THE CALIFORNIA CONSUMER PRIVACY ACT

IT'S NOT TOO LATE TO GET STARTED!

November 21, 2019

orrick

Introductions

Heather Sussman

Global Co-Chair

Cyber, Privacy &
Data Innovation

Kyle Kessler

Managing Associate

Cyber, Privacy &
Data Innovation

AGENDA

- Overview
- CCPA Requirements
  - Who is Covered by the CCPA
- Compliance Plan
  - Critical Compliance Obligations
  - Leveraging GDPR Compliance Efforts
- Enforcement and Penalties
- The Future of Privacy Regulations at the State and Federal Levels

CCPA REQUIREMENTS

Overview

CCPA Go-Live

5 Weeks and 5 Days

CCPA Private Right of Action For Data Breaches

5 Weeks and 5 Days

CCPA Attorney General Enforcement Date

31 Weeks and 5 Days

CCPA Requirements: Who is Covered?

The CCPA applies to any for-profit entity that:

- Does business in California
- Collects, receives or accesses California residents' personal information
- Decides **why and how** such personal information is used, AND
- Satisfies at least one of the following criteria:
  - **$25 MM Revenue** – Has annual gross revenue over $25 million;
  - **Trades/Transfers Data** – Annually buys, receives for commercial purposes, sells or shares for commercial purposes the personal information of 50,000 California consumers, households or devices; or
  - **Data Broker** – Derives 50% or more of annual revenue from selling consumers' personal information

– The CCPA also applies to an entity that **controls** or **is controlled** by a covered business that shares **common branding**.

CCPA Requirements: Scope

The CCPA does not apply to:

- PI collected, processed, sold or disclosed pursuant to:
  - the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA) and the California Financial Information Privacy Act (FIPA).
  - ***BUT**, data collected under these exemptions can arguably serve as the basis of a private right of action under the CCPA in the event of a qualifying data breach.*
- Certain health-related PI and drivers' license PI processed pursuant to other federal statutes and regulations (HIPAA, the Common Rule, CMIA, DPPA)

PRACTICE NOTE: CCPA exempts only the personal information collected pursuant to these statutes, **but** a business may collect other types that are subject to the CCPA (e.g., IP address, cookie data, employee data, etc.).

CCPA Requirements: Scope

The CCPA Amendments also provide key **limited exemptions**:

- **AB-25** provides a limited CCPA exemption for **employee data** until January 1, 2021.
- Employee data means:
  - Personal information that is collected by a business about a natural person in the course of the natural person **acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business** to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.
  - Personal information that is collected by a business that is emergency contact information of the natural person… to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.
  - Personal information that is necessary for the business to retain to administer benefits for another natural person… to the extent that the personal information is collected and used solely within the context of administering those benefits.

But, the employee exemption does not apply to:

- section 1798.100(b), which requires a CCPA-covered business to disclose "at or before the point of collection" the categories of personal information to be collected and the purposes for which such information will be used, and
- section 1798.150, which permits a private right of action for breaches caused by a business' violation of the duty to implement and maintain reasonable security procedures and practices.

CCPA Requirements: Scope

The CCPA Amendments also provide key **limited exemptions**:

- **AB-1355** creates a **B2B exemption** from most provisions of the CCPA until January 1, 2021.
- B2B information means:
  - "personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency."

  But, the B2B exemption does not apply to:

  - section 1798.120 the right to opt out of sales of personal information.
  - section 1798.150, which permits a private right of action for breaches caused by a business' violation of the duty to implement and maintain reasonable security procedures and practices.

Definition of “Consumer”

Consumer is:

a natural person who is a California resident . . . however identified, including by any **unique identifier**.

- **“Unique identifier”** or **“Unique personal identifier”** means a persistent identifier that can be used to recognize a consumer, a family or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers or similar technology; customer number, unique pseudonym or user alias; telephone numbers, **or other forms of persistent or probabilistic identifiers** that can be used to identify a particular consumer or device. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

- “**Probabilistic identifier**” means the identification of a consumer or a device to **a degree of certainty of more probable than not** based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

Incredibly broad!

CCPA: “Personal Information” is Defined Broadly

DEFINITION – Information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, to a particular ***consumer*** or ***household***. Categories of PI include:

THE USUAL SUSPECTS

- Name
- SSN
- Financial Information *(exc. GLBA)*
- Contact Information
- Signature
- Physical Characteristics
- Insurance Policy Number
- Other Gov’t IDs
- Health Data *(exc. HIPAA)*
- Passport
- Driver's License

INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY

- Search History
- Browsing History
- Cookie Data
- Interest Data
- IP Address
- Online Interactions

PROFESSIONAL, EMPLOYMENT AND EDUCATION-RELATED INFORMATION

BEHAVIORAL AND PROFILING DATA

- Tendencies
- Products/Services Considered
- Inferences
- Interest Data
- Search History
- Order History
- Purchase History

BIOMETRIC AND GEOLOCATION INFORMATION

SENSORY DATA

- Audio
- Electronic
- Visual
- Thermal
- Similar Information
- Olfactory

PROTECTED CLASSIFICATIONS

- Race
- Citizenship
- Color
- National Origin
- Military Status
- Religion
- Gender Identity and Expression
- Sex
- Medical Condition or Disability
- Marital Status
- Age
- Genetic Information

COMPLIANCE PLAN

CRITICAL COMPLIANCE OBLIGATIONS

CCPA: Critical Compliance Obligations

1. Notice & Transparency
2. Data Subject Rights
3. “Do Not Sell” Requirements
4. Reasonable Security

Practice Note: With only weeks left before the January 1 date, a focus on implementing sufficient disclosures and a means for consumers to submit requests should be the first priority for most businesses moving forward.

CCPA: Critical Compliance Obligations

Notice & Transparency – Required Disclosures

- A **Business** must update its privacy notice to **DISCLOSE**:
  - the categories of PI it collects, sells and otherwise discloses for a business purpose;
  - the categories of sources of the PI;
  - the business or commercial purposes for collecting or selling the PI;
  - the categories of third parties with whom the business sells or otherwise discloses the PI; and
  - a description of the consumers' rights and the designated methods for submitting requests.

Important Note: Purpose Specification and Use Limitation (See 1798.100(b))

*Effective: **January 1, 2020** (+12-Month Lookback)*

CCPA: Critical Compliance Obligations

Personal Information Inventory

Categories of PI Collected ***Check all that apply***	**Purposes for Collecting PI** ***How and why is PI collected?***	**Categories of PI Disclosed** ***Check all that apply***	**Purposes for Disclosing PI** ***How and why is PI disclosed?***
☒ Identifiers ☐ CA Customer Records ☐ Protected Classification Characteristics ☒ Commercial Info ☐ Biometric Info ☐ Internet/Network Info ☒ Geolocation Data ☐ Sensory Info ☐ Professional/ Employment Info ☐ Education Info ☐ Other PI ☐ Inferences	*We collect name, email, phone number, Ad IDs, transaction info and GPS location data using our mobile app in order to provide our services and target ads.*	☒ Identifiers ☐ CA Customer Records ☐ Protected Classification Characteristics ☐ Commercial Info ☐ Biometric Info ☐ Internet/Network Info ☒ Geolocation Data ☐ Sensory Info ☐ Professional/ Employment Info ☐ Education Info ☐ Other PI ☐ Inferences	*We share Ad IDs and GPS location with third parties who use this info for market research purposes.*

CCPA: Critical Compliance Obligations

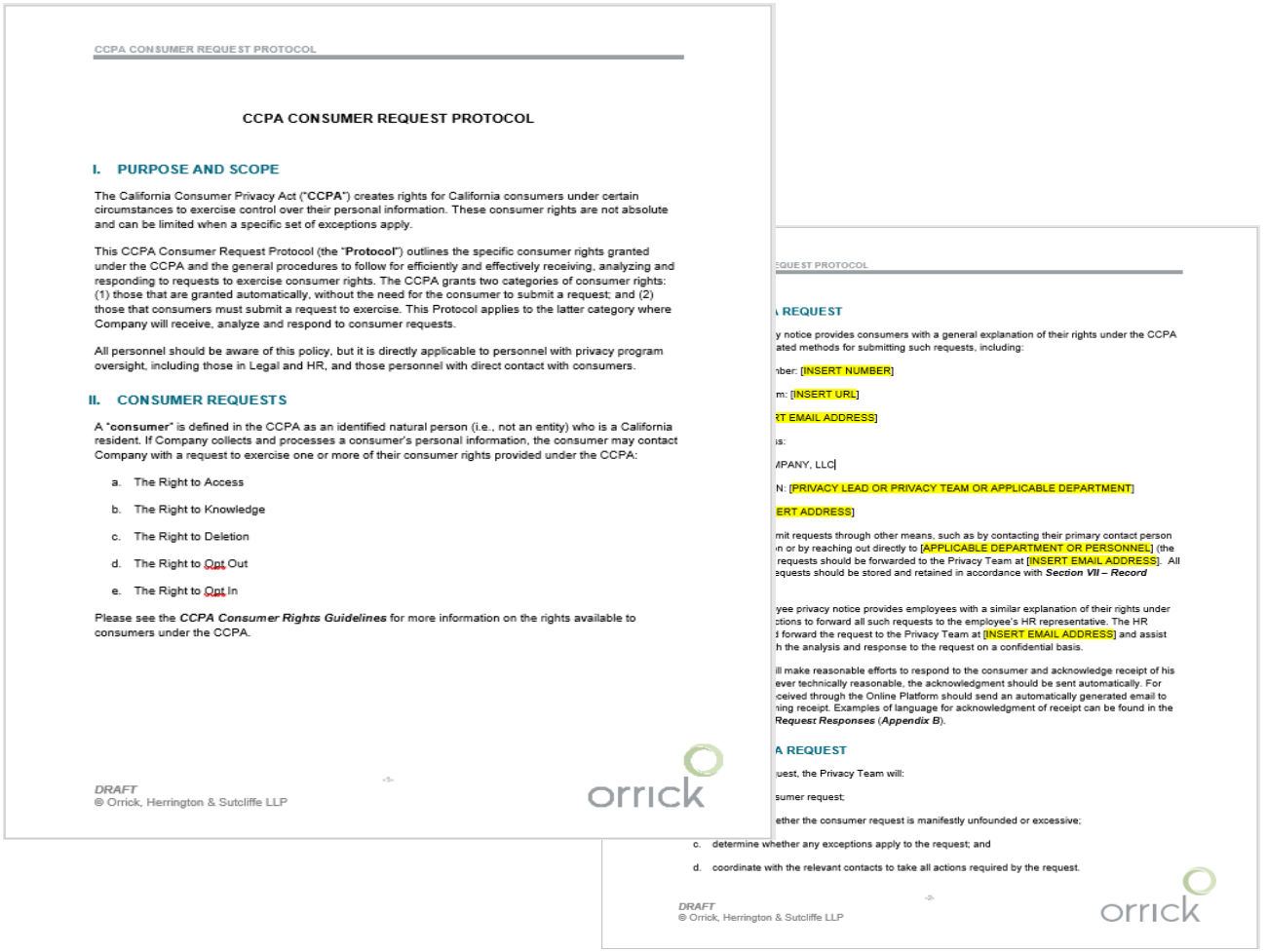
Data Subject Rights – Highlights

- Must **PROVIDE INFORMATION**: requested by the consumer about the processing of that consumer's PI (tailored version of privacy policy disclosures)
- Must **PROVIDE ACCESS**: to the PI collected over the past 12 months in a portable format within 45 days, in response to a "verifiable consumer request"
- Must **DELETE**: PI upon a "verifiable consumer request" (and direct "service providers" to delete), subject to exceptions
- Right to **OPT OUT**: of the "sale" of PI (more on this in a few slides)

Effective: January 1, 2020 (+12-Month Lookback)

CCPA: Critical Compliance Obligations

Consumer Request Protocols



CCPA CONSUMER REQUEST PROTOCOL

CCPA CONSUMER REQUEST PROTOCOL

I. PURPOSE AND SCOPE

The California Consumer Privacy Act ("**CCPA**") creates rights for California consumers under certain circumstances to exercise control over their personal information. These consumer rights are not absolute and can be limited when a specific set of exceptions apply.

This CCPA Consumer Request Protocol (the "**Protocol**") outlines the specific consumer rights granted under the CCPA and the general procedures to follow for efficiently and effectively receiving, analyzing and responding to requests to exercise consumer rights. The CCPA grants two categories of consumer rights: (1) those that are granted automatically, without the need for the consumer to submit a request; and (2) those that consumers must submit a request to exercise. This Protocol applies to the latter category where Company will receive, analyze and respond to consumer requests.

All personnel should be aware of this policy, but it is directly applicable to personnel with privacy program oversight, including those in Legal and HR, and those personnel with direct contact with consumers.

II. CONSUMER REQUESTS

A "**consumer**" is defined in the CCPA as an identified natural person (i.e., not an entity) who is a California resident. If Company collects and processes a consumer's personal information, the consumer may contact Company with a request to exercise one or more of their consumer rights provided under the CCPA:

a. The Right to Access
b. The Right to Knowledge
c. The Right to Deletion
d. The Right to Opt Out
e. The Right to Opt In

Please see the ***CCPA Consumer Rights Guidelines*** for more information on the rights available to consumers under the CCPA.

DRAFT
© Orrick, Herrington & Sutcliffe LLP

orrick

EQUEST PROTOCOL

A REQUEST

y notice provides consumers with a general explanation of their rights under the CCPA
ated methods for submitting such requests, including:

nber: [INSERT NUMBER]

m: [INSERT URL]

RT EMAIL ADDRESS]

is:

MPANY, LLC

N: [PRIVACY LEAD OR PRIVACY TEAM OR APPLICABLE DEPARTMENT]

ERT ADDRESS]

mit requests through other means, such as by contacting their primary contact person
n or by reaching out directly to [APPLICABLE DEPARTMENT OR PERSONNEL] (the
requests should be forwarded to the Privacy Team at [INSERT EMAIL ADDRESS]. All
equests should be stored and retained in accordance with ***Section VII – Record***

yee privacy notice provides employees with a similar explanation of their rights under
ctions to forward all such requests to the employee's HR representative. The HR
forward the request to the Privacy Team at [INSERT EMAIL ADDRESS] and assist
h the analysis and response to the request on a confidential basis.

ll make reasonable efforts to respond to the consumer and acknowledge receipt of his
ever technically reasonable, the acknowledgment should be sent automatically. For
ceived through the Online Platform should send an automatically generated email to
ning receipt. Examples of language for acknowledgment of receipt can be found in the
Request Responses (***Appendix B***).

A REQUEST

uest, the Privacy Team will:

sumer request;

ether the consumer request is manifestly unfounded or excessive;

c. determine whether any exceptions apply to the request; and
d. coordinate with the relevant contacts to take all actions required by the request.

DRAFT
© Orrick, Herrington & Sutcliffe LLP

orrick

CCPA: Critical Compliance Obligations

"Do Not Sell" Obligations – CCPA

- Must **ENABLE OPT-OUT**:
  - of data "sales" of "personal information" to "third parties"
    - This is subject to exceptions
    - Includes enabling opt-outs through a "Do Not Sell My Personal Information" homepage link
- Must **OBTAIN OPT-IN CONSENT**:
  - for the "sale" of a child's PI to a third party
    - Children <13 – affirmative authorization of a parent
    - Children 13-16 (or <16?) – affirmative authorization of a child
  - Applies when a business has "***actual knowledge***" of a child's age; business cannot "***willfully disregard***"

PRACTICE NOTE: consider creating a separate "homepage" dedicated to California residents.

CCPA: Critical Compliance Obligations

- "**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***.
- a business **does not sell** personal information when:
  - A consumer uses or directs the business to intentionally disclose personal information to, or intentionally interact with, a third party (with limitations).
  - The business uses or shares an identifier for the purposes of alerting third parties the consumer has opted out of the sale of personal information.
  - The business uses or shares with a service provider personal information that is necessary to perform a business purposes, but only if:
    - The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.
    - The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.
  - 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 in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115.

CCPA: Critical Compliance Obligations

CCPA – Service Provider v. Certified Partner v. Third Party

Service Provider	• A for-profit entity that processes PI **on behalf of a business** and for a "business purpose"
	• Must have a **written contract** that prohibits retaining, using or disclosing the PI for any purpose (including any commercial purpose) other than:
	  • performing the services specified in the contract for the business; OR
	  • **as otherwise permitted by the CCPA**

Other "Person" (also called a **"Certified Partner"**)	• A **person** that receives PI for a **"business purpose"**
	• Must have a **written contract** that:
	  • prohibits the person from **selling the PI**;
	  • prohibits retaining, using or disclosing the PI for any purpose (including any commercial purpose) other than performing the services specified in the contract;
	  • prohibits retaining, using or disclosing the PI **outside of the direct business relationship** between the person and the business; AND
	  • **includes a certification** that the person understands the above restrictions and will comply with them

Third Party	• An entity or person that **is not a "business"** and **does not receive PI subject to a written contract** with a "**service provider**" or "**certified partner**."

CCPA: Critical Compliance Obligations

Proposed AG Regulations

Now open for public comment, with public hearings December 2-5, 2019.

Highlights include:

- Enhanced disclosures in Privacy Notice and notices at time of collection.
- Provide the online or offline (if applicable) method by which the consumer may submit an opt-out of sales request.
- Enhanced disclosures for financial incentives.
- Notices must comply with accessibility requirements.
- Specific requirements for Consumer Rights Requests and special rules regarding minors under 16.

COMPLIANCE PLAN

LEVERAGING GDPR COMPLIANCE EFFORTS

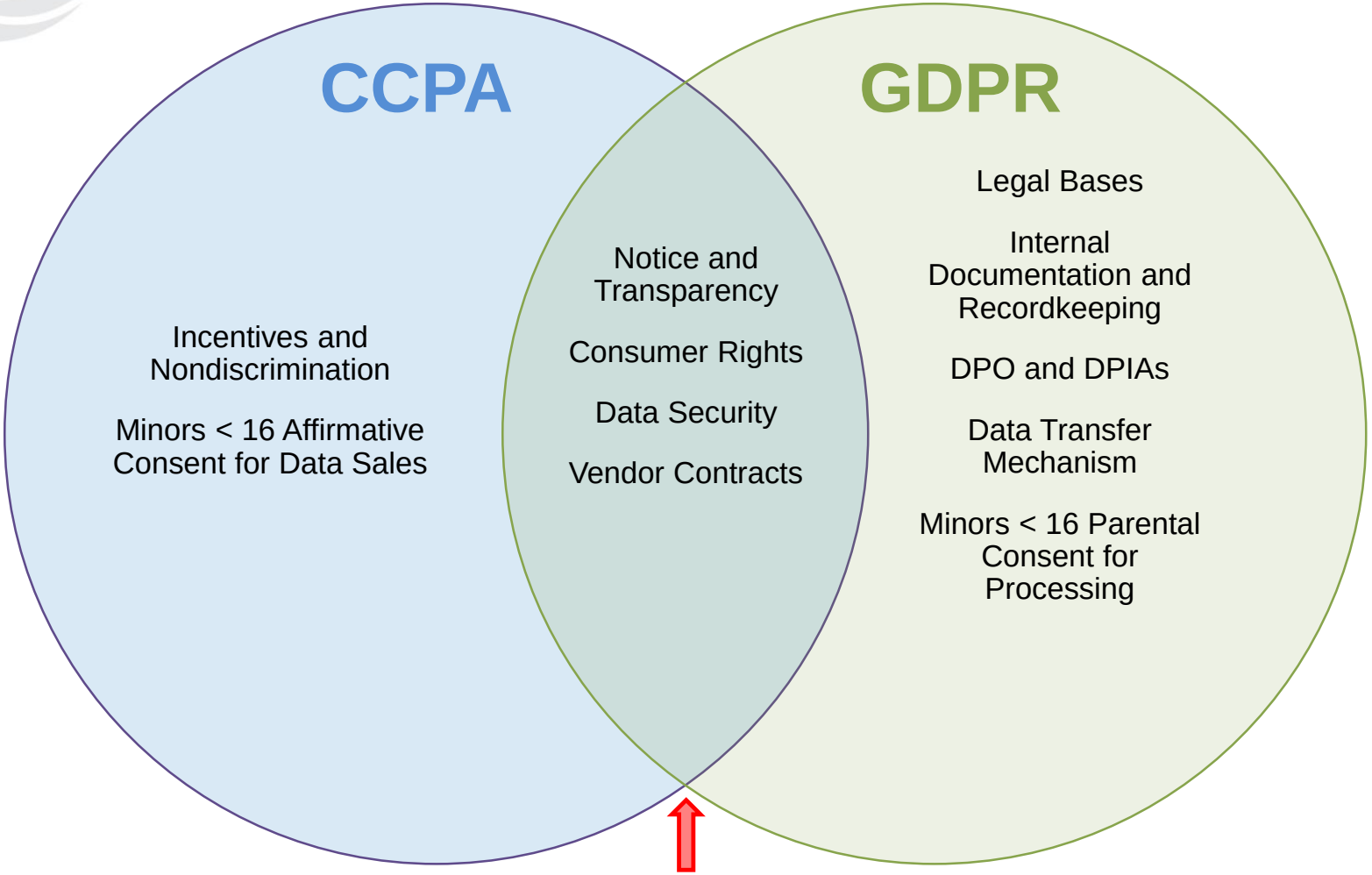
CCPA v. GDPR Covered Entities and Individuals

	Who Must Comply	Who Is Protected
CCPA	For-profit entity **(“business”)**: • Doing business **in CA**, • **Collecting PI** of consumers, • **Controlling** use of **PI**, and • Meeting **revenue / data threshold**	Individuals who are **California** residents **(“consumers”)**.
GDPR	Any person acting as **“controller”** or **“processor”**: • Established **in EU**, • **Offering goods/services in EU**, or • **Monitoring subjects** in EU	All identified or identifiable individuals **(“data subjects”)**. **No citizenship or residency requirement**.

CCPA v. GDPR What is Protected

	In-Scope Information	Exceptions
CCPA	**"Personal Information"** Identifies, **relates to**, describes, is **capable** of being **associated with** or could **reasonably be linked** with a particular **consumer** **or household**.	**Carveouts Include**: • GLBA data • FCRA data • CFIPA data • **Aggregate** data • **Deidentified** data
GDPR	**"Personal Data"** **Relates** to a **data subject**.	**Anonymous info is exempt** and some financial data may be more easily processed through pseudonymisation

CCPA v. GDPR Compliance items



There are significant differences between the CCPA and GDPR, even where the regimes overlap. GDPR-compliant notices, policies and procedures will need to be revised or expanded to align with the CCPA.

Build On Existing Practices

Article 30 Record of Processing

Personal Information Inventory

Privacy Notices

Supplemental Regional Disclosures

Data Subject Request Mechanism and Protocol

Supplemental Consumer Rights Guidelines

Processor, Vendor and Third-Party Management

Service Provider and Certified Partner Handbook

Data Security and Incident Response

Address Risks Relating to CCPA Private Right of Action

Training

Supplemental Training Program

CCPA ENFORCEMENT AND PENALTIES

Enforcement and Penalties

ENFORCEMENT:

- State AGs have broad authority to enforce the laws.
- Each business has a 30-day cure period before the AG may bring an enforcement action.

PENALTIES:

- Injunction; civil penalty of **$2,500** or (if intentional) **$7,500** per violation.

Enforcement and Penalties

Private Right of Action – Data Breaches

- The CCPA provides consumers with a limited private right of action when their:
  - "nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the **duty to implement and maintain reasonable security procedures and practices** appropriate to the nature of the information."
- Violations of this provision are subject to statutory penalties of $100 to $750 per incident.

Enforcement and Penalties

What is "Reasonable" Security?

- **CIS20 Controls (potential California baseline)?**
- **New York DFS Cybersecurity Regulation?**
- **Massachusetts Privacy Regulation?**
- **Common themes:**
  - written information security program
  - governance
  - ongoing risk assessment and management
  - employee training
  - vendor management
  - an incident response plan

PRACTICE NOTE: consider maintaining attorney-client privilege during security assessments.

CIS20 Controls

THE FUTURE OF PRIVACY REGULATIONS AT THE STATE AND FEDERAL LEVELS

Domino Effect?

- California is a leader in state-enacted privacy law.
  - Passed the first state data breach law in 2002.
  - By 2018, all 50 states had similar laws →

    "patchwork" regulation (no federal law)
- CCPA has already likewise become a model for other states:
  - 15 states have since proposed new privacy laws.
  - Expect differing approaches to notice requirements, data portability, consumer rights, etc.
  - CCPA 2.0 is also being considered!
    - California Privacy Rights and Enforcement Act (CPREA)
    - New ballot initiative that Alastair Mactaggart announced for the November 2020 ballot in California

Nevada's Revised Privacy Law (SB 220)

- Establish a **DESIGNATED ADDRESS** for Nevada consumers to submit "do not sell" requests
- **DO NOT SELL** any "covered information" after receiving a "verified" consumer request
  - A "sale" is the exchange of "covered information" for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons
- **RESPOND** to verified requests within 60 days of receipt
- subject to 30-day extension if "reasonably necessary," with notice to the consumer

****Effective: October 1, 2019****

Federal Privacy Law?

- Recent momentum by industry leaders and advocacy groups
- Notable proposals
  - **Data Care Act of 2018**: fiduciary duties for online service providers (care, loyalty, confidentiality)
  - **Privacy Bill of Rights Act**: would require the FTC to promulgate regulations that grant rights to consumers
  - **New Senate Dem Principles – A Framework For Comprehensive Federal Privacy Legislation (November 18, 2019)**
    - Led by Senators Maria Cantwell, Dianne Feinstein, Sherrod Brown, and Patty Murray, Senate Democrats Say New Principles Should Be the Baseline for Any Comprehensive Federal Privacy and Data Security Legislation

Orrick's CCPA and GDPR Readiness Assessment Tools

Orrick's ccpa READINESS ASSESSMENT

Test your company against the provisions under the CCPA

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your CCPA project plan

Visit: orrick.com/Practices/CCPA-Readiness

Orrick's GDPR Readiness Assessment Tool

Stress test your company against the provisions under the GDPR

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your GDPR project plan

QUESTIONS?

orrick

Orrick's Privacy Law Webinar Series

- ✓ Want to learn about the new U.S. privacy laws and the impact they may have on your business?
- ✓ Missed a past webinar?
- ✓ Want to attend our next webinar?

California was the first U.S. state to enact a sweeping new privacy law, the CCPA, which comes into effect in January 2020. Nevada has now enacted a scaled-down version of the CCPA that is now effective.

- ✓ Visit **https://www.orrick.com/Cyber-Privacy-Webinars-Videos**

Orrick's CCPA & GDPR Readiness Assessment Tools

Orrick's ccpa READINESS ASSESSMENT

Test your company against the provisions under the CCPA

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your CCPA project plan

Visit: orrick.com/Practices/CCPA-Readiness

Orrick's GDPR Readiness Assessment Tool

Stress test your company against the provisions under the GDPR

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your GDPR project plan

Visit: orrick.com/Practices/GDPR-Readiness

Trust Anchor

An established point of trust in a cryptographic system from which a process of validation can begin

Blog: blogs.orrick.com/trustanchor
Twitter: @Trust_Anchor

Heather Egan Sussman

Partner
Boston

T 617 880 1830
E hsussman@orrick.com

Honors

- *Chambers USA* 2019
- *The Legal 500 United States* 2019
- *Cybersecurity Docket's* "Incident Response 30″ 2016, 2018, 2019
- *Massachusetts Lawyers Weekly* "Top Women of Law" 2015
- *Best Lawyers* 2018-2019

Education

- J.D., Boston College Law School, 2000
- B.A., University of Massachusetts Dartmouth, 1996, *magna cum laude*

Heather Egan Sussman is Global Co-chair of Orrick's Cyber, Privacy & Data Innovation practice and the leader of Orrick's Boston Office. Her practice focuses on privacy, cybersecurity and information management, and she is ranked by *Chambers USA* and *The Legal 500 United States* as a leader in her field. *Chambers* explains companies turn to Heather because she is "generous with her time and endeavors greatly to educate her clients and understand a given client's risk profile."

Heather's practice focuses on privacy, cybersecurity and information management. Heather routinely guides clients through the existing patchwork of laws impacting privacy and cybersecurity around the globe. In the United States this includes advising on federal and state laws such as CCPA, FCRA, ECPA, TCPA, HIPAA, CAN-SPAM, GLBA, state breach-notification laws, and state data-security laws, as well as existing self-regulatory frameworks, including those covering online advertising and payment-card processing. Outside of the United States, she manages teams of talented counsel around the world to deliver seamless advice for clients that operate across many jurisdictional lines, developing comprehensive privacy and cybersecurity programs that address competing regulatory regimes. Heather drafts online privacy notices for global rollout and implements data-transfer mechanisms for the free flow of data worldwide. She helps clients develop and achieve their data innovation strategies, so they can leverage the incredible value of data and digital technologies in ways that not only meet compliance obligations but also support innovation, deliver value to the business, meet security needs and solidify brand and consumer trust. Heather helps clients reduce the risk of privacy and security incidents and, in the event of a privacy or security breach, she helps companies respond. She guides clients through comprehensive privacy and cybersecurity assessments worldwide. Heather also regularly counsels businesses on how to mitigate risks associated personal data.

Kyle Kessler

Managing Associate
Los Angeles

T 213 612 2437
E kkessler@orrick.com

Education

- Southwestern School of Law, J.D., 2015
- University of Notre Dame, B.A., 2007

For Kyle Kessler, data privacy is where her passion for the law and for cutting-edge programs meets technology. With a background in marketing, public relations and communications, she translates marketing concepts into legal terms. Kyle brings more than a decade of business acumen and experience to her work, and companies turn to her for advice that blends practical business strategies with in-house and outside counsel perspectives.

As a privacy advisor, Kyle is undaunted by the complexity of state, federal and international data privacy and security requirements. She evaluates and advises clients on data collection, storage, use and transfer, as well as breach laws and regulations. Kyle advises on the Children's Online Privacy Protection Act (COPPA), California Online Privacy Protection Act (CalOPPA), the new California Consumer Privacy Act of 2018 (CCPA) and on the EU General Data Protection Regulation (GDPR) from a U.S. perspective.

Kyle also advises and collaborates with her clients on general consumer protection and marketing/advertising matters. For instance, she regularly reviews marketing assets to ensure legal compliance across all channels. She also advises on unfair and deceptive trade practices, compliance issues relating to the Federal Trade Commission and the National Advertising Division (NAD) of the Better Business Bureau, the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA), as well as on other state and federal laws.

Before joining Orrick, Kyle was an in-house attorney at one of the *Forbes* 100 Largest Private Companies, and she has experience in the retail industry working in, among other things, data protection, incident response, unfair and deceptive trade practices and consumer-protection matters.

Kyle is an active member of the International Association of Privacy Professionals (IAPP), the LGBT Bar Association of Los Angeles and Women in Security and Privacy (WISP).

orrick