Data Protection in the USA

Eduardo Isaac Soto Barrera, Lawyer (Mexico), Mag. iur. (Mx), Mag. iur. (D), Hanover
Antonia Herfurth, Lawyer (Germany), Hanover and Munich

August 2021

The USA is home of the most valuable and powerful tech companies in the world. The reason why these companies are so successful is because they collect tremendous amounts of personal data of their users. The EU's General Data Protection Regulation (*GDPR*) is popular; it regulates the processing of personal data. The US data protection regulations, on the other hand, are not popular. Therefore, this Compact provides an overview of the US data protection landscape.

Legislation at federal level

In the USA, no comprehensive federal data protection act exists, unlike the GDPR in the EU. Hence, no regulatory authority dedicated to overseeing data protection law exists either. The Federal Trade Commission (*FTC*) is primary responsible for enforcing privacy and data security requirements, but primarily a competition authority with the additional competence of consumer protection. However, data protection rules exist for single sectors such as economy and trade, health and finance.

Legislation based on national security

The USA Freedom Act of 2015 states that US authorities are not allowed to store telecommunication data, only telecommunication providers are allowed to do so. But US authorities are granted access to data if they present a potential risk coming from the person concerned. The Foreign Intelligence Surveillance Act of 1978 (*FISA*) builds the legal basis for data collection abroad through US intelligence services. FISA lays down requirements under which personal data can be processed to counter terrorism.

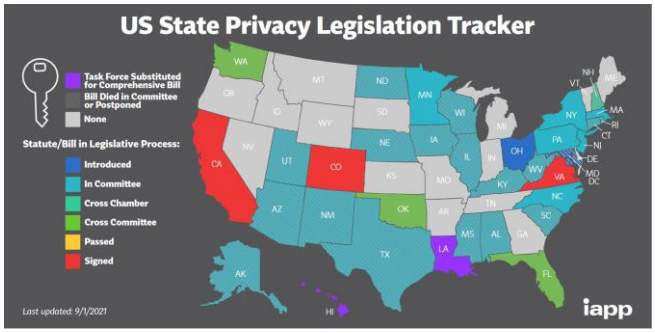
Legislation based on data protection

The Fair Credit Reporting Act of 1970 (*FCRA*) regulates the handling of collected information from consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services. The Privacy Act of 1974 protects personal information which is maintained in systems of records by federal agencies. The act lays down rules for agencies for the processing of data and guarantees rights to individuals such as access to their data and correction in case of inaccuracies. The Electronic Communications Privacy Act of 1986 (*ECPA*) was initially enacted to extend the competence of the US

government to wiretap telephone calls. Due to several amendments, the government's competences were partly shortened, now it also contains rules to protect private electronic communication from unauthorized government access. The Computer Fraud and Abuse Act of 1986 establishes rules on cybersecurity, such as protection from accessing a computer without or in excess of authorisation. The processing of personal health information is regulated by the Health Insurance Portability and Accountability Act of 1996 (*HIPAA*). Privacy and security requirements for financial institutions are set out by the Gramm-Leach-Bliley Act of 1999. The Children's Online Privacy Protection Act of 2000 protects children's privacy by focusing on how operators of commercial websites and online services target children.

Legislation at state level

Since no federal act on data protection exists, states have established data protection acts – sectoral and comprehensive ones. However, regarding comprehensive acts, states are at different points in their development. While Maine and Nevada, for example, have no data protection laws at all, they are in preparation in New York and North Carolina, and have even been signed in California, Colorado and Virginia.



Source:
https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Map.pdf

The role model, however, is California. It has based its data protection law, the California Consumer Privacy Act (*CCPA*), on the GDPR. When coming into effect in January 2020, the CCPA introduced new user rights. The privacy activist group *Californians for Consumer Privacy* still considered the CCPA not strict enough, therefore, initiated a stricter law. The new California Consumer Privacy Rights Act (*CPRA*) will come into effect on 1 January 2023 and will even be stricter than the GDPR.

This Compact looks closer at the CCPA and the CPRA, not only because they are the forefront of US data protection laws, but because California is the hub of the world's most powerful tech companies which collect significant amounts of data. If companies want to make business in the US, they very like cannot ignore the Californian data protection law, therefore, tend to take this as a standard.

The US role model – California Consumer Privacy Act

The CCPA is applicable where a company or organisation makes business in California; a "business" requires a profit-oriented activity. The CCPA is even applicable where a business is not physically present in California but collects personal information of consumers located in the state. The business must not only make business in California but either obtain annual gross revenues in excess of $ 25,000,000 in the preceding calendar year *or* alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices *or* derives 50% or more of its annual revenues from selling consumers' personal information.

If a business falls under the CCPA, the act provides several rights to consumers, such as the right of information which personal information a business has collected and eventually transferred to a third party and the right to access (data portability). Furthermore, the individual has the right to prohibit the selling of personal data to a third party through an opt-out mechanism and the right to delete personal information.

Businesses falling under the CCPA underlie certain requirements, for example they must keep personal information safe (data security), must offer two ways

on their website to contact them and must answer consumer requests within 45 days. They also must inform consumers about their online privacy policies and must place an opt-out tool on their website which is easy to detect for consumers ("Do not sell my info" button). The CCPA also establishes special protection for minors.

Important is, that the act only protects consumers in California.

One step further – California Consumer Privacy Rights Act

The CPRA partly changes the scope of applicability. A business falls under the act when it alone or in combination, annually buys, sells, or shares the personal information of *100,000 or more* consumers or households. Compared to the CCPA, personal information of 100,000 consumers must be affected, not only 50,000 anymore. But the act broadens the scope of applicability where it states that a business also falls under the CPRA where it derives 50% or more of its annual revenues from selling *or sharing* consumers' personal information. Here, the Californian legislator added the act of "sharing".

The CPRA establishes an agency to implement and enforce the law, the California Privacy Protection Agency (*CPPA*) – the first of its kind in the USA.

Already existing rights will be modified and new rights introduced, such as the right to correct inaccurate personal information or the right to restrict the use of sensitive personal information. Additionally, the CPRA codifies the principles of purpose limitation, storage limitation and data minimization which are already known from the GDPR.

GDPR vs CCPA vs CPRA

The following table compares the provisions of the GDPR, the CCPA and the CPRA:

Source: https://www.linkedin.com/posts/dltsays_ccpa-gdpr-cpra-activity-6606221910663663616-e8vv

Data transfer between the EU and the USA

Currently, the GDPR is one of the strictest data protection law in the world, making it difficult to process personal data from the EU to a third country.

Safe Harbour and Privacy Shield

For the last 20 years, the transfer of personal data between the EU and the USA was unproblematic due to the *Safe Harbour Principles* and the *Privacy Shield*. Both frameworks enabled a safe and therefore free transfer of data. However, with its *Schrems I decision* in 2015, the European Court of Justice declared the Safe Harbour Principles invalid. Its follow-up regulation, the Privacy Shield, was declared invalid by the Court in 2020, *Schrems II decision*. Since then, the EU considers the USA an unsafe third country again.

Current solutions

From an EU point of view, the transfer of personal data to the USA can only be based on other mechanisms established by the EU: binding corporate rules (*BCRs*) and standard contractual clauses (*SCCs*).

BCRs are a framework for the processing of personal data within a company. Based on their BCRs, international companies can transfer personal data globally, even if the receiving part of the company is located in an unsafe third country.

SCCs are standard clauses which allow the – internal and external – transfer of personal data to unsafe third countries. They can be downloaded from the European Commission's website and freely used. However, they may not be changed or amended, instead must be used as published by the Commission. As parts of the existing SCCs were 30 years old, the Commission issued a modernised set on 4 June 2021.

Outlook

US data protection law is a patchwork. Instead of a comprehensive federal data protection act, numerous sectoral acts on federal and state level exist. Neither a dedicated data protection authority exists nor a uniform definition of "personal information". There is criticism that some of the existing acts are so old that they no longer do justice to the current digital situation and do not actually protect personal information but offer the US authorities numerous loopholes to obtain information after all.

For this reason, a federal data protection act has already been discussed for many years in the USA. Especially big international companies support the harmonisation. With California pushing forward its data protection, it is expected that the federal legislator will follow. Just as the EU and the USA are working on a new framework to safely transfer personal data between them.

ALLIURIS

The ALLIURIS GROUP consists of 20 law firms and 400 business lawyers within Europe, Asia and America. (www.alliuris.law).

……..

Your contact:
Alisha Daley-Stehr,
Alliuris Communication

info@alliuris.org
Fon 0049-511-307 56-0
Fax 0049-511-307 56-10

……..

IMPRINT

EDITORS

ALLIURIS A.S.B.L.
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS
BRUSSELS

MANAGEMENT
Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-50 505056-20 Fax +49-511-307 56-60

BRUSSELS · PARIS · LONDON · AMSTERDAM · AMERSFOORT . LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · MOSCOW · MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI ·GUANGZHOU NEW DELHI · NEW YORK · MEXICO CITY · SAO PAULO · RIO DE JANEIRO · BRASILIA BUENOS AIRES

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt