g. Health Insurance Portability and Accountability Act of 1996 for processing of personal information related to health). The self-regulating model is very similar to sectoral model, but regulation is not represented by specific acts rather by codes of conducts or sectoral codes drafted and adopted by market players from specific sectors. The co-regulating model is a combination of sectoral and self-regulating models. Specific legal framework adopted by legislator exists and the framework is complemented by sectoral rules developed by sectors. The latter is represented in Indonesia.

As highlighted above, the implementation of OECD principles is different in the EU and the US resulting in complex and sectoral model of regulation. However, some authors argue that the implementation of the OECD principles achieves the same results with different processes (see Bennett, 1988). It may be added that protection of privacy as such is approached differently in these countries from the human rights perspective. Within the European Union the right to data protection exists and is a fundamental part of the Charter of fundamental rights of EU (hereinafter known as "the Charter"). However European legislation differentiates between right to privacy and right to data protection and treats them like two separate rights. Article 7 of the Charter states that "*everyone has*

[1] Annex to the Recommendation of the Council of 23rd September 1980: Guidelines governing the protection of privacy and transborder flows of personal data.
[2] See e.g. Article 5 GDPR or Convention 108.
[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. OJ L 201, 31.7.2002, pp. 37–47.

the right to respect for his or her private and family life, home and communications." Proposal of the new ePrivacy Regulation[4] explicitly refers to the Article 7 in proposed Recital 1.[5] Article 8 of the Charter confers right to data protection according to which "*everyone has the right to the protection of personal data concerning him or her.*"[6] Furthermore the Charter states fundamentals of processing of personal data in section 2 of the pertinent article: "*Personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*" Supervision over the data protection area shall be deemed by independent supervisory authorities.[7] The specification of Article 8 is represented by General Data Protection Regulation.[8]

Protection of (information) privacy in the United States of America is not derived from human rights legislation. The protection of privacy has evolved throughout the years in different sectors. Absence of general privacy regulation is often criticized by many authors (Bignami, 2007). It has to be also noted that federal legislation is often supported by specific state legislation.

From the historical point of view (see Solove, 2016) the most notable cornerstone was the publication of Warren and Brandeis´s article The Right to Privacy emphasizing the importance of having a remedy in privacy-related cases (Warren & Brandeis, 1890). In 1960 William Prosser created a typology of privacy torts based on the above-mentioned article (Prosser, 1960). Supreme Court of the United States continually developed protection of privacy based on the fourth amendment of the US Constitution reading: "*The right of the people to be secure in their persons, houses, papers, and effects, [a] against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"[9] However, the provision protects only US citizens against unreasonable searches and seizure and does not constitute general privacy protection as in the Convention or the Charter (see Zanfir, 2012). US government in its developed legislation tackled contemporary issues of privacy protection.[10] Privacy laws are widely fragmented in common law, federal legislation, state law and state constitutions (Levin & Nicholson, 2005). Wide range of privacy rules are set forth as consumer protection and sector specific. These acts include The Fair and Accurate Credit Transactions Act 2003 or the CAN-SPAM Act 2003 (see more in Pernot-LePlay, 2020a). The protection of consumers is closely related to enforcement of rights of data subjects similar to the ones provided by GDPR. The latter is a reason for comparing consumer privacy protection in the selected state with legislation adopted in

[4] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

[5] *„Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the parties involved in a communication. The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e-mail, internet phone callsand personal messaging provided through social media."*

[6] Article 8 sec. 1 of the Charter.

[7] Article 8 sec. 3 of the Charter.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, pp. 1–88.

[9] E.g. Katz v. United States, 389 U.S. 347 (1967).

[10] See e.g. Telephone Consumer Protection Act of 1991 or Driver´s Privacy Protection Act of 1994.

DOI: 10.46282/blr.2020.4.2.171

the EU. The US legislator attempted to adopt comprehensive privacy legislation in the form of The Consumer Privacy Bill of Rights in 2012, however the bill never became a law. On the other hand, several states show convergence of EU data protection laws into their state legislation (Pernot-LePlay, 2020b). One of such laws is CCPA.

From the point of view of future development, it shall be emphasized that the USA plans to adopt general privacy regulation on the federal level. This aim is supported by the fact that the USA declared that the country may become a party to the Council of Europe's Convention 108.[11]

3. TERRITORIAL SCOPE

3.1. Territorial scope of the GDPR

GDPR is comprehensive data protection law applicable in the EU. Based on the material scope the regulation applies to the processing of personal data[12] wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[13] The material scope of the GDPR is broad and is not limited only to some processing operations like sale, erasure or analysis of personal data.

Territorial scope of GDPR is set out in Article 3. The Article states three regimes of applicability of GDPR considering territorial aspects of processing of personal data. The first regime applies *"to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."*[14] The second regime is applicable when controller or processor is established outside EU but processes personal data of data subjects located in the EU with regard to (i) the offering of goods and services regardless requirement of payment or (ii) monitoring of behaviour.[15] The third regime is applicable to entities outside of EU by virtue of public international law.[16] Territorial scope of GDPR has been explained in published Guidelines 3/2018 on the territorial scope of the GDPR[17] drafted by European Data Protection Board (EDPB) and provides valuable guidance to applicability of the Article 3 GDPR.

1. First regime – application of establishment criterion

Application of establishment criterion regime is composed of three criteria that have to be assessed: (a) if an establishment is in the EU, (b) if processing of personal data is carried out in the context of the activities of an establishment and (c) if it is applicable regardless of whether the processing takes place in the EU or not. Such threefold approach is also preferred by EDPB. All criteria shall be fulfilled cumulatively.

[11] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the second annual review of the functioning of the EU-U.S. Privacy Shield, https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf , p. 7 (accessed on 20.03.2020).

[12] Personal data being identified as *„any information relating to an identified or identifiable natural person ('data subject')."* Article 4 (1) GDPR.

[13] Article 2 (1) GDPR.

[14] Article 3 (1) GDPR.

[15] Article 3 (2) GDPR.

[16] Article 3 (3) GDPR.

[17] European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).* Available at: https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en (accessed on 20.03.2020).

The first criterion to be taken into account is whether processing activities are conducted by "an establishment in the EU." GDPR does not define what an establishment is. However, recital 22 GDPR states that "*Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.*" The notion of establishment has been further clarified by the Court of Justice of European Union (hereinafter known as the "CJEU") in cases *Weltimmo*[18] and *Google Spain*.[19] In *Weltimmo* CJEU noted that establishment within the meaning of the law "*extends to any real and effective activity — even a minimal one — exercised through stable arrangements.*"[20] In terms of exercise through stable arrangements the CJEU added that "*both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned.*"[21] In terms of services provided via internet the threshold for stable arrangement may be quite low.[22]

An example of application of the first regime might be when US-based company has a branch in the European Union acting as "EU Headquarters."

Context of the activities of an establishment is the second criterion to be considered. EDPB emphasizes case-by-case analysis and approach.[23] The criterion shall be assessed via relationship between a data controller or processor outside the EU and revenue raised in the EU. An inextricable link is a prerequisite as per the decision of CJEU in the *Google Spain* case.[24] If the inextricable link between a company established outside EU and EU establishment is found, processing activities of the EU establishment shall fulfil the criterion in question. According to the older opinion of Article 29 Working Party (former EDPB) the revenue may also present evidence of an inextricable link.[25] "*The EDPB recommends that non-EU organisations undertake an assessment of their processing activities, first by determining whether personal data are being processed, and secondly by identifying potential links between the activity for which the data is being processed and the activities of any presence of the organisation in the Union.*"[26]

An example of this situation may be when a US-based company establishes a subsidiary in the territory of EU and the establishment conducts marketing activity in the EU. This is the case when inextricable link is clear as processing of personal data is directly connected to the US-based company and EU subsidiary. The same shall be held towards mutual profitability of activities of aforementioned entities.

[18] CJEU decision in *Weltimmo v NAIH* (C-230/14).
[19] CJEU decision *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12).
[20] Weltimmo, para 31.
[21] Weltimmo, para 29.
[22] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 16 November, p. 6.
[23] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 16 November, p. 7.
[24] Google Spain, para 56 „*the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.*"
[25] Article 29 Data Protection Working Party Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain: „*In addition, the judgement suggests that other business models, and different forms of activity (including revenueraising) in an EU Member State may also trigger the applicability of EU law, although the assessment must be made on a case by case basis.*"
[26] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 16 November, p. 8.

DOI: 10.46282/blr.2020.4.2.171

The third criterion is that the regime under Article 3 (1) is applicable regardless of whether the processing takes place in the EU or not. The emphasis is therefore put on irrelevancy of place of processing activities after fulfilling the first two criteria. After the fulfilment of the two previous conditions the place of processing itself is not an essential feature of applicability GDPR in regards to territorial scope. The case may be illustrated by a US company that collects personal data of data subjects residing in the United States, Mexico and Panama but the processing of datasets is conducted within a branch located in Paris. Although the collection of personal data takes place outside of the EU, the processing of person data takes place in the EU and therefore GDPR is applicable. The same shall be held towards a Paris company that has a legally indistinct branch in the USA that processes personal data. In this case, while the processing activities are taking place in the USA, that processing is carried out in the context of the activities of the company in Paris and thus GDPR is applicable.

2. Second regime – targeting criterion (extra-territorial scope of GDPR)

GDPR is applicable also in cases where an establishment is not located in the territory of the EU. Article 3(2) of the GDPR provides that "*this Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*" The common criterion for both alternative targeting criterions is that it relates to data subjects who are in the Union. The scope is thus not limited by citizenship or residence and the broad application is derived from human rights aspects as founding pillars of the European Union and EU society. The latter is explicitly confirmed by Recital 14 GDPR: "*the protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data*". An example may be a US company without an establishment in the EU that is a provider of a social network mobile app available and directed to consumers from the EU. Processing of personal data of data subjects using this app in Rome or Paris would fall under the territorial scope of GDPR. The situation would be different if the app would be intended only for the US market and not available for download in the European Union.

The first targeting criterion is the offering of goods and services. The offering of services also includes the offering of information society services, defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 as "*any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".[27] Whether the payment has been provided is not of the essence while evaluating the criterion.[28] For fulfilling the criterion the goods or services shall be intentionally offered to data subjects in the EU. The latter confirms Recital 23 GDPR stating that "*in order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.*" However, it is not sufficient to trigger the criterion if website is accessible as such in the territory of EU. More indicating factors include language of the website, delivery to the EU, references of customers from EU or currency used within EU. Interpretation of notion of "directing activity" within the meaning

[27] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 16 November, p. 14.
[28] See more in particular, CJEU, C-352/85, *Bond van Adverteerders and Others vs. The Netherlands State*, 26 April 1988, par. 16, and CJEU, C-109/92, Wirth [1993] Racc. I-6447, par. 15.

of Article 15(1)(c) of Regulation 44/2001 (Brussels I) may be of the essence when determining intention to sell goods and services. The guidance on the notion of directing activity is provided in the CJEU case *Pammer v Reederei Karl Schlüter GmbH & Co* and *Hotel Alpenhof v Heller* (joined cases C-585/08 and C-144/09).[29] Naturally, specific circumstance of each case have to be carefully evaluated and taken into account.

GDPR would be applicable in the situation when a US company without any branches or other establishments in the EU area has a website for selling books and magazines with possible delivery to the EU countries. The website also allows to make a payment in euros and contains references from customers from the EU that have bought books in the past. Those three aspects are strong indications that offering of goods is directed towards EU customers.

The second targeting criterion is monitoring of data subjects' behaviour. Recital 24 GDPR provides clarification of the latter: "*in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.*" As EDPB notices, the scope of Article 3 (2) b) is broader than targeting as such. The article shall be triggered by various monitoring activities including processing personal data via wearables or smart devices.[30] Taking into account the guidance monitoring in line with Article 3 (2) b) may be encompassed within behavioural advertisement; geo-localization activities, in particular for marketing purposes; online tracking through the use of cookies or other tracking techniques such as fingerprinting; personalized diet and health analytics services online; CCTV; market surveys and other behavioural studies based on individual profiles or monitoring or regular reporting on an individual's health status.

An example of targeting criterion in this case would be a US company without establishment in the EU that analyses the data of customers in a shopping mall located in Berlin for the purpose of marketing analysis.

3. Third regime – public international law

Article 3 (3) GDPR constitutes specific legal regime of processing of personal data governed by virtue of public international law. The provision states that "*this Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law*". This regime applies to embassies, consulates and diplomatic missions in general. Respected definitions and statuses of aforementioned entities are governed by the

[29] One or more of the following factors shall be considered: The EU or at least one Member State is designated by name with reference to the good or service offered; The data controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns directed at an EU country audience; The international nature of the activity at issue, such as certain tourist activities; The mention of dedicated addresses or phone numbers to be reached from an EU country; The use of a top-level domain name other than that of the third country in which the controller or processor is established, for example ".de", or the use of neutral top-level domain names such as ".eu"; The description of travel instructions from one or more other EU Member States to the place where the service is provided; The mention of an international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers; The use of a language or a currency other than that generally used in the trader's country, especially a language or currency of one or more EU Member states; The data controller offers the delivery of goods in EU Member States.

[30] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 16 November, p. 19.

DOI: 10.46282/blr.2020.4.2.171

Vienna Convention on Diplomatic Relations of 1961 and the Vienna Convention on Consular Relations of 1963.

3.2. Territorial scope of the CCPA

Discussion of territorial scope of the CCPA shall start with several notes regarding the applicability of the legislation itself. It shall be noted that this is not a federal law applicable to the United States of America as a whole but only to one state – California. Deriving from the name of the act itself, CCPA relates to consumers. The Consumer is defined as a natural person who is a California resident.[31] Based on the California Code of Regulations a California resident is understood to be every individual who is in the State for other than a temporary or transitory purpose and every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are non-residents in light of California Code of Regulations.[32] Obligations in CCPA do not apply to every organization residing in California. CCPA applies under five conditions. The first condition is that the organization conducts business for profit. Secondly, the organization collects consumer´s personal information. Third condition is that the organization determines the purposes and means of the processing of consumer´s personal information. The fourth condition is related to territorial applicability – the company must conduct business in California. The fifth condition is that the company shall meet one of the following conditions: (i) has annual gross revenues in excess of twenty-five million dollars ($25,000,000); and/or (ii) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; and/or (iii) derives 50 percent or more of its annual revenues from selling consumers' personal information.[33] Furthermore, the applicability of CCPA is not limited to the processing of personal information on the Internet (Goldman, 2018).

In regard to territorial applicability, CCPA applies to organizations doing business in California.[34] However, what exactly constitutes doing business in California is not defined in CCPA and may trigger application for companies not having establishment in the territory of the USA. The possibility of extra-territorial applicability of CCPA is also recognized by some authors (Pernot-LePlay, 2020b). Certain aid is provided by California Franchise Tax Board stating that: "*doing business in California if it actively engages in any transaction for the purpose of financial or pecuniary gain or profit in California or if any of the conditions (in law) are satisfied.*" These conditions are explicitly stated in section 23101 of the Revenue and Taxation Code of the California and are as follows: (i) the taxpayer is organized or commercially domiciled in California; (ii) sales, as defined in subdivision (e) or (f) of R&TC 25120, of the taxpayer in California, including sales by the taxpayer's agents and independent contractors, exceed the lesser of $500,000 or 25 percent of the taxpayer's total sales. For purposes of R&TC Section 23101, sales in California shall be determined using the rules for assigning sales under R&TC 25135,

[31] Section 1798.140. 7 (G) CCPA.
[32] Section 17014 of Title 18 of the California Code of Regulations.
[33] Section 1798.140.
[34] Section 1789.140 (c) (1): *„Business means…A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information,* ***that does business in the State of California****, and that satisfies one or more…"*

R&TC 25136(b) and the regulations thereunder, as modified by regulations under Section 25137; (iii) real and tangible personal property of the taxpayer in California exceed the lesser of $50,000 or 25 percent of the taxpayer's total real and tangible personal property; (iv) the amount paid in California by the taxpayer for compensation, as defined in subdivision (c) of R&TC 25120, exceeds the lesser of $50,000 or 25 percent of the total compensation paid by the taxpayer; or (v) for the conditions above, the sales, property, and payroll of the taxpayer include the taxpayer's pro rata or distributive share of pass-through entities. "Pass-through entities" means partnerships, LLCs treated as partnerships, or S corporations.[35]

Furthermore, CCPA states that the obligations imposed on businesses shall not restrict a business's ability to collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of CCPA, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold.[36]

4. COMPARISON AND SCENARIOS OF APPLICABILITY

Taking into account aforementioned findings, the comparison may be drafted and potential scenarios of applicability for companies doing business in the EU and California may be analysed.

In line with distinction of Article 3 GDPR the assessment shall reflect intra-territorial application and extra-territorial application. Taking into account provisions of GDPR and CCPA related to intra-territorial application, both acts are clear on that matter. GDPR applies to processing of personal data conducted within the context of activities of establishment in the European Union. As highlighted above, the interpretation of what the terms "establishment" and "context of activities" mean is very broad and also minimum activity may qualify to fulfil the criterion. CCPA states the criterion as "doing business in California." The term shall be interpreted in line with California Franchise Tax Board. Therefore, the criterion is closely connected to domicile (similarly to establishment) or revenue in the context of taxpaying in California.

Extra-territorial application of GDPR is stated in Article 3 (2) and applies processing of personal data related to offering of goods and services or monitoring of data subjects' behaviour located in the European Union. Two specific criteria are set out to establish extra-territorial applicability of GDPR. The terms are interpreted by recitals and guidelines mentioned above. It is not yet clear if CCPA has extra-territorial application at all as the act remains silent on the issue. However, the rational view is that CCPA should be applicable also to companies not domiciled in California fulfilling other criteria. Especially, out-of-California entity may be caught by CCPA when it meets one of the conditions stated in 23101 of the Revenue and Taxation Code of California.

[35] Section 23101 of the Revenue and Taxation Code of California.
[36] Section 1798.145 (a) (6) CCPA.

DOI: 10.46282/blr.2020.4.2.171

	GDPR	CCPA
Intra-territorial application	- Establishment in the EU criterion (broadly interpreted)	- Doing business in California criterion (domicile or revenue)
Extra-territorial application	- Offering goods or services or monitoring behaviour of data subjects in the EU - International public law applicability	- Probably yes (see criteria in section 23101 of the Revenue and Taxation Code of California)

Figure 1: Comparison of territorial application of GDPR and CCPA. Source: Author

There are three basic scenarios of applicability of GDPR and CCPA considering the above comparison. First scenario is that GDPR and CCPA will be both applicable to the company. Second scenario is when only GDPR will be applicable to the company. Third scenario is when only CCPA will be applicable to the company.

First scenario: Application of both acts (GDPR & CCPA)

The first scenario with applicability of both GDPR and CCPA may be split based on the geolocation of the company.

If we have a company A based in Warsaw or in territory of another EU Member State and the company A process personal data, GDPR applies as per Article 3 (1). It is not essential whether data subjects are located in the EU or not.[37] CCPA would be applicable if the company A did business in California (please see considerations above).

If we have a company B located in California with direct application of CCPA, GDPR would be also applicable in two cases. The first case is when company B has an establishment in the EU that is processing personal data in the context of its activities. Second case is when company B does not have establishments in the EU but directs offering of goods or services or monitor behaviour of data subjects located in the EU.

Two subsequent notes have to be made towards the issue of applicability of both acts with regard to the personal applicability of GDPR. GDPR differentiates between controller and processor.[38] Without any further elaboration on the notions, controller is defined as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or*

[37] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 16 November, p. 9.

[38] Similarly CCPA differentiates between „businesses" and „service providers" in section 1798.140. **Business** *„means…A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies…"* **Service provider** means *„a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business."*

Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."[39] On the other hand, a processor means *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."* The basic difference is that a controller determines purposes (and means) of processing of personal data and a processor shall have authorization to process personal data on behalf of the controller (see more in Berthoty et al., 2018, p. 163 et seq.).

In case that a company with the establishment in the EU (GDPR is applicable) appointed a processor in California, the processor would be bound by several obligations laid down directly by GDPR.[40] The processor not subject to the GDPR will therefore become indirectly subject to some obligations imposed by controllers while CCPA would be applicable as well after fulfilling thresholds set out by law would be applicable as well.

The reverse situation is less clear from the legal point of view. In case that a company established in California (subject to CCPA) is not covered by Article 3 (2) GDPR and appoints processor located in the EU, it would require more in-depth analysis of relationship between the companies. There is a probability that a processor in the EU (not subject to establishment criterion based on Article 3 (1) GDPR) would still be covered by processor obligations laid down by GDPR. However, this is without prejudice to applicability of GDPR to a controller established in California.[41]

In case of applicability of both data protection regimes, various obligations are triggered. On the one hand, compliance with basic principles of processing personal data and subsequent obligations is required in terms of GDPR. On the other hand, CCPA entails individual rights of consumers that go beyond the rights enshrined in GDPR e.g. right to opt out from the sale of personal data. Both acts include severe sanctions for the violation of respective data protection laws (for further comparison see Kessler, 2019).

Second scenario: Application of GDPR

As stated above, GDPR distinguishes between intra-territorial application and extra-territorial application. A company is bound by the provisions of Article 3 when it is established in the territory of the EU or directs sale of goods and services or monitors behaviour of data subjects in the EU. A situation when only GDPR applies would be a company established in Warsaw processing personal data of customers in the EU without being domiciled or paying taxes in California (see respective thresholds above). Another example would be a company domiciled in Seattle providing application to customers in the EU and directing its sale there. The same conclusion towards business in California shall be applicable as in the previous case.

Third scenario: Application of CCPA

The third scenario is for a company that is not caught by the applicability of Article 3 GDPR and only CCPA applies. This is for example the company that is doing business in California for profit and other conditions laid down by CCPA are applicable e.g. a start-up AC ltd. selling autonomous vehicles only in the territory of California and only to residents of California based on special trial regime established by Californian government. AC ltd collects and processes personal data about its customers and users of autonomous vehicles. However, the company shall limit its activities with regard to the EU. It must not have establishment in the EU processing personal data or direct its

[39] GDPR, Article 4 (7)
[40] See Article 28 GDPR.
[41] Please see discussion in EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 16 November, pp. 11-13.

DOI: 10.46282/blr.2020.4.2.171

activities towards data subjects in the EU with regard to offering goods or services or monitoring of the behaviour. This would not be the case if a customer drives an autonomous vehicle in the territory of the EU.

5. CONCLUSION

Protection of information privacy is fairly different in the European Union and the United States of America especially in terms of legislative approach. EU adopts general legislation dealing with data protection issues for public and private sector respectively. USA prefers sectoral approach with a wide range of specific-aimed legislation on the federal level and state-level.

Comparing territorial scope of GDPR and CCPA it may be concluded that GDPR explicitly set forth for conditions of intra-territorial and extra-territorial activity. CCPA is not that clear in wording of the legislation although it is widely presumed that it may apply also on companies not established in California. The article analyses three possible scenarios of applicability of GDPR and CCPA. It shall be concluded that it is possible for both acts to be applicable for one company taking into account territorial scope of the legislation. If this is the case, several obligations arising from GDPR and CCPA respectively are triggered and "burden" the entity processing of personal data.

BIBLIOGRAPHY:

Andraško, J. (2017). Theoretical aspects of public administration electronic services. *Bratislava Law Review*, 1(2), 119-128, DOI: https://doi.org/10.46282/blr.2017.1.2.76.

Bennett, J. C. (1988). Different processes, One result: The Convergence of Data Protection Policy in Europe and the United States. In *Governance: International Journal of Policy and Administration,* 1(4), 415-441, DOI: https://doi.org/10.1111/j.1468-0491.1988.tb00073.x.

Berthoty, J. et al. (2018). *Všeobecné nariadenie o ochrane osobných údajov*. Praha: C.H. Beck.

Bignami, F. (2007). European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining. *Boston College Law Review,* 48 (3), 609-698. Available at http://lawdigitalcommons.bc.edu/bclr/vol48/iss3/ (accessed on 20.03.2020).

Goldman, E. (2018). *An Introduction to the California Consumer Privacy Act (CCPA)*. Available at https://www.ssrn.com/abstract=3211013 (accessed on 20.03.2020).

Kessler, J. (2019). Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource." *Southern California Law Review,* 93 (1), 99-128.

Kuner, Ch. (2013). *Transborder Data Flow Regulation and Data Privacy Law*. First edition. Oxford: University Press.

Levin, A. & Nicholson, M. (2005). Privacy law in the United States, the EU and Canada: The Allure of the Middle Ground. *University of Ottawa Law and Technology Journal*, 2(2), 357-395.

Solove, D. (2016). A Brief History of Information Privacy Law. In *PROSKAUER ON PRIVACY, PLI, 2016 GWU Law School Public Law Research Paper No. 215*.

Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271 (accessed on 20.03.2020).
Pernot-LePlay, E. (2020a). China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU? *Penn State Journal of Law & International Affairs*, 8(1), 49-117.
Pernot-LePlay (2020b). EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model? *Colorado Technology Law Journal*, 18(1), 101-124.
Prosser, W. (1960). Privacy. *California Law Review*, 48 (3), 383-423, DOI: https://doi.org/10.2307/3478805.
Umhoefer, C. (2019). CCPA vs. GDPR: the same, only different. *Intellectual Property and Technology News*. April 11, 2020. Available at: https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/ (accessed on 20.03.2020).
Zanfir, G. (2012). EU and US Data Protection Reforms. A Comparative View. *European Integration Realities and Perspectives*, the 7th Edition of the International Conference, 217-223. Available at: http://www.proceedings.univ-danubius.ro/index.php/eirp/article/viewFile/1305/1182 (accessed on 20.03.2020).
Warren, S. & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review,* 4(5), 193-220.
Annex to the Recommendation of the Council of 23rd September 1980: Guidelines governing the protection of privacy and transborder flows of personal data.
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).
REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the second annual review of the functioning of the EU-U.S. Privacy Shield, available at: https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf (accessed on 20.03.2020).
CJEU decision in *Weltimmo v NAIH* (C-230/14).
CJEU decision *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12).
EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 16 November.
Article 29 Data Protection Working Party Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain.