CCPA & GDPR:

Overlaps and Gaps to Consider in Your Harmonized Privacy Program

Doug Boykin, CIPP/E, CIPM, Privacy Engineer, OneTrust

OneTrust

Privacy Management Software

Agenda

1 | CCPA vs. GDPR: Scope

2 | CCPA vs. GDPR: Individual Rights

3 | CCPA vs. GDPR: Vendor Risk

2019 – The Year for Global Privacy

OneTrust
Privacy Management Software

GDPR: The Global Privacy Catalyst

The EU General Data Protection Regulation changed the {privacy} world.

- **Changed the business & consumer outlook on privacy**
- **Extraterritorial scope forced companies to implement privacy into business**
- **Changed the way companies interact with customers, employees and vendors**
- **Sparked development of new privacy laws around the globe**

OneTrust
Privacy Management Software

Privacy laws are here… and growing

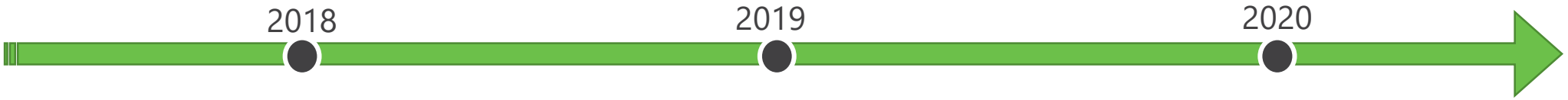
European Union GDPR:
May 2018

Colorado Data Privacy Act
September 2018

Vermont Act 171
January 2019

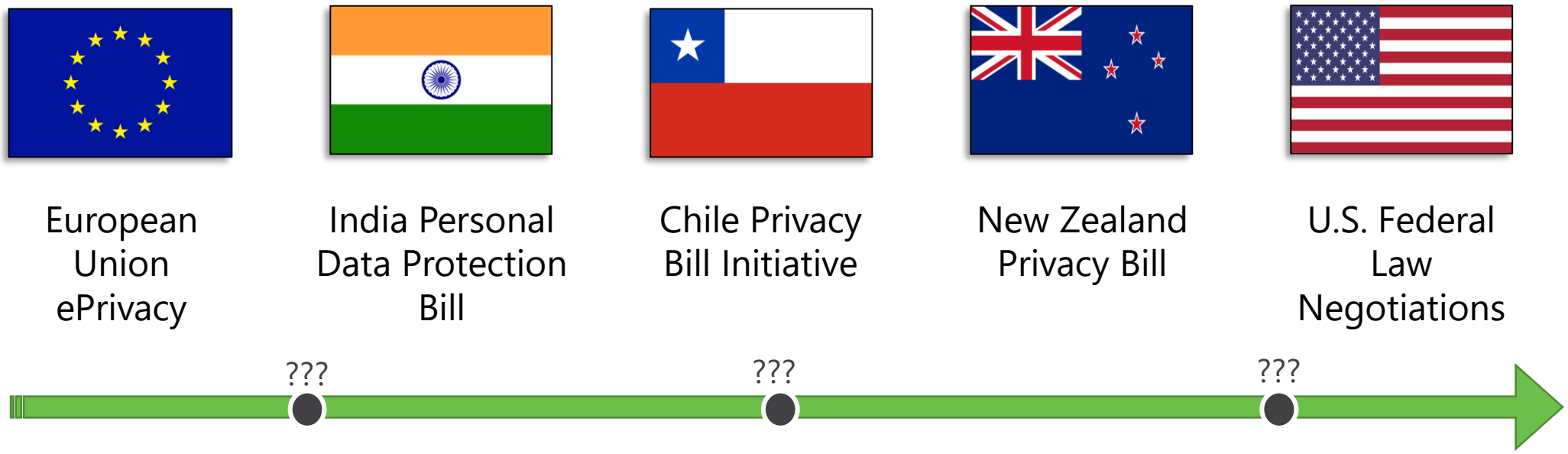
California Consumer Privacy Act
January 2020

Brazil LGPD
February 2020



OneTrust
Privacy Management Software

Other laws still being negotiated



Scope: Who is Covered?

CCPA vs. GDPR Match-up

OneTrust

Privacy Management Software

CCPA Application

Business

- **For profit** organization (sole proprietorship, partnership, corporation, LLC, association, or other legal entity)
- That **collects consumer personal information** (online or offline)
- Determines the purpose and means of the **processing** (GDPR equivalent of controller)
- Does **business in the State of California**

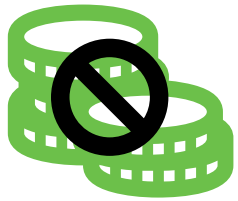
Meets One or More

- Annual gross revenues in excess of **$25 million**
- Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, the personal information of **50,000** or more consumers, households, or devices.
- Derives **50 percent** or more of its annual revenues from selling consumers' personal information.

GDPR Application

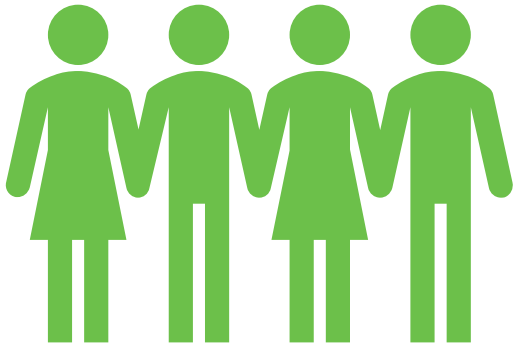
Processor

- Processing of **personal data of controllers** established in the EU, or
- Processing of **personal data of EU residents** by non-EU controller/processor, where it relates to:
  - offering of goods or services, or
  - monitoring of EU residents' behaviour (as so far as the behaviour takes place in the EU) ; or
- Processing of personal data by a controller not established in the EU, but in a place where **Member State law applies by virtue of public international law**.
  - E.g. an EU Member State embassy



If either of these conditions are met, GDPR applies – regardless size, revenues, amount of personal data processed, etc.

Covered Individuals



Consumers

- Natural person who is a California Resident

Data Subjects

- Identified or Identifiable natural person
- NOT necessarily EU resident – in cases of EU-established controllers

Bottom Line Compliance Requirements

Conduct an assessment when:

- ✓ Only GDPR applies
- ✓ Only CCPA applies
- ✓ BOTH apply

Establish a system where it is immediately clear which laws apply to which sets of personal data

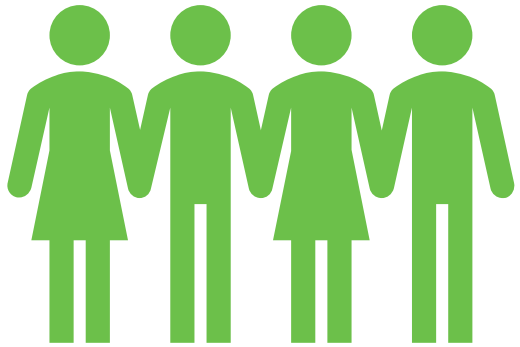
What Information is Covered?

CCPA vs. GDPR Match-up

OneTrust

Privacy Management Software

Covered Information



Personal Information

Information that could be reasonably linked, directly or indirectly, with a particular CA consumer or household.

Personal Data

- Any information relating to an identified or identifiable natural person ('data subject')
- EU residents or not

CCPA Personal Information is BROADER than the GDPR

Person or Household

Real name

Postal Address

Unique personal identifier

Alias

Online identifier

Social security number

Passport number

Drivers license number

Email address

Account name

Internet or other electronic activity

Browsing history

Search history

Consumer's interaction with web, app or ad

Inferences drawn from any of the information identified to create a profile

Psychological trends

Intelligence

Preferences

Behavior

Aptitudes

Predispositions

Abilities

Characteristics

Attitude

OneTrust

Privacy Management Software

Bottom Line Compliance Requirements

- ✓Update personal information mapping so you can track **broader set of data** required by the CCPA
- ✓Update Data Mapping Records to include the **wider scope** of CCPA Personal Information

Broader definition → more vendors processing personal information → wider reach of individuals' rights (more systems concerned)

Individuals' Rights

CCPA vs. GDPR Match-up

OneTrust

Privacy Management Software

Three
Consumer Rights
under California Consumer Protection Act

Right of Information

Right to Opt-Out

Right of Deletion

OneTrust
Privacy Management Software

Nine
Data Subject Rights under the GDPR

Right to be informed *Article 13, 14* *Recitals 60-62*	**Right of Access by the Data Subject** *Article 15* *Recitals 63 & 64*	**Right to Rectification** *Article 16, 19*
Right to Erasure *Article 17, 19* *Recitals 65 & 66*	**Right to Restriction of Processing** *Article 18, 19* *Recital 67*	**Right to Data Portability** *Article 20* *Recital 68*
Right to Object *Article 21* *Recital 69 & 70*	**Automated Individual Decision Making** *Article 22* *Recital 71 & 72*	**Right to Withdraw Consent** *Article 7* *Recital 32, 33, 41, 43*

Individual Rights Matchup

CCPA	GDPR
Business obligation to inform	Right to be Informed
Right to request information	Right of Access
-	Right to Rectification
Right of Deletion	Right to Erasure
-	Right to Restriction of Processing
Right to request information *(partial)*	Right to Data Portability
Right to Opt-Out	Right to Object
-	Automated Individual Decision Making
Right to Opt-Out	Right to Withdraw Consent

OneTrust
Privacy Management Software

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Obligation to Inform vs. Right to be Informed

CCPA

GDPR

Business Obligation to Inform

- **Categories** and **purposes** of personal information collected
- Right consumers have to ask for **deletion** of their personal information
- If PI is sold, customers have **right to opt-out** of sale. This must be disclosed in its online privacy policy

Right to be Informed

- Identity and **contact details of controller** and representatives
- The contact details of the **DPO**
- Purposes and **legal basis for processing**. If applicable, what legitimate interests are pursued
- **Recipients** or categories of recipients of the personal data
- Any **cross-border data transfer** involved
- The **data retention** for the personal data collected

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Right to Request Information vs Right of Access

CCPA

GDPR

Right to Request Information

- Right to obtain **confirmation**, **access** and **information** about processing, regardless of how it was collected
- Should not **adversely affect** the rights of others
- Initial copy is **free**, reasonable fee for additional copies
- Must provide **electronic form**
- Can request **specific subset** if data amount is large

Right of Access

- Right to request information about **categories and pieces** of personal information collected. Trigger:
  - 1) If business collections PI and
  - 2) If business sells/discloses PI
- Other requirements
  - Must be “verifiable consumer request”
  - **Free**, up to once per year
  - Mail or electronic

OneTrust
Privacy Management Software

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Right of Deletion vs. Right to Erasure

CCPA 

Right of Deletion

- May request deletion of **any PI** collected by the business
- **Nine exceptions**, including:
  - Comply with legal obligation
  - Security purposes
  - Complete transaction that PI was collected for
  - Engage is research or public interest (same as GDPR)

GDPR 

Right to Erasure

- Can request right to erasure when:
  - Data no longer necessary for the purpose
  - Withdraw consent and no other legal basis of processing
  - Successful exercise of right to object
  - Unlawful processing
  - Comply with EU or Member State law
- Exceptions include:
  - Freedom of expression/information
  - Required by law
  - Research or public interest
  - Defending legal claims

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Right of Request Information vs. Right to Data Portability

CCPA

GDPR

Right to Request Information *(partial)*

- **Not as comprehensive** as the GDPR requirements
- Format requirement regarding Businesses' compliance with the Request for Information
- Information transmitted in a **portable and readily useable format** that allows the consumer to **transfer personal information** to another entity

Right to Data Portability

- Right to receive personal data in a **structured, commonly used and machine-readable format**
- Right to have the personal data **transmitted** to another controller, **where technically feasible**

OneTrust
Privacy Management Software

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Right to Opt-Out vs. Right to Object

CCPA

GDPR

Right to Opt-Out

- Consumer can request at any time a business to stop selling PI to third party
- Business must wait 12 months to ask consumer to opt back into sale of PI
- Includes cookies, advertising IDs, list rentals, etc.
- Must have link on homepage that says "**Do not sell my personal information**"

Right to Object

- Right to object to processing "on grounds relating to his or her particular situation, at any time"
- Scope includes processing based on **legitimate interests**, based on performance of task in **public interest**/exercise of official authority and **research purposes**
- No exceptions for direct marketing

OneTrust
Privacy Management Software

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Right to Opt-Out vs. Right to Withdraw Consent

CCPA

GDPR

Right to Opt-Out

- Consumer can request at any time a business to stop selling PI to third party
- Business must wait 12 months to ask consumer to opt back into sale of PI
- Includes cookies, advertising IDs, list rentals, etc.
- Must have link on homepage that says "**Do not sell my personal information**"

Right to Withdraw Consent

- Right to withdraw consent **at any time** when basis of process is based on consent
- Must be **as easy to withdraw** consent as it is to give consent

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Vendor Management

CCPA vs. GDPR Match-up

OneTrust

Privacy Management Software

Terminology & Concepts

EU GDPR

Calif. CPA

Controller	Business
Processor	Information Recipient

Terminology & Concepts

EU GDPR

Calif. CPA

Controller

Business

Processor

Information Recipient

AKA **VENDORS**

GDPR Context

Controllers are responsible for not only their own data protection measures, but also those of their processors.

Responsibility of the Controller
Article 24
Recitals 74-77, 83

Processor
Article 28
Recital 81

Processing under a Controller or Processor
Article 29

Transfer Subject to Appropriate Safeguards
Chapter V (Articles 44-50),
Recitals 101-116

CCPA Context

Businesses have to keep track of their vendors & whom they sell the personal information

Consumers' Direct Right of Action
CCPA – 1798.150(a)

California Attorney Generals Office

Information Recipient Liability
CCPA – 1798.140(w)(2)(B)

Compliance with Consumers' rights to information, deletion & opt-out

GDPR Responsibilities of Controllers & Processors

Scope

All processing of personal data by a processor as **instructed** by a controller

Other Requirements

- Take into account nature of processing and risks (**likelihood and severity**)
- **Demonstrate** compliance
- Implementation of data **protection** policies

Article. 24, 28, 29

Summary

- Controllers shall only use processors providing **sufficient guarantees** to implement appropriate technical and organisational measures
- Processors shall not engage another processor without **prior specific or general written authorisation** of the controller.
- Processing by a processor shall be governed by a **contract**
- Processors shall engage other processors only under the **same data protection obligations**
- May not process personal data **except on instructions** from the controller

CCPA Responsibilities of Businesses & Information Recipients

Scope

- All processing of personal data by a processor as **instructed** by a controller
- **Personal data** definition is **wider** than under the GDPR.

Other Requirements

- **Prevent** and sustain personal data breaches – maintain breach policy and process to communicate with vendors.
- Maintain processing records up-to-date to comply with rights of consumers.

Article. 24, 28, 29

Summary

- Businesses should conduct data & system inventory and **review/broaden their data processing records and data processing agreements** (due to broader definition of personal data).
- Businesses must ensure that they can alert 3rd parties to stop processing personal information in case of deletion and opt-out from selling of information.
- Businesses must beware of buying information from a reseller – it shouldn't be used unless there is express consent from the individual.
- Processing by an information recipient shall be governed by **a written contract**
- Information recipients **cannot sell** the personal information
- Information recipients cannot retain, use or disclose the personal information for any other than the contractual purpose.

GDPR: Required Contractual Terms – Article 28(3)

1. Subject-Matter and Duration of Processing
2. Nature and Purpose of Processing
3. Types of Personal Data and Categories of Data subjects
4. Obligations and Rights of the Controller
5. Process only on Written Instructions of Controller
6. Ensure Confidentiality
7. Implement Appropriate Technical and Organisational Measures
8. Obtain Controller's Consent to Engage Sub-Processors
9. Assist Controller with GDPR Obligations
10. Delete or Return Personal Data
11. Demonstrate Compliance (Accountability
12. Allow for Audits by Controller

12 Requirements

OneTrust
Privacy Management Software

CCPA: Required Contractual Terms – Section 1798.140(w)(2)

6

Requirements

1. Recipients Prohibition from Selling Personal Data
2. Recipients Prohibition From Retaining, Using or Disclosing the Information for Any Purposes Other Than for the Specific Purpose of Performing the Services Specified in the Contract
3. Recipients Prohibition from Retaining, Using, or Disclosing the Information Outside of the Direct Business Relationship with the Business
4. Ensure Confidentiality
5. Specification of the Purpose of Performing the Services
6. Recipients Certification of Understanding the Restrictions and to Comply with Them

How to Comply with Both?

Look for **holistic approach**: instead of aiming to address the legislations individually, try to reconcile them within one global privacy management framework.

Combine GDPR's **more detailed requirements** with CCPA's specific requirements & modalities. Conduct a GAP analysis and based on it incorporate the missing operational and technical solutions to comply with CCPA AND the GDPR.

Build a Global Privacy Program or Strategy

Build a Global Privacy Program to work across many regulations.

- **Scalable and individualized to your company's needs, budget and size**
- **Not necessarily in-house – can be outsourced or use technology**
- **Software tools can be used to facilitate the research**
- **Build on the compliance work you have already accomplished**

OneTrust
Privacy Management Software

OneTrust Privacy Management Software Platform

Privacy Program Management

Assessment Automation
PIA | DPIA | PbD | InfoSec

Data Mapping Automation
Discovery, ROPA, Inventory

PbD Automation
Automated PbD Checklists

Global Readiness Tracker
Planning & Exec Dashboard

Marketing Consent, Preferences, & Subject Rights

Cookie Compliance
Web Scan & Consent

Universal Consent
Central Records of Consent

Preference Center
End User Self-Service

Data Subject Rights Portal
End to End Automation

Incident and Breach Response

Incident Intake
Maintain Central Register

Global Breach Law Engine
Trigger Requirements

Risk Assessment
Analyse Risk and Harms

Notification and Reporting
Track Obligations

Vendor Risk Management

Self-Service Assessments
CSA, SIG, VSA, Custom

Compliance Scanning
Policy and Cert Auto-Detect

4th Party Management
Detect Sub-Processors

Contract & DPA
Track Key Terms

PrivacyConnect

CCPA & GDPR Community by OneTrust

100+ Events Across 80+ Global Cities

Free CCPA & GDPR Workshops
5 CPE Credit Hours
OneTrust Certification Program in Select Cities

Monthly Privacy Webinar Series
Hosted by Top Tier Law Firms & Consultancies

Local Community Chapters
Latest Privacy News & Events in your City

Amsterdam	Rome	San Francisco	Philadelphia
Dublin	Brussels	Chicago	Minneapolis
London	Prague	New York	Detroit
Paris	Manchester	Washington DC	Portland
Oslo	Tel Aviv	Atlanta	Kansas City
Stockholm	Lisbon	Houston	Raleigh
Helsinki	Budapest	Toronto	St. Louis
Belfast	Stuttgart	Denver	San Diego
Geneva	Berlin	Phoenix	Austin
Zurich	Bucharest	Boston	Cleveland
Warsaw	Barcelona	Charlotte	Hong Kong
Vienna	Frankfurt	Seattle	Sydney
Milan	Dubai	Columbus	Melbourne
Madrid	Doha	Los Angeles	Singapore
Athens	Abu Dhabi	Indianapolis	Seoul

”This was the best GDPR-focused conference I have ever been to. This was not just a high-level look into requirements, but an in-depth educational experience for myself and my colleagues.”

RSVP TODAY

PrivacyConnect.com

Learn More

ON-DEMAND WEBINARS

DOWNLOAD WHITEPAPERS

ANALYST RESEARCH

www.onetrust.com/resources

OneTrust
Privacy Management Software