Privacy Law Comparison

GDPR, California CCPA and CPRA, Canada PEPIDA

Version 1.1

September 23, 2020

info@assuredSPC.com

Assured SPC

While the California Consumer Privacy Act is the most stringent privacy law in the US at this time, it may undergo changes after the November 3, 2020 CA ballot initiative that is called the California Privacy Rights Act (CPRA). Many US businesses may also be covered by GDPR for EU/EAA residents and the Canadian PIPEDA privacy law if personal information of Canadians is moved across the border. Here is a comparison of these laws that may be useful to those that need to manage risk of privacy compliance or are involved in the operationalization of multiple laws.

	EXISTING LAW			*PROPOSED*
	European Union GDPR	**California CCPA**	**Canada PIDEDA**	**California CPRA**
JUDICIAL SCOPE				
Who can exercise rights?	Natural persons (data subjects)	California Residents	Canadian Residents	California Residents
Who has obligations?	All govt and non-govt legal entities and individuals established in the EU or offering goods or services to EU residents	For-profit businesses that do business in the State of California and meet thresholds AND any entity that controls or is controlled by a covered business and that shares common branding with the business.	Private-sector organizations in Canada that manage personal information for commercial activity. Provincial privacy laws can be preemptive but businesses that operate in Canada and move PI across provincial or national borders (e.g. to the US) are subject to PIPEDA.	Same as CCPA
Thresholds	None. However, there is a limited small-business exemption for certain obligations	$25 million annual revenue or 50,000+ records or 50% of annual revenue derived from selling consumers personal data	None	$25 million annual revenue or 100,000+ records or 50% of annual revenue derived from selling or sharing consumers' personal data

	EXISTING LAW			*PROPOSED*
	European Union GDPR	**California CCPA**	**Canada PIDEDA**	**California CPRA**
How is Personal Data or Personal Information defined?	Personal data means any information relating to a natural person ('data subject') that can be used directly or indirectly to identify that person, e.g. "by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Personal information is information that identifies, relates to, or could reasonably be linked with you or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.	Personal information includes any factual or subjective information about an identifiable individual e.g., age, name, ID numbers, income, ethnic origin, opinions or disciplinary actions; PI includes employee files, credit records, loan records, medical records.	Same as CCPA
Exclusions to coverage of Personal Data or Personal Information	None defined	Any Personal information that is in the scope of federal and state healthcare laws by organizations covered by those laws (Confidentiality of Medical Information Act, HIPAA), credit reporting (FRCA), financial control (GLBA). Any B2B and employee personal information until Jan 1, 2022	Business contact information for communication. PI used for personal reasons, an organization's collection, use, etc. for journalistic, artistic or literary purposes. Non-profits, political parties, educational institutions and hospitals collection of personal information for non-commercial activities.	CPRA extends the CCPA exclusions of PI with an exception for public information would also include certain information that is made available to the general public by the consumer or from widely distributed media e.g., social media.

	EXISTING LAW			*PROPOSED*
	European Union GDPR	**California CCPA**	**Canada PIDEDA**	**California CPRA**
DEFINITION & STRUCTURE				
Broad definition of covered data	**Y**	**Y**	**Y**	**Y**
"Controllers" and "Processors"	**Y**	**Y**	**Y**	**Y**
Excludes "de-identified" data	**Y**[2]	**Y** (businesses & service providers)	**N**[3]	**Y** (businesses & service providers)
Excludes "publically available information"	**N**	**Y**	**Y**	**Y**
PSEUDONYMOUS DATA				
Recognizes pseudonymous data	Y[4]	Indirectly[5]	**N**	Indirectly[5]
INDIVIDUAL RIGHTS				
Right to access	**Y**	**Y**	**Y**	**Y**
Right to correct	**Y**	**N**	**Y**	**Y**
Right to delete	**Y**	**Y**	**Y**[6]	**Y**
Right to portability	**Y**	**Y**	**N**	**Y**
Internal appeals process	**Y**[6]	**N**		**N**
Opt of of "Sale"	**Y**	**Y**	**N**	**Y**
Opt out for "Targeted Advertising"	**Y**[7]	**Y**[8]	**N**	**Y**
Opt out of "Profiling"	**Y**	**N**	**N**	**N**
Opt out of Automated Decision Making	**Y**	**N**	**N**	**Y**
Consent for Sensitive Data	**Opt-in**	**N/A**	**Y**	**Opt-out**

	EXISTING LAW			*PROPOSED*
	European Union GDPR	**California CCPA**	**Canada PIDEDA**	**California CPRA**
OBLIGATIONS ON COMPANIES				
Lawful bases for collection	**Y**	**N**	**N**	**N**
Privacy Policies	**Y**	**Y**	**Y**	**Y**
Risk Assessments for High-Risk Activities	**Y**[9]	**N**	**N**	**N**
Data Minimization	**Y**	**N**	**Y**	**Y**
Purpose Limitation	**Y**	**N**	**Y**	**Y**
Duty to Avoid Secondary Use	**Y**	**N**	**Y**	**Y**
Security Requirements	**Y**	**Y**	**Y**	**Y**
Non-Discrimination	**Y**[10]	**Y**	**N**	**Y**
FACIAL RECOGNITION PROVISIONS				
Protections for Commercial Use of Facial Recognition	**Y**	**N**	**N**	Indirectly
ENFORCEMENT				
Enforcement by State AG or Govt. Body (DPA)	**Y**	**Y**	**Y**	**Y**[11]
Enforcement by Individuals	**Y**[12]	**Y**[13]	**N**	**Y**[13]

Notes:

1. This comparison is a modified and updated version of a comparison of originally produced by the Future of Privacy Forum, February 12, 2020. That document is titled "A New U.S. Model for Privacy? Comparing the Washington Privacy Act to GDPR, CCPA, and More". Click here for the URL

2. GDPR defines personal data very broadly. Its provisions do not apply to data which does not relate to an "identified or identifiable person" or to personal data "rendered anonymous in such a manner that the data subject is no longer identifiable."

3. It is unclear whether de-identified data is out of scope for PEPIDA at this time. See the article here.

4. GDPR - More precisely, GDPR recognizes "pseudonymization" as a method to decrease privacy risks and comply with certain obligations.

5. CCPA and CPRA - Indirectly, individual rights to access and delete pseudonymous data in California may be limited in practice due to challenges with verifying consumer requests. CPRA extends the definition of a breach to any definition contained in any other California law.

6. PEPIDA implies that Individuals may request deletion after the normal retention period of the company or after the purpose of collection has been fulfilled. PEPIDA says that businesses may delete data as an option for a request for correction.

7. GDPR - An individual can object to any processing of their personal data conducted pursuant to certain lawful bases, at which point the controller may no longer process the data unless it demonstrates "compelling legitimate grounds" to override that person's interests, rights, and freedoms. If such processing is conducted with consent, the consent must be easy to withdraw at any time (Article 7.3). Finally, the GDPR includes an absolute right to object to "direct marketing."

8. CCPA does not restrict targeted advertising if it can be conducted without "selling" data. Many believe that the term selling includes cookies used for targeted advertising. In contrast, the CPRA ballot Initiative contains a broader opt-out provision (of both "sale" and "sharing") and specifically limits service providers from engaging in any "cross-context behavioral advertising."

9. GDPR - Companies engaged in high-volume or high-risk processing must appoint a Data Protection Officer (DPO) who handles requests, communications, and appeals.

10. GDPR does not include an explicit provision stating that a data subject must not be discriminated against on the basis of their choices to exercise rights. However, it is implicit from other principles of the GDPR that individuals must be protected from discrimination on these grounds.

11. The CPRA creates a new agency for enforcement of consumer rights called the California Privacy Protection Agency.

12. GDPR - mix of EU judicial rights & individual redress from regulators.

13. CCPA & CPRA - a personal right of action exists for security breaches.

About Assured SPC

Assured SPC helps organizations minimize compliance risk by providing services for the lifecycle of information security and privacy programs. We assist organizations assess, design and operationalize requirements for privacy compliance including HIPAA, the California Consumer Privacy Act, GDPR, PEPIDA and the NY SHIELD Act. And we help organizations assess risk and define a security architecture that provides "reasonable security procedures and practices and safeguards" that are associated with customer and regulatory compliance.

In addition to credentials and years of experience driving information security and privacy programs, Assured SPC's senior staff have uniquely deep experience as IT Leaders. We regularly help organizations prepare for AICPA SOC2 audits and HITRUST CSF assessments. We also offer virtual c-level leadership for SMB businesses, including Chief Information Security Officers (vCISO), Chief Information Officer (vCIO) and Privacy Officer services.