CENTER FOR DEMOCRACY & TECHNOLOGY

Privacy Framework Comparisons (Dec. 2018)

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
DEFINITIONS & SCOPE:			
Personal Information -- A federal privacy law must have a broad definition of PI in order to match changes in technology and be consistent with modern privacy laws like California and the EU.	The CCPA broadly defines "**personal information**" to mean information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Noteworthy provisions: ● Personal information covers **household** level data. ● **"Relates to"** is potentially all-encompassing. ● Inferred data can become PI when attached. ● Technical identifiers are recognized as potentially PI.	The GDPR broadly defines "**personal data**" to mean any information relating to an identified or identifiable data subject based on direct or indirect identification.	CDT builds on the existing FTC definition and the Wyden discussion draft to define "**personal information**" as any information that is "linked or reasonably linkable *by the covered entity*" to an individual or consumer device. Noteworthy provisions: ● Data "reasonably linkable" to a consumer device is covered, capturing technical identifiers. ● Inferred data can be PI.
Exceptions to Personal Information -- De-identification exceptions should be carefully tailored. Employer-employee relationships are beyond the scope of this bill.	CCPA excludes **aggregate** and "**deidentified**" data. These terms remain subject to interpretation by the California AG.	GDPR does not cover **anonymous data**, which has been strictly cabined per WP29 guidance. **Pseudonymous data** is covered but receives less protection.	CDT definition excludes: ● **Employee Information** ● Individual rights do not require covered entities (CEs) to take actions to convert information into personal information.

CENTER FOR DEMOCRACY & TECHNOLOGY

Privacy Framework Comparisons (Dec. 2018)

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
Covered Entities -- A federal privacy law should presumptively cover all entities, regardless of sector or size.	CCPA applies to businesses with: ● $25 million in gross revenues ● Personal information of 50,000 consumers ● 50% of revenue from data sales	GDPR is broadly applicable to: ● Businesses ● Nonprofits ● Government Entities	CDT is broadly applicable to: ● Unregulated online and offline businesses ● ISPs and FCC "common carriers" ● Nonprofits
Controller/Processor --	CCPA applies to "businesses" which are akin to data controllers. Service providers have no specific obligation but to act at the direction of a business.	GDPR establishes obligations on data controllers and data processors. Obligations of processors include: ● Record keeping requirements ● Implement appropriate security measures ● DPIAs and DPOs ● Breach notification responsibilities	CDT places primary obligations on "covered entities," service providers, and "third parties." "Service providers" are to be contractually bound by covered entities, with a basic prohibition that service provider cannot "sell or license" any personal information. Third parties are required to meet the privacy promises of original covered entities. Reasonable oversight by CEs is required.
INDIVIDUAL RIGHTS:			
	CCPA includes the following affirmative data rights: ● Right to Know ● Right of Access ● Right to Portability ● Right to Delete ● Right to Opt-Out of Sale ● Non-Discrimination Based on Exercise of Rights	GDPR includes the following affirmative data rights: ● Right to Know ● Right of Access ● Right to Portability ● Right to Correct ● Right to Erasure ● Right to Restrict Processing ● Right to Object	CDT includes the following affirmative rights, subject to limitations: ● Right to Know ● Right of Access ● Right to Portability ● Right to Correct [Limited] ● Right to Delete

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
		• Rights with respect to automated decisionmaking and profiling	
Right to Know -- See "DISCLOSURES" below for additional information.	In addition to existing California law governing online privacy policies, CCPA requires companies to provide information at the point of collection about: • Categories of PI • Purposes for which those categories shall be used. Upon request, individuals may receive information about: • Categories of PI • (Categories of) Sources of PI • Business/Commercial Purposes for Collecting/Selling PI • Categories of Third Parties • "**Specific pieces of personal information**" collected.	GDPR requires comprehensive disclosures at the point of collection that include, among other things, the purposes for processing, retention periods, and who data is shared with. See below.	CDT requires machine-readable notices that disclose: • Types of PI and names of third parties • General purposes of use • Description of the rights provided by this framework • Description of any controls offered See below.
Right to Access -- Access rights are at the core of the CCPA and GDPR. A federal privacy law must include a broad right to access information from covered entities.	CCPA envisions a 2019 AG rulemaking to determine "**verified requests**" for 12 months of personal information, including categories and "**specific pieces**" of information.	GDPR gives individuals a right to obtain: • Confirmation of data processing • Copies of personal data • Other supplementary information, e.g., privacy notice disclosures	CDT gives individuals the right to obtain personal information and the **names of third parties** with whom personal information is shared, licensed, or sold. **Exceptions:** • Individual cannot confirm identity

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
	Exceptions: ● Limits for "manifestly unfounded or excessive" requests	**Exceptions:** ● Information covering trade secrets or intellectual property ● Controller balances whether access adversely affects the rights of other individuals ● Controllers who hold lots of data may require specification from individuals	● Access is limited by law ● CE makes an individualized determination that access creates a risk to another individual
Right to Portability	CCPA includes a "shadow" portability right wherever access is provided electronically for 12 months of personal information.	GDPR provides for data portability where personal data is provided based on individual consent of contract and is processed automatically.	CDT provides for a general data portability right, or the ability to "download" personal information, and directs NIST to convene a process to scope and identify reasonable limits on portability.
Right to Correct	N/A	GDPR gives individuals the right to obtain rectification, including by means of a supplementary statement.	CDT permits individuals to correct information where it could be used for an eligibility determination, educational opportunities, or is health information.
Right to Delete	CCPA gives individuals a right to request deletion of data subject to many overbroad exceptions, such as "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business," and other uses "compatible with the context in which the consumer	GDPR gives individuals a right to erasure when: ● Data is no longer necessary ● The individual withdraws consent ● The company has no overriding legitimate interest ● Where processing is unlawful	CDT gives individuals a reasonable right to delete, which CEs may not make unreasonably difficult to do. **Exceptions:** ● Individual cannot confirm identity ● Deletion is limited by law ● CE makes an individualized determination that access

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
	provided the information.	The "Right to Be Forgotten" is a special requirement for platforms that make personal information widely available online.	creates a risk to another individual ● Retention is needed to complete a transaction, for security or repair errors ● Peer-reviewed ongoing research subject to existing ethical safeguards
Right to Restrict	N/A	GDPR gives individuals the right to restrict how PI is used in some circumstances such as the PI is inaccurate, no longer needed, or has been unlawfully processed.	N/A
Right to Object	CCPA provides a qualified opt-out right for the "selling" of personal information.	GDPR gives individuals a right to object to the processing of PI in certain circumstances, *and* an absolute right to object to direct marketing.	N/A
Automated Decisionmaking & Profiling Rights	N/A	GDPR gives individuals rights around automated decisions, including profiling, that have "legal or similarly significant effect." Specifically, data controllers must provide certain transparency about these practices and often obtain consent.	N/A
Fees & Denials	CCPA requires: ● Requests to be handled free of charge ● "Reasonable fees" permitted for "manifestly unfounded or excessive	GDPR requires: ● Requests to be handled free of charge ● "Reasonable fees" permitted for "manifestly unfounded or excessive requests"	CDT requires: ● Requests to be handled free of charge ● "Reasonable fees" permitted for "unfounded or excessive requests"

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
	requests" ● Individuals informed of any denials	● Individuals informed of any denials	● Individuals informed of any denials
RESPONSIBILITIES OF COVERED ENTITY:			
Redress	CCPA establishes time frames for responding to consumer requests, explaining any rights consumers may have to appeal business decisions. CCPA also provides for a limited private right of action for some data breaches under existing California law.	GDPR includes detailed provisions on complaints and private rights of action: ● Individual right to compensation ● Timeframes for responding to complaints ● Ability for individual to bring complaint to home DPA	CDT directs CEs should: ● Provide an accessible means to make a complaint or inquiry ● Respond within a reasonable period of time -- no longer than 30 days ● Provide information about how to contact regulators
Data Security	N/A. CCPA does not address data security save for providing a limited private right of action under existing California law (for violations of duty to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information").	GDPR includes a **72-hour data breach incident notification** requirement and calls for "**appropriate technical and organisational measures**" to address data security.	CDT does not include a breach notification requirement, but envisions comprehensive **data security rulemaking by the FTC**.
Data Sharing Limitations	CCPA provides an opt-out right for the "selling" of personal information. **Limits on Third Parties:**	Limiting data collection and sharing is at the core of several provisions of the GDPR. Personal data may not be made accessible without the individual's intervention to an	CDT requires third parties be contractually held to the same privacy/security expectations as a covered entity and requires certain covered entities to take action against

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
	CCPA differentiates between service providers and third parties; there are no restrictions on third parties save they must respect the consumer's ability to opt-out of having information sold.	indefinite number.	third parties if they obtain actual knowledge of privacy/security violations. Reasonable oversight of contracts is required.
DISCLOSURES: CDT envisions disclosures and transparency efforts both as a responsibility of CEs to the public and an affirmative individual right ala CCPA and GDPR.			
Privacy Policies	In addition to existing California law governing online privacy policies, CCPA requires companies to provide information at the point of collection about: ● Categories of PI ● Purposes for which those categories shall be used	GDPR requires comprehensive privacy notices that include purposes for processing, retention periods, and who data is shared with.	CDT requires machine-readable notices that disclose: ● Types of PI and names of affiliate of third parties information sold/licensed to ● Description of individual rights ● Notice of material changes ● Privacy controls, including de-identification ● Effective date
Additional Disclosures	CCPA requires business disclose their California privacy rights and have "Do Not Sell My Personal Information" page.	N/A	For larger CEs, CDT requires **certified periodic disclosures** that detail: ● Specific purposes for collecting PI ● Comprehensive privacy risk

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
			impact assessment ● Material changes over the past year ● Material privacy and security incidents and the covered entity's response
Data Brokers	N/A	N/A	CDT requires data brokers to register with the FTC and provide information into their sources of personal information and how individuals may exercise their individual rights with respect to data brokers.
ACCOUNTABILITY PRACTICES:			
Data Protection Officers	N/A	GDPR requires entities to appoint an independent "data protection officer" if engaged in large scale monitoring or processing of certain sensitive types of data.	N/A
Risk Assessments	N/A	GDPR requires entities to undertake risk assessments for high-risk processing activities and to keep records of these assessments, as well as their legal basis for any processing.	N/A
DECEPTIVE DATA PROCESSING PRACTICES:	N/A	N/A	CDT codifies existing FTC enforcement precedent with respect to deceptive statements and omissions regarding privacy practices.

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
UNFAIR DATA PROCESSING PRACTICES:			
General Approach	CCPA gives consumers a **broad right to opt-out from the "sale"** of personal information.	GDPR requires all data processing to have a legal basis. Companies must generally **obtain consent for processing of special data categories**: ● Race and ethnic origin ● Religious or philosophical beliefs ● Political opinions ● Trade union memberships. ● Biometric data used to identify an individual ● Genetic data ● Health data ● Data related to sexual preferences, sex life, and/or sexual orientation	CDT makes unlawful **secondary** uses of certain data by making them presumptively "unfair" absent an exception designated by the FTC, including: ● Biometric identification and verification ● Precise geospatial tracking ● Probabilistic tracking ● Tracking of children ● Disclosure of content and parties to communications ● Audio and visual recording ● Secondary use of health information
Global Exceptions	The CCPA places no limitations on data use for "business purposes," which are broadly defined to include internal research and efforts to enhance products or services.	GDPR permits processing exceptions for: ● Consent ● Necessary for carrying out obligations of employment, social security, or social protection law ● "Vital interests" ● Data manifestly made public, legal defense	CDT provides exceptions for: ● Security and fraud ● Imminent danger ● Repairing errors in intended functionality ● Research ● Legal compliance CDT gives the FTC rulemaking authority to create **additional or individual exceptions**.

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
		• Substantial public interest • Healthcare exceptions and public health	Consent is not an exception from the general prohibition.
Security & Fraud	CCPA permits businesses to retain information to "[d]etect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity."	GDPR recognizes processing "strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest."	CDT permits processing "for detecting and preventing security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity; or prosecuting those responsible for that activity."
Imminent Danger	N/A	GDPR permits processing in the "vital interests" of the data subject is always permitted.	CDT permits processing permitted preventing imminent danger to the personal safety of an individual or group of individuals.
Research	• Internal research or development is a "business purpose" • Certain rights (e.g., deletion) not required for "research" that is "public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws"	• Research with "special categories" of data generally requires consent • Research can be a compatible use if controller has a legal basis for processing • Different understandings of archiving/historical/public interest research • Safeguards required	Public or peer reviewed scientific, medical, historical, or statistical research in the public interest that adheres to all other applicable ethical standards or laws, with informed consent permitted.
Legal Compliance	Yes	Yes	Yes

	California Consumer Privacy Act	General Data Protection Regulation	CDT Discussion Draft
UNFAIR TARGETED ADVERTISING:			
	CCPA gives consumers a **broad right to opt-out from the "sale"** of personal information. Consumers may obtain inferential information that is part of a consumer profile, if it constitutes personal information.	GDPR provides: ● Absolute right to object to direct marketing (opt-out) ● Right to transparency and consent to "profiling" and "automated decisionmaking" that has legal effect or similar impact	CDT directs the FTC to engage in **rulemaking** to address advertising that is likely to result in unlawful discrimination.
ENFORCEMENT:			
Primary Enforcement	CCPA is primarily enforced by the California Attorney General.	GDPR is enforced by member state data protection authorities and includes rights for data subjects to sue companies.	CDT grants joint enforcement to the FTC and state Attorneys General, with the FTC having the ability to take preemptive action.
Penalties	● Civil penalties of $2,500 per violation ● $7,500 per each intentional violation ● Injunctions are also available	Penalties of up to €20 million or 4% of the worldwide annual revenue	CDT gives civil penalty authority to the FTC in the amount of $16,500 per covered person.