GDPR and CCPA: Key challenges for getting compliant and staying compliant

Southern California Regional Compliance & Ethics Conference

January 25, 2019

Introductions

Kim Richardson

Kim Richardson is Asst. Gen. Counsel of Privacy, Advertising & Marketing at Mattel, Inc. She also serves as an Adjunct Professor of Cybersecurity and Regulatory Compliance at Loyola Law School, Los Angeles.

The opinions expressed in this presentation are her own and do not necessarily represent the positions, strategies or opinions of Mattel, Inc. or any of its affiliated companies or of Loyola Law School.

R. Olivia Samad

R. Olivia Samad is privacy counsel at Southern California Edison, one of the nation's largest electric utilities, delivering power to 15 million people in 50,000 square-miles across central, coastal and Southern California.

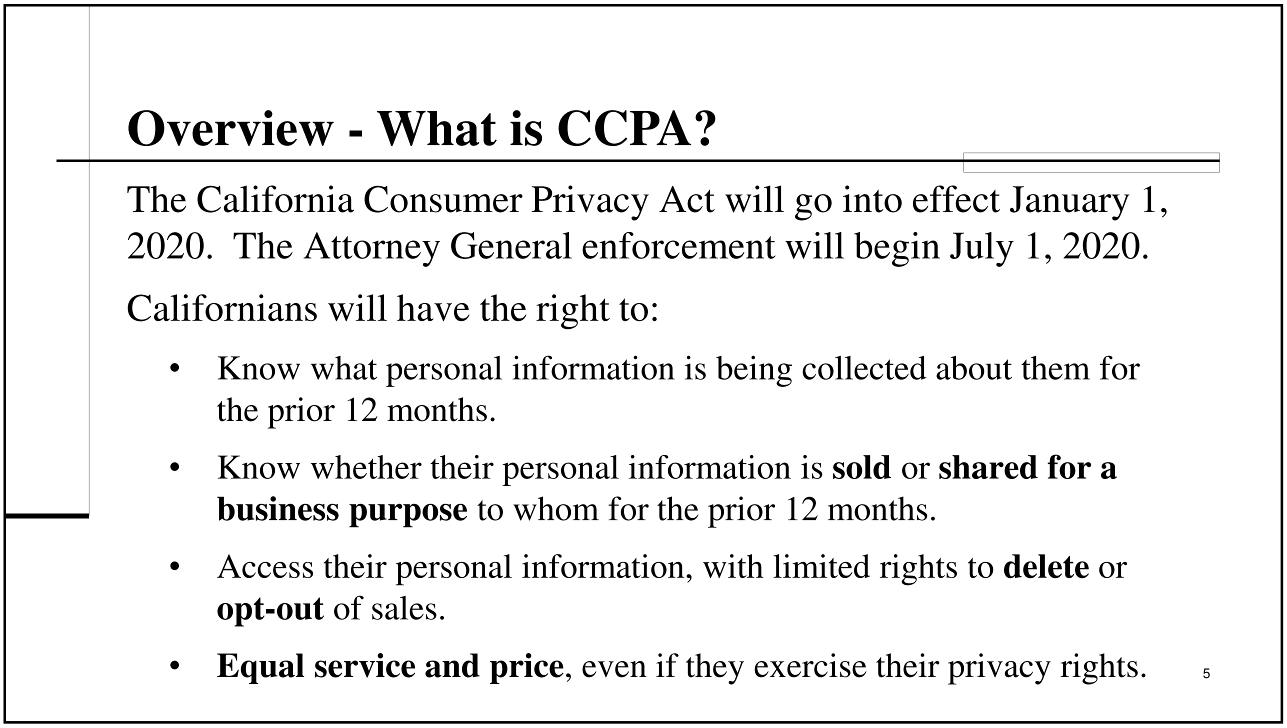
The opinions expressed in this presentation are her own and do not necessarily represent the positions, strategies or opinions of Southern California Edison, its parent company Edison International or any of their affiliates.

Agenda

1. **Overview of GDPR and CCPA**
2. **Key compliance requirements and activities**
3. **Compliance planning considerations**
4. **Questions**

Overview - What is GDPR?

- The General Data Protection Regulation is comprehensive EU data protection legislation that took effect May 25, 2018.
- Replacing the 1995 EU Data Protection, GDPR sought to increase harmonization across EU member states.
- GDPR provides for increased individual rights for EU residents and demands greater accountability from organizations.
- Penalties for violations can be the greater of 20M Euro or 4% of global turnover.

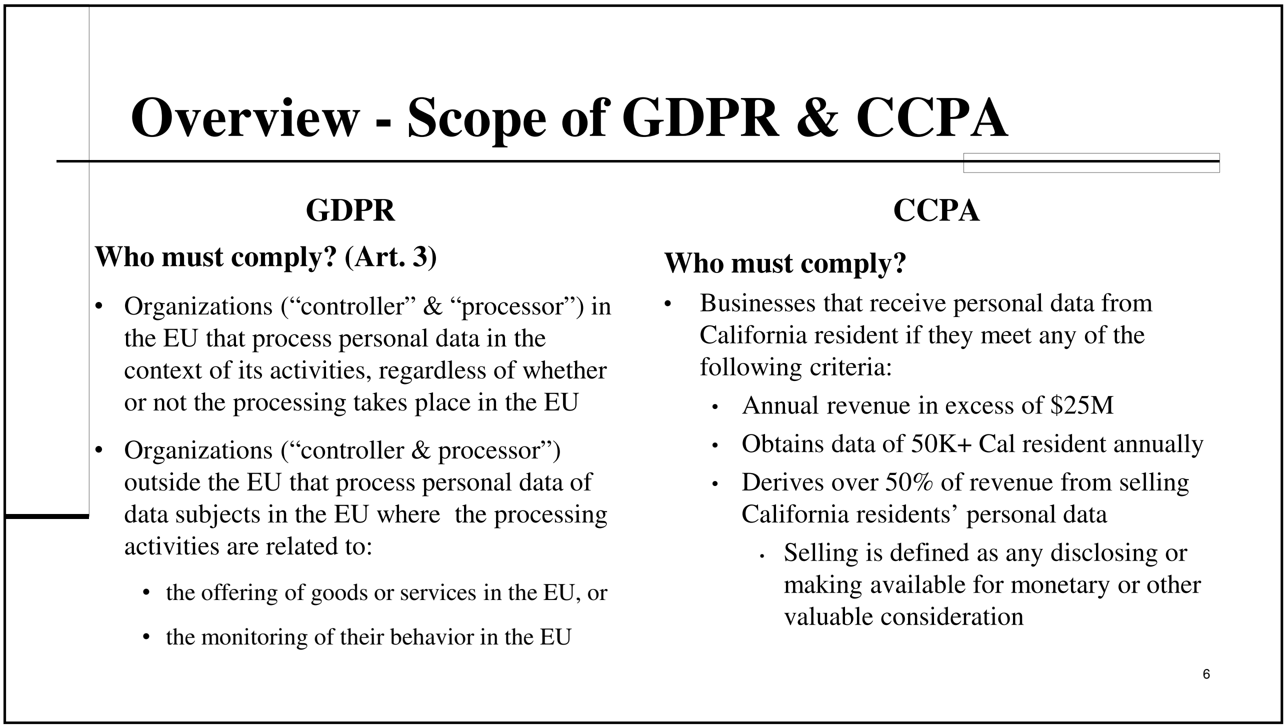


Overview - What is CCPA?

The California Consumer Privacy Act will go into effect January 1, 2020. The Attorney General enforcement will begin July 1, 2020.

Californians will have the right to:

- Know what personal information is being collected about them for the prior 12 months.
- Know whether their personal information is **sold** or **shared for a business purpose** to whom for the prior 12 months.
- Access their personal information, with limited rights to **delete** or **opt-out** of sales.
- **Equal service and price**, even if they exercise their privacy rights.



Overview - Scope of GDPR & CCPA

GDPR

Who must comply? (Art. 3)

- Organizations (“controller” & “processor”) in the EU that process personal data in the context of its activities, regardless of whether or not the processing takes place in the EU
- Organizations (“controller & processor”) outside the EU that process personal data of data subjects in the EU where the processing activities are related to:
  - the offering of goods or services in the EU, or
  - the monitoring of their behavior in the EU

CCPA

Who must comply?

- Businesses that receive personal data from California resident if they meet any of the following criteria:
  - Annual revenue in excess of $25M
  - Obtains data of 50K+ Cal resident annually
  - Derives over 50% of revenue from selling California residents’ personal data
    - Selling is defined as any disclosing or making available for monetary or other valuable consideration

Overview - Scope of GDPR & CCPA

GDPR

Who is protected?

- Natural persons who are present in the EU

What data is covered?

- "Personal data" means any information relating to an identified or identifiable natural person ("data subject")

CCPA

Who is protected?

- Consumer is defined as "any natural person who is a California resident"

What data is covered?

- Any "information that… identifies or relates to…a particular consumer or household"

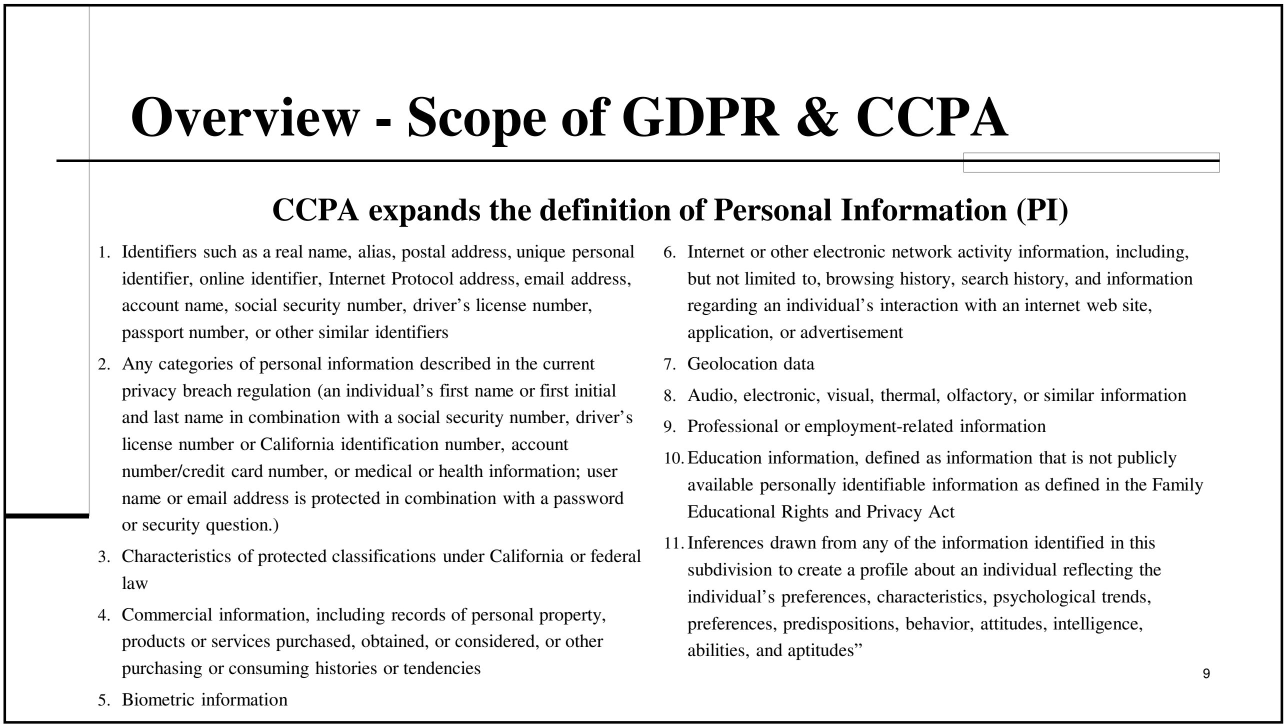
Overview - Scope of GDPR & CCPA

GDPR's broad definition of personal data accounts for new technology:

- 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;

Processing of **Special Categories** of data is restricted (**Art. 9):**

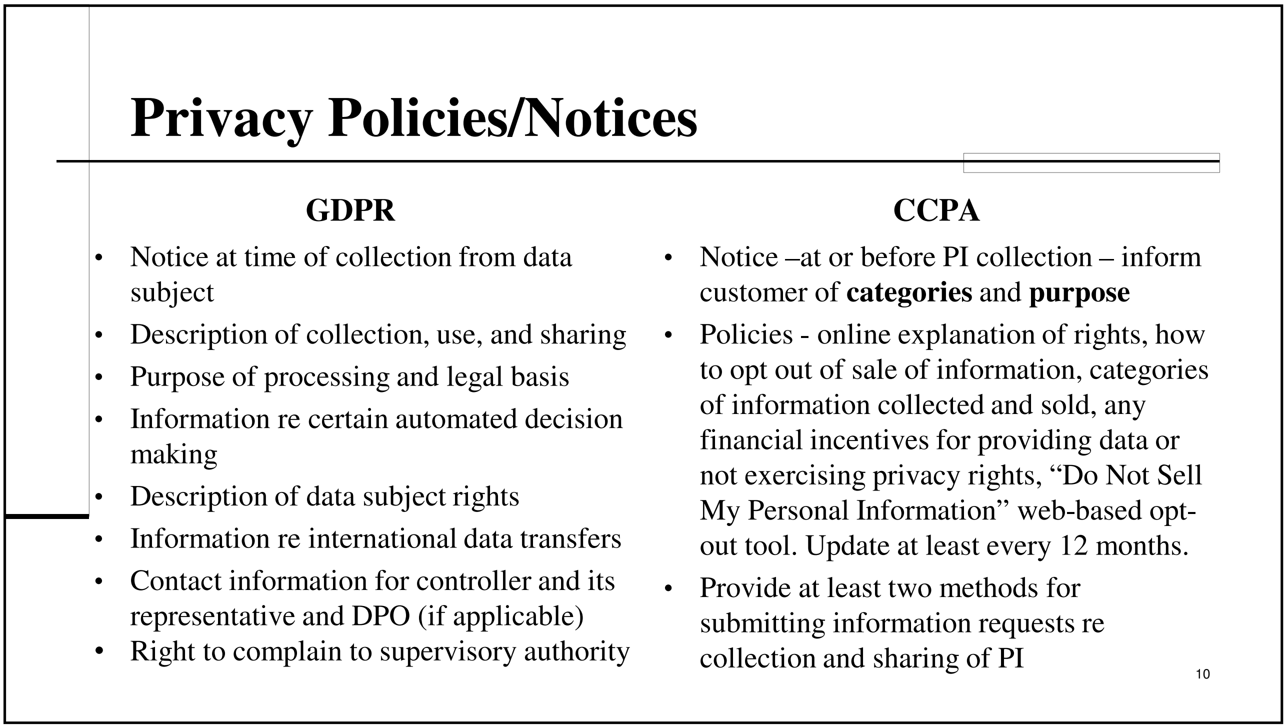
- Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited



Overview - Scope of GDPR & CCPA

CCPA expands the definition of Personal Information (PI)

1. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers
2. Any categories of personal information described in the current privacy breach regulation (an individual's first name or first initial and last name in combination with a social security number, driver's license number or California identification number, account number/credit card number, or medical or health information; user name or email address is protected in combination with a password or security question.)
3. Characteristics of protected classifications under California or federal law
4. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
5. Biometric information
6. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding an individual's interaction with an internet web site, application, or advertisement
7. Geolocation data
8. Audio, electronic, visual, thermal, olfactory, or similar information
9. Professional or employment-related information
10. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act
11. Inferences drawn from any of the information identified in this subdivision to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes"



Privacy Policies/Notices

GDPR

- Notice at time of collection from data subject
- Description of collection, use, and sharing
- Purpose of processing and legal basis
- Information re certain automated decision making
- Description of data subject rights
- Information re international data transfers
- Contact information for controller and its representative and DPO (if applicable)
- Right to complain to supervisory authority

CCPA

- Notice –at or before PI collection – inform customer of **categories** and **purpose**
- Policies - online explanation of rights, how to opt out of sale of information, categories of information collected and sold, any financial incentives for providing data or not exercising privacy rights, "Do Not Sell My Personal Information" web-based opt-out tool. Update at least every 12 months.
- Provide at least two methods for submitting information requests re collection and sharing of PI

Individual Rights

GDPR (one month to respond)

Access & Portability

- Obtain copy of data. In some cases, right to receive data in structured form for transfer

Rectification: Correct inaccurate data, and in some cases, incomplete data

Objection & Restriction:

- Prohibit certain processing (e.g. direct marketing) & limit certain processing

Erasure ("Right to be Forgotten")

- Deletion of data in some circumstance
- Vendor assistance/cooperation

CCPA (45 days to respond)

Access & Portability

- access to "specific pieces of personal information" in the last 12 months in portable, readily usable format

Objection & Restriction

- Opt out of sale or sharing of data in some cases.

Erasure ("Right to be Forgotten")

- Delete data received "from the consumer"
- Direct service provider to delete information

Vendor Management

GDPR

Processor Contracting (Art. 28)

- Processor agreements must contain sufficient guarantees of compliance, including, for example:
- process data only as instructed by controllers
- use appropriate measures for secure processing
- delete or return data once processing is complete

CCPA

"Service provider" acts as an exception and not a business obligation.

If a business discloses information with a "**service provider**" (versus a "**third party**") to perform a **business purpose**, that is not a "**sale**"

Businesses have an obligation to direct service providers to delete personal information

Consumers may not opt-out of disclosures to service providers

Data Security & Breach Notification

GDPR

Appropriate Security (Art. 32)

- Controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk

Breach Notification (Art. 33)

- Controller notifies Supervisory Authority within 72 hours (where feasible), unless unlikely to result in a risk to individuals
- Controller notifies data subject if breach is likely to result in *high risk* to individuals
- Definition of breach and personal data differs from U.S.

CCPA

Private right of action

Consumer may sue under CA safeguards law for breach of reasonable security procedures for $100 to $750 per consumer per incident or actual damages, whichever is greater. (PI is defined by CCV 1798.81.5)

Enforcement by State Attorney General

A business violates the Act if "it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance"

$2,500 in civil penalties for each violation

$7,500 for each intentional violation

GDPR Accountability

Privacy By Design & Default (Art. 25)

- Controller will implement appropriate technical and organizational measures, such as pseudonymization and data minimization, to integrate compliance into data processing

Data Protection Impact Assessments (Art. 35)

- Controller will perform a Data Protection Impact Assessment for high risk processing activities

Record or Processing Activity (Art. 30)

- Controllers and processors will maintain a record or processing, including categories of data subjects & personal data, purpose of processing, security measure, and additional details

Data Protection Officer (Art. 37)

- When there is systematic monitoring of data subjects on a large scale or large scale processing of sensitive data

Compliance Planning Considerations

1. Global or specific approach – consider whether you will apply requirements only to covered individuals or more broadly
2. Data mapping and inventory – start early to identify data held and purpose of processing
3. Privacy Policies – plan for updates
4. Vendor agreements – consider time required to update contracts
5. Individual rights – consider processes, tools, automation & training
6. PIA/DPIA – consider if and when this is advisable, even when not required, and process for completion and documentation

Thanks for your participation!