FINANCE, OPERATIONS & TECHNOLOGY SUMMIT 2019

OCTOBER 6-9, 2019
COLORADO SPRINGS, CO
Eric Rankin
VP of Product Development
Simpleview
Disclaimer

This presentation, discussion, and its content are not exhaustive resources on Data Privacy and they should not be relied on as legal advice. Because legal information is not the same as legal advice – the application of law to one’s specific circumstances, we recommend consulting a lawyer if you need legal advice on how to interpret the legislation. This content is information for awareness purposes and to inspire you to review your current policies and practices.
GDPR
What is GDPR?

The Fundamental Principles of GDPR

1. Lawfulness, fairness, transparency
2. Purpose Limitations
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and confidentiality
CCPA vs. GDPR
<table>
<thead>
<tr>
<th>Subject</th>
<th>Personal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCPA</td>
<td>Any data that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with particular consumer. A “consumer” is a California resident</td>
</tr>
<tr>
<td>GDPR</td>
<td>An identifiable natural person is one who can be identified, directly or indirectly, in particular 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.</td>
</tr>
<tr>
<td>Expectation</td>
<td>Household is in debate</td>
</tr>
</tbody>
</table>
## Comparison

<table>
<thead>
<tr>
<th>Subject</th>
<th>Transfer of Personal Data to third countries or international organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CCPA</strong></td>
<td>Cross-border data transfers are not restricted. All transfers to “service providers” require a written agreement containing certain provisions (that is, there is the CCPA equivalent to Article 28 of the GDPR)</td>
</tr>
<tr>
<td><strong>GDPR</strong></td>
<td>Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if the conditions laid down in Article 44 – 50 are complied with by the controller and processor to ensure that the level of protection of natural persons guaranteed by the GDPR. Transfers on the basis of an adequacy decision and methods such as BCR, Contract Clauses, etc. or in the case of EU-US transfer, the Privacy Shield.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>Data Portability</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>CCPA</strong></td>
<td>There is a limited recognition of this right under the CCPA. Specifically, Cal. Civ. Code Sec. 1798.100 provides that data subjects that exercise their right to access, must receive the data &quot;by mail or electronically and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transit this information to another entity without hindrance&quot; There is a related and somewhat contradictory provision on this under Cal. Civ. Code Sec. 1798.130(a)(2).</td>
</tr>
<tr>
<td><strong>GDPR</strong></td>
<td>Article 20: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.</td>
</tr>
</tbody>
</table>
The GDPR applies to “data controllers” which has a very broad definition. The CCPA applies only to businesses of a very specific size or type.

- Unlike the CCPA, the GDPR covers areas such as:
  - Regulating data processors (service providers)
  - Principles of data processing

The Differences

- Legal bases for processing
- Specific data security measures
- Appointing a data protection officer
- Empowering data protection authorities
- Certification schemes and codes of conduct
- Overseas transfers
The Differences

Unlike the GDPR, the CCPA requires businesses to:

• Publish up-to-date information specifically about their personal information trading practices

• Specifically allow individuals to opt out of the sale of their personal information

• The GDPR requires data controllers to publish a comprehensive Privacy Policy. The CCPA requires businesses to publish a specific Privacy Policy about their personal information trading practices.

• The GDPR provides a broader set of rights that allow individuals a high degree of control over their personal information. The CCPA provides some of these rights, but with more exemptions for businesses.

• The GDPR and CCPA are enforced via a different system of penalties.
CCPA
California Consumer Privacy Act of 2018

- Effective – January 1, 2020
- Enforcement – July 1, 2020
- Look-back to January 1, 2019
- Applies to companies worldwide, B2C and B2B
- Disclosure requirements, opt-in, opt-out re. “selling of personal information”
- New consumer rights to access, deletion, and porting of personal data
- New penalties
- New statutory damages in case of data security breaches
Who is Protected?

- Consumer = any California resident
- Natural persons
- Residency as defined in tax regulations
- Would include employees, patients, tenants, students, parents, children, etc.
Five Keys to Preparation

1. Determine if you are a business collecting or selling
2. Transparency and notice obligations
3. Responding to consumers personal information access requests
4. Rights of erasure objection to sale and non-discrimination
5. Penalties and enforcement
1. Determine if you are a business collecting or selling

- Any business worldwide doing business in California;
- exceeding thresholds of:
  - annual gross revenues of $25 million;
  - personal information of 50,000 or more California residents, households, or devices annually; or
  - 50% or more annual revenue from selling California residents' personal information.
- Parent companies and subsidiaries sharing the same branding, even if they themselves do not exceed the applicable thresholds.
Five Keys to Preparation

1. Determine if you are a business collecting or selling

- Clarifying in written contracts with business partners that Personal Information is not communicated for consideration
- Invoking statutory exceptions for
  - user-directed sharing
  - sharing with service providers
  - opt-out compliance
  - M&A transactions
Five Keys to Preparation

1. Determine if you are a business collecting or selling

Who must comply?
"Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.
Five Keys to Preparation

1. Determine if you are a business collecting or selling

"Selling" means any sharing of Personal Information for valuable consideration

- Decide: To Sell or Not to Sell Personal Information

- If selling
  - "Do Not Sell My Personal Information" link
  - Seek opt-in from 13-16 year old Californians, parental consent from children under 13

- Refrain from seeking opt-in for 12 months from California residents who have opted out
- No discrimination
- Free services, premium, trials?
For purposes of this title, a business does not sell personal information when:

A. A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title.

B. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions.

C. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

1. Determine if you are a business collecting or selling
Five Keys to Preparation

1. Determine if you are a business collecting or selling

For purposes of this title, a business does not sell personal information when:

C. The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purposes if both of the following conditions are met: services that the service provider performs on the business' behalf, provided that the service provider also does not sell the personal information.

   I. The business has provided notice that information being used or shared in its terms and conditions

   II. The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.
For purposes of this title, a business does not sell personal information when:

D. The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction (…)

1. Determine if you are a business collecting or selling
Five Keys to Preparation

2. Transparency and notice obligations

• Disclosure of Generic Collection Practices Upon Request.
  • Upon a consumer’s request, a business shall disclose “the categories and specific pieces of personal information the business has collected.”
  • At or before collection of a consumer’s personal information, a business shall “inform consumers as to the categories of
  • personal information to be collected and the purposes for which the categories of personal information shall be used.” The business shall not collect undisclosed categories, or make undisclosed uses, of personal information.
Five Keys to Preparation

2. Transparency and notice obligations

<table>
<thead>
<tr>
<th>Update Privacy Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide at or before collection: categories of personal information (PI) to be collected and underlying purposes (information may be provided elsewhere)</td>
</tr>
<tr>
<td>• Separate lists of categories of PI collected, sold or disclosed for a business purpose in the preceding 12 months (explicitly state if not sold or disclosed)</td>
</tr>
<tr>
<td>• Categories of sources of PI collected</td>
</tr>
<tr>
<td>• Business/commercial purposes for collecting or selling PI</td>
</tr>
<tr>
<td>• Categories of third parties receiving PI</td>
</tr>
</tbody>
</table>
Five Keys to Preparation

2. Transparency and notice obligations

Update Privacy Policies

- Description of the rights to access, deletion, to obtain information about disclosures, to opt out of sales, and not to be discriminated against

- If PI is sold: Fact that PI collected may be sold and clear and conspicuous link, titled "Do Not Sell My Personal Information", to webpage that enables opt-out

- Method(s) for submitting requests including, at a minimum, toll-free telephone number and, where maintained by the business, website address
Three Keys to Preparation

3. Responding to consumers personal information access requests

- **Request Mechanisms.** The law specifies many operational details about how consumers may make their requests and how businesses must and cannot treat those requests.

- Among other things, for the disclosures about collected and sold/disclosed personal information, the business must allow the consumer to make requests by at least two methods, including a toll-free number and a website (if the business has a website).
Five Keys to Preparation

4. Rights of erasure objection to sale and non-discrimination

Erasure.
- Upon a consumer’s request, a business shall delete any personal information about the consumer that the business collected from the consumer.

Specifications for Privacy Policies.
- Among other requirements, a business’ privacy policy must notify consumers about their erasure rights, collections and sales/disclosures of personal information, the opt-out/opt-in rights for data sales, and restrictions on privacy-based discrimination.
## Five Keys to Preparation

4. Rights of erasure objection to sale and non-discrimination

### Access, Deletion rights

Implement processes and policies to:

- verify the identity of individuals making requests
- timely provide portable copies
- delete personal information or claim statutory exception
- obtain assistance of service providers
Five Keys to Preparation

4. Rights of erasure objection to sale and non-discrimination

A business shall not discriminate against a consumer

A. Denying goods or services to the consumer.
B. Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
C. Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer’s rights under this title.
D. Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
Five Keys to Preparation

5. Penalties and enforcement

- Statutory damages $100-$750 per incident, per consumer
- $7,500 per intentional violation
- $2,500 for unintentional violations, if the company fails to cure the unintentional violation within 30 days of notice
- Cal State AG, Consumer Privacy Fund
CCPA Rights & Obligations

- The CCPA, while passed, is still actively changing: in the fall of 2019
- Final clarifications may not be until 2020, after the law is already in effect
- The California state legislature, may amend between now and January 1, 2020 operational date
- July 1, 2020 Attorney General-enforcement date
The Details

- General Disclosure and Privacy Notice Requirements
  - General Disclosure Requirements for the Collection, Sale, and Disclosure for a Business Purpose of Personal Information
- Disclosure Requirements for Financial Incentives
- Website Disclosure Requirements
  - Verifiable Consumer Request for Disclosure and Deletion
  - Methods to Submit a Request
- Steps to Verify a Consumer Request
- Information to be Disclosed in Response to a Consumer Request for Disclosure of Collection, Sale, or Disclosure for a Business Purpose

- Procedure to Respond to a Verifiable Consumer Request for Disclosure of Collection, Sale, Disclosure for a Business Purpose, or for Deletion
- Consumer’s Right to Opt Out of the Sale of Personal Information
- Obligations Regarding a Consumer’s Right to Opt Out
- Responding to a Consumer’s Request to Opt Out
- Penalties and Enforcement
- Business’s Obligation for Reasonable Security Procedures
What Data is Protected?

"Personal information" means 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.
What Data is Protected?

Personal information includes, but is not limited to, the following:

A. Identifiers such as a unique personal identifier, online identifier Internet Protocol address, or other similar identifiers.

B. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

C. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

D. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
How to Comply as an Employer?

**Employees:**

- can ask employers to disclose the categories and specific pieces of information collected. Once request is verified, information must be provided free of charge. No current mechanism for withholding sensitive HR records relating to the employee in response to such a request.

- can ask for their personal information to be deleted. Employer is allowed to retain information if it’s necessary for performance of the employment contract or based on other limited exceptions.

- have to be informed at or before point of collection about the categories of personal information collected and purposes of use. No additional categories of information can be collected without prior notice.

- have to be informed if personal information sold or disclosed to a third party for a “business purpose” (broadly defined as use for operational purposes). Can also opt-out of sale.
How to Comply as an Employer?

- Update employee privacy policies or notices with newly required information including a description of employee rights.
- Put in place written agreements with service providers receiving employee personal information restricting sale or unauthorized use of employee information.
- Make available designated methods for employees submitting data access requests, including, at a minimum, a toll-free telephone number.

- CA Legislature is looking to revise/clarify areas further before effective date.
- Currently 11 states with law on the Docket
- House and Senate are working on federal proposals
Resources

- International Association of Privacy Professionals (IAPP)
  - https://iapp.org/
  - Affordable basic membership
    - Constant information and updated
    - Articles, tools and guidance from many disciplines

- DLA PIPER
  - https://www.dlapiperdataprotection.com
    - Global privacy law
    - Updated and maintained content
    - Side by side comparisons of any laws
## Resources

### CaCPA: What To Disclose and Where To Disclose It

<table>
<thead>
<tr>
<th>WHAT MUST BE DISCLOSED</th>
<th>WHO MUST DISCLOSE</th>
<th>WHERE TO DISCLOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Collector of personal information</td>
<td>Seller of personal information</td>
</tr>
<tr>
<td>Categories of personal information collected about the consumer</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of the sources from which the personal information was collected</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Business or commercial purpose for collecting or selling personal information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of third parties with whom the business shares personal information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Specific pieces of personal information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of personal information sold</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of third parties to whom personal information was sold by category or categories of personal information sold for each third party to whom personal information was sold</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of personal information disclosed for a business purpose</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>A list of the categories of personal information sold about consumers in the preceding 12 months or, if no sale occurred, that fact</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>A list of categories of personal information disclosed for a business purpose in the preceding 12 months or, if no disclosure occurred, that fact</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
## Resources

<table>
<thead>
<tr>
<th>WHAT MUST BE DISCLOSED</th>
<th>WHERE TO DISCLOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Collector of personal information</td>
</tr>
<tr>
<td>Consumer’s rights: To request access to their personal information, along with one or more designated methods for submitting such requests</td>
<td>X</td>
</tr>
<tr>
<td>Consumer’s rights: To request deletion of their personal information</td>
<td>X</td>
</tr>
<tr>
<td>Consumer’s rights: To opt out of the sale of their business information</td>
<td>X</td>
</tr>
<tr>
<td>Not to be discriminated against for exercising any of their other California rights</td>
<td>X</td>
</tr>
<tr>
<td>Financial Incentives programs: Notice of any financial incentives pursuant to Section 1798.125(b)</td>
<td>X</td>
</tr>
<tr>
<td>Financial Incentives programs: Clear description of material terms of any financial incentive program</td>
<td>X</td>
</tr>
</tbody>
</table>
THANK YOU

Eric Rankin
erankin@simpleviewinc.com

www.simpleviewinc.com