Data Privacy & Compliance for AICP Members Under CCPA and GDPR.

Privacy Presentation by

Ellenoff Grossman & Schole LLP

Atul Singh Honeah Mangione

Ellenoff Grossman & Schole LLP

Characters of Privacy

Data subject

Hi! My Name Is….

Controllers

Hi! I collect your data.

Processor

Hi! I follow directions.

Data Brokers

I'm buying your data.

Governing Authority

Are you following the rules?

Data Processing

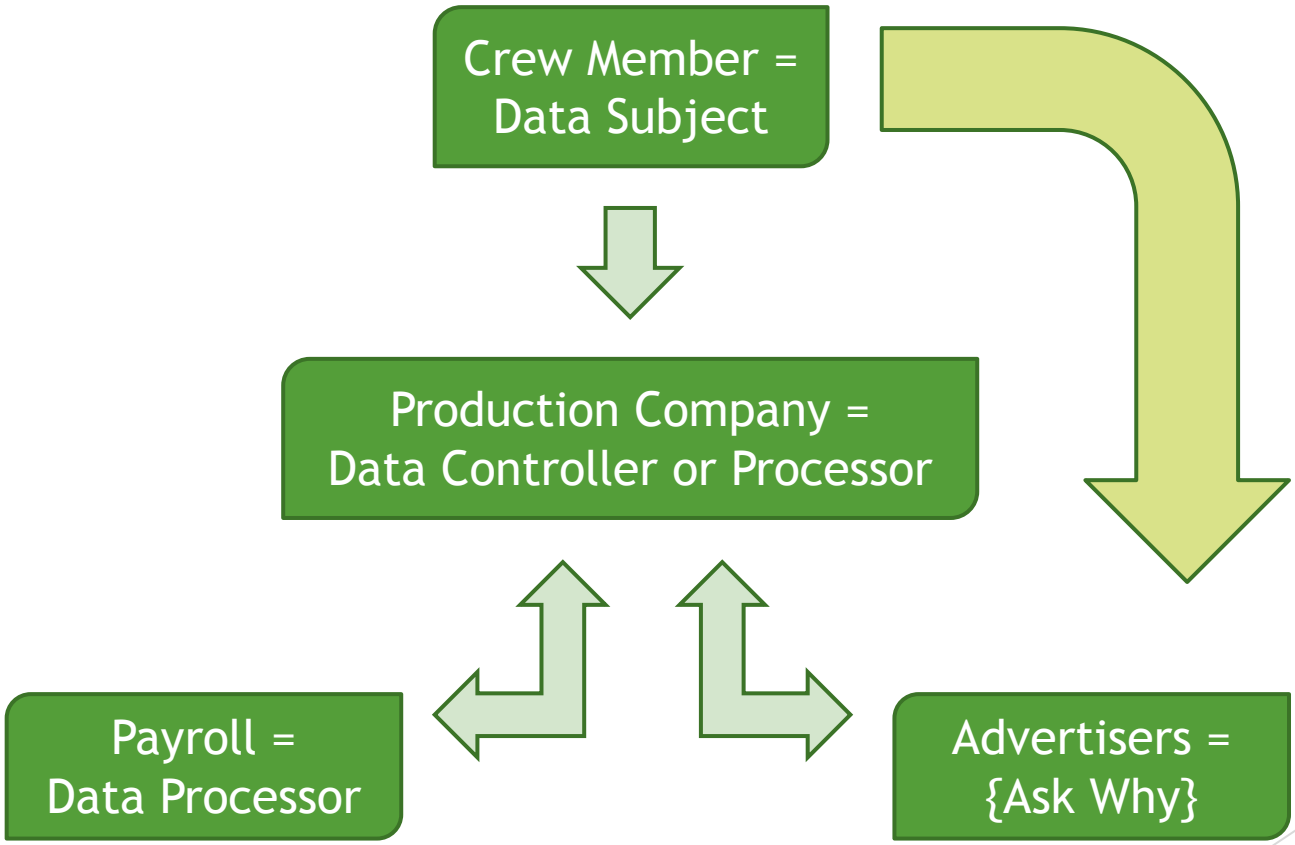
- Meaning: operation or set of operations performed upon personal data/personal information
  - Collection, recording, organizing, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available
- Nature of Processing: either automated or not

Objectives: 1. LAWFULNESS
2. FAIRNESS
3. TRANSPARENCY

General Requirements:

- Limit collection to what is necessary for the purpose
- Take steps to ensure collected data is accurate
- Data is secure with appropriate safeguards
- Do not keep for longer than necessary

Possible Data Flow



What are CCPA and CPRA?

- CCPA is the "California Consumer Privacy Act" – A privacy protection law from 2018 meant to protect the Personally Identifiable Information ("PII") of CA residents
- CPRA is the "California Privacy Rights Act" and is an amendment to CCPA approved by CA voters in November 2020 pursuant to "Proposition 24"
- CPRA expanded the rights available to CA residents under CCPA and went into effect January 1, 2023

Who needs to comply with CPRA?

- Any for-profit business that collects CA consumers' PII or on whose behalf such PII is collected and that, either jointly or with others, determines the purposes and means of processing of such PII and meets at least one of the following thresholds:
  - Had gross revenues in excess of $25 million in the preceding calendar year;
  - Annually buys, sells, or shares the PII of 100,000 or more CA consumers, households, or devices; or
  - Derives 50% or more of its annual revenues from selling CA consumers' PII.

What Is PII Under CCPA/CPRA?

- PII is any information that identifies, relates to, or could reasonably be linked with a CA resident or household. It can include name, social security number, email address, address, phone number, geolocation data, fingerprints, and inferences from other personal information that could create a profile about the person's preferences and characteristics.
- CPRA expanded definition of PII by adding a category of "Sensitive Personal Information" which includes: biometric information, CA identification card number, contents of consumers' email, mail, or texts unless business is intended recipient, credit or debit card number combined with security code or password, drivers' license number, ethnic origin, financial account number (which permits access to account), genetic data, health information, passport number, philosophical beliefs, precise geolocation, racial origin, religious beliefs, sex life or sexual orientation, social security number, or union membership.

What is PII Under CPRA (cont'd)?

- As of January 1, 2023, PII collected from employees and independent contractors is PII under the CPRA.
- Employees and contractors, therefore, have all the same potential rights under CPRA as do consumers.

What is Not PII Under CCPA/CPRA?

- PII does not include "publicly available" information or lawfully obtained, truthful information that is a matter of public concern. "Publicly available" means PII that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

What Rights Are Created Under CCPA/CPRA?

CCPA created the following:

- Right to know what PII is being collected and how it is used and shared;
- Right to request deletion of PII;
- Right to opt out of "sale" or "sharing" PII with third parties (both of which have specific definitions);
- Right to opt-in to sale of PII if under 16;
- Right to non-discrimination for exercising CCPA rights;
- Right to data portability;
- Right to private right of action (limited to data breaches and for only certain unredacted or unencrypted information).

CPRA added the following:

- Right to correct inaccurate PII;
- Right to limit use and disclosure of sensitive PII.

What is “selling” or “sharing” under CCPA/CPRA?

- “Sale”, “Sell”, or ” Selling” is selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s PII by the business to a third party **for monetary or other valuable consideration**
- “Sharing” means sharing, 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 a third party **for cross-context behavioral advertising**, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.
- Key Takeaways – A sale can include benefits other than money and “sharing” has a specific and a narrow definition under CPRA

Right to Limit Use of Sensitive PII

- CPRA permits businesses to use sensitive PII for the following purposes without offering right to opt out:
  - Performing services reasonably expected by the consumer;
  - Providing goods or services reasonably expected by the consumer;
  - Ensuring security and integrity of the consumer's information;
  - Other short-term and transient uses (e.g., non-personalized advertising as long as information not shared with third party or used to build profile about consumer);
  - Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business; or
  - Product or service improvement.
- After Jan. 1, 2023, if a business wants to use sensitive PII for something other than the purposes described above, the business has to include that additional purpose in their notice at collection and inform the consumer of their right to opt-out of the additional use and include a link on its website titled "Limit the Use of My Sensitive Personal Information"

Notice at Collection under CCPA/CPRA

- Purpose: inform data subjects about (categories of) information collected, purpose for collection, and whether that information is sold or shared
- Deviations from Stated Notice: not permissible
- Scope of "Collection": unlimited
  - Online collection (using cookies/trackers)
  - Offline collection (using paper forms)
  - Oral collection (using telephone/in person conversations)
- Additional Req't of Notice:
  - Must be reader friendly and accessible
  - Must provide link/website to privacy policy and opt-out rights

Sample of notice:

Notice Regarding Personal Information Collected

[COMPANY NAME] (“we”) collects your personal information and sensitive personal information in order to assemble a production crew for a particular assignment and for payroll purposes. This notice serves to inform you of our handling of your personal information and sensitive information.

We may collect the following personal information and sensitive personal information listed in the table below. The table also lists our expected retention period, and use purposes for collecting and retaining your information. The information in bold is deemed “sensitive personal information” under the California Privacy Rights Act of 2020 (CPRA). Sensitive personal information is a subtype of personal information consisting of specific information categories. While we collect information that falls within the sensitive personal information categories listed in the table below, the CCPA does not treat this information as sensitive because we do not collect or use it to infer characteristics about a person.

Personal Information Category	Retention Period	Business Purpose	Sharing
First name, last name, address, email address, phone number, account name, **Social Security number, driver's license number**	7 years	Identify you for a (prospective) job Employment and payroll purposes	Shared with advertisers to complete production/creative tasks

We will not sell the personal information, including any sensitive personal information, we collect or share it with third parties for the purpose of cross-context behavioral advertising.

To view our full privacy [policy/notice], visit [PRIVACY POLICY URL].

If you have any questions about this Notice or need to access it in an alternative format due to having a disability, please contact [COMPANY EMAIL ADDRESS] and [COMPANY PHONE NUMBER].

[EFFECTIVE DATE]

Retention of Personal Information under CCPA/CPRA

- Golden Rule: Do not retain information for longer than necessary for the purpose collected
- Notice of Retention: Must disclose either how long personal information will be retained, or the criteria used to determine retention period, subject to the Golden Rule.
- Federal and State laws may impose retention requirement

Personnel Records under Cal. Labor Code § 1198.5(a)	**Three Years After termination**

Deletion Request Exceptions

1. Complete the transaction for which the PII was collected, fulfill the terms of a written warranty or product recall, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;
3. Debug to identify and repair errors that impair existing intended functionality;
4. Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law;
5. Comply legal obligations (e.g., litigation holds, tax purposes);
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent;
7. To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business (best interpreted as a "legitimate interests" exception);
8. Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

The General Data Protection Regulation (GDPR)

- Became effective May 25, 2018
- Designed to give EU citizen more control over their personal data
- Key attributes:
  - ensure that Personal Data is gathered legally and under strict conditions;
  - Personal Data is Protected from misuse and exploitation
  - Respect Rights of Data Owners

To Whom does GDPR Apply

- Any organization operating within the EU and engaged in any professional or commercial activity
  - What if the Data is Not Processed in the EU?
    - GDPR still applies if data is stored outside of EU
    - GDPR still applies if data is used outside of EU
- Any organizations outside of the EU that…
  - (i) offer goods or services to customers or businesses in the EU or
  - (ii) monitors online behavior of EU citizens/residents

Personal Data under GDPR

- Personal Data: as any information that relates to an identified or identifiable natural person.
- What format of Data is “Personal Data”?
  - Under GDPR, personal data is format-agnostic
    - Personal Data can be in the form of images, video, audio, numerals, and words.
  - If data does not directly associate or identify a person, is it still personal data?
    - Personal data is data that creates both direct and indirect associations with a person.
      - E.g. Direct Association: financial information; address, phone number
      - E.g. Indirect Association: evaluations relating to the behavior patterns of a person

Processing of Personal Data under GDPR

1. **Consent**
   - **Must be freely given, clear, and easy to withdraw**
2. **Performance of a Contract**
   - **Processing activity to enter into or perform a contract**
3. **Legitimate Interest**
   - **Processing Activity is Normally Expected on Balance**
     I. **Is this processing activity necessary for the organization to function?**
     II. **Does the processing activity outweigh any risks to a data subject's rights and freedoms?**
4. **Vital Interest**
   - Processing is Required to Save Life
5. **Legal Requirement**
   - E.g. Information Security, Employment
6. **Public Interest**
   - **Processing Occurs on behalf of Government Entity**

Notice to Data Subjects under GDPR

- Who is responsible for providing notice:
  - Data Controller
- What are the data controller's responsibilities?
  - Identify controller and provide contact information
  - Describe purpose for collection/legal basis for processing
  - Identify recipients (if any) of personal data; whether transfer to third country;
  - Define period of retention
  - Notify data subjects of rights

Data Subject Rights

1. **Right to be informed:**
   - Data subjects have the right to be informed about the collection and use of their personal data.
2. **Right to access**
   - Data subjects have the right to view and request copies of their personal data.
3. **Right to rectification**
   - Data subjects have the right to request inaccurate or outdated personal information be updated or corrected.
4. **Right to be forgotten/Right to erasure**
   - Data subjects have the right to request their personal data be deleted. Note that this is not an absolute right and may be subject to exemptions based on certain laws.
5. **Right to data portability**
   - Data subjects have the right to ask for their data to be transferred to another controller or provided to them. The data must be provided in a machine-readable electronic format.
6. **Right to restrict processing**
   - Data subjects have the right to request the restriction or suppression of their personal data.
7. **Right to withdraw consent**
   - Data subjects have the right to withdraw previously given consent to process their personal data.
8. **Right to object**
   - Data subjects have the right to object to the processing of their personal data.
9. **Right to object to automated processing**
   - Data subjects have the right to object to decisions being made with their data solely based on automated decision making or profiling.

Transfer of Personal Data under GDPR to non-EU Country

- General Principle: Transfer of personal data to non-EU country (that is deemed inadequate) is unlawful.
- Transfer can be made lawful if:
  - Non-EU country is exempt because it has equivalent privacy standards and adequacy decisions
  - There are appropriate safeguards in place; data subjects have enforceable rights and effective legal remedies
    - Use standard contractual clauses
  - There is derogation of the specific situation
    - Data Subject consents after being informed of risks of transfer
    - Transfer necessary for performance of contract

Comparison of GDPR and CPRA

GDPR

- A Data Controller can be any person/entity, including public bodies
- Applies to businesses that have a presence in EU
- Must have a legal basis to process data or consent

CPRA

- Business is defined, and generally applies to big, for-profit businesses
- Applies to businesses that operate in California
- Must have notice prior to or at point of collection

Deletion Requirement

Data Subjects have Right to Deletion under CPRA and GDPR

- General Principles
  - Must delete according to deletion policy term
  - Must delete when reason/purpose no longer applicable
  - Must delete upon request
- EXCEPTIONS (CPRA)
  - Internal use aligned with consumer's relationship with biz
  - Internal use compatible with context for providing info
- EXCEPTIONS (GDPR)
  - Legal obligations/Exercise of Official Authority
  - Reasons of Public Interest

Data Retention

Data Should be an Asset, Not a Liability

How long retain and How to Dispose

- CPRA

Retain only for so long as necessary for disclosed purpose.

- Data collected for one purpose should not be processed for another
- Must disclose data policy at or before collection

- GDPR

Retain only for so long as necessary for disclosed purpose.

- Data collected for one purpose should not be processed for another
- Must disclose data policy at or before collection

Recommendation:

- Retain Data for Statutory Minimum Period and
- Communicate the Periods with your Employees