Comparison of Existing and Proposed U.S. Privacy Laws and GDPR

Assured SPC has amended a comparison of key features of GDPR, California's CCPA and proposed privacy legistation for this November's ballot: California's CPRA and Washington's WPA 2020[12]. The chart compares the following key features: (1) jurisdictional scope; (2) definitions and structure; (3) pseudonymous data; (4) individual rights; 5) obligations on companies; (6) facial recognition provisions; and (7) enforcement. We hope that you find this information useful.

	EXISTING LAW		*PROPOSED*	
	European Union GDPR	**California CCPA**	**California CPRA**	**Washington WPA 2020**
JUDICIAL SCOPE				
Who can exercise rights?	Natural persons (data subjects)	California Residents	California Residents	Natural persons who are Washington 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.	Same as CCPA	Non-gov't legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington.
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	$25 million annual revenue or 100,000+ records or 50% of annual revenue derived from selling or sharing consumers' personal data	100,000+ records during a calendar year; or derives 50%+ annual revenue from the sale of personal data and processes or controls personal data of 25,000+ consumers
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.	Same as CCPA	WPA defines personal data as "any information relating to an identified or identifiable natural person," including an identifier such as an identification number or online identifier
Exclusions to coverage of Personal Data or Personal Information		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	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.	De-identified data and any B2B and employee personal data when individuals act in those roles.

DEFINITION & STRUCTURE				
Broad definition of covered data	Y	Y	Y	Y
"Controllers" and "Processors"	Y	Y	Y	Y
Excludes "de-identified" data	Y[1]	Y (businesses & service providers)	Y (businesses & service providers)	Y
Excludes "publically available information"	N	Y	Y	Y

	EXISTING LAW		*PROPOSED*	
	EU/EAA GDPR	**California CCPA**	**California CPRA**	**Washington WPA 2020**
PSEUDONYMOUS DATA				
Recognizes pseudonymous data	Y[2]	Indirectly[3]	Indirectly[3]	Y
INDIVIDUAL RIGHTS				
Right to access	Y	Y	Y	Y
Right to correct	Y	N	Y	Y
Right to delete	Y	Y	Y	Y
Right to portability	Y	Y	Y	Y
Internal appeals process	Y[4]	N	N	Y
Opt of of "Sale"	Y	Y	Y	Y
Opt out for "Targeted Advertising"	Y[5]	N[6]	Y	Y
Opt out of "Profiling"	Y	N	N	Y
Opt out of Automated Decision Making	Y	N	Y	Y
Consent for Sensitive Data	Opt-in	N/A	Opt-out	Opt-in
OBLIGATIONS ON COMPANIES				
Lawful bases for collection	Y	N	N	N
Privacy Policies	Y	Y	Y	Y
Risk Assessments for High-Risk Activities	Y	N	N	Y
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-Descrimination	Y[7]	Y	Y	Y
FACIAL RECOGNITION PROVISIONS				

Protections for Commercial Use of Facial Recognition	Y	N	Indirectly	Y
ENFORCEMENT				
Enforcement by State AG or Govt. Body (DPA)	Y	Y	Y[8]	Y
Enforcement by Individuals	Y[9]	Y[10]	Y[10]	N[11]

1. 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."

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

3. 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.

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

5. 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."

6. CCPA does not restrict targeted advertising if it can be conducted without "selling" data. In contrast, the 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."

7. 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.

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

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

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

11. WPA 2020 has been amended to clarify that it does not override the existing rights of Washington residents to bring actions under Washington State's Consumer Protection Act for conduct or behavior that would amount to an unfair or deceptive practice . Similarly, residents of California (and many other states) have the ability to bring lawsuits to challenge privacy violations when they violate unfair and deceptive practices (UDAP) state laws.

12. A New U.S. Model for Privacy? Comparing the Washington Privacy Act to GDPR, CCPA, and More, Future of Privacy Forum, February 12, 2020 - https://fpf.org/2020/02/12/a-new-model-for-privacy-in-a-new-era evaluating-the-washington-privacy-act/