

March 5, 2019

GDPR and New California Privacy Law Update

Andrew Clearwater, OneTrust

Daniel Gottlieb, McDermott Will & Emery

Kate Heinzelman, Sidley Austin

SIDLEY

Kate Heinzelman

+1 202 736 8416

kheinzelman@sidley.com

OneTrust

Andrew Clearwater

+1 207-766-6654

aclearwater@onetrust.com

**McDermott
Will & Emery**

Daniel F. Gottlieb

+1 312 984 6471

dgottlieb@mwe.com

Daniel F. Gottlieb



**Daniel F. Gottlieb,
Partner, Chicago**

Tel: +1 312 984 6471

Mobile: +1 312 282 3305

Email: dgottlieb@mwe.com

Education

Northwestern University
School of Law, JD, cum
laude, 1999

University of Michigan,
BA, with highest
distinction, 1994

Daniel F. Gottlieb counsels a wide range of health care industry clients, including health care providers, colleges and universities, health information technology (IT) vendors and life sciences companies, regarding privacy and data protection matters, health IT acquisitions, and development and deployment of digital health solutions. In particular, Daniel has deep experience advising US health sector and academic clients regarding the applicability and implementation of GDPR, HIPAA, FERPA, TCPA, CAN-SPAM and other US and international data protection laws.

Daniel is a co-leader of the McDermott's Global Privacy and Cybersecurity Practice.

Kate Heinzelman



Counsel

*Privacy and
Cybersecurity Practice*

Washington, D.C.

+1 202 736 8416

kheinzelman@sidley.com

KATE HEINZELMAN is a member of Sidley's Privacy and Cybersecurity, Healthcare, and Commercial Litigation groups. Her practice focuses on investigations, counseling, and litigation on technology, privacy, and regulatory matters, particularly in the healthcare and life sciences sectors. Kate brings to her practice substantial experience working with a broad range of government agencies and federal programs across the national security, healthcare, and energy and environmental fields. Before joining Sidley, Kate was Deputy General Counsel at the Department of Health & Human Services. While there, she oversaw a variety of projects and agencies, including components of the Centers for Medicare & Medicaid Services, the Public Health Division, the Office for Civil Rights and the Office of the National Coordinator. Before joining the Department of Health & Human Services, Kate worked in the White House Counsel's Office as Special Assistant and Associate Counsel to President Barack Obama. In this role, she advised the President and his Administration on crisis response, national security, privacy and technology, energy, and environmental matters. Kate also served as Counsel to the Assistant Attorney General for National Security at the Department of Justice, where she provided counsel to departmental leadership on national security operational and litigation matters as part of the division's front office.

Kate served as a law clerk to Chief Justice John G. Roberts, Jr. on the U.S. Supreme Court.

Publications

- Co-Author, "Carpenter v. United States: A Revolution in Fourth Amendment Jurisprudence?," Pratt's Privacy & Cybersecurity Law Report Volume: 4 Number: 9 (November/December 2018).
- Co-Author, "Federal Judge Invalidates U.S. Health and Human Services' Approval of Changes to Kentucky Medicaid Program," Sidley Healthcare Update (July 5, 2018).
- "After LabMD, questions remain for the healthcare sector," Digital Health Legal, Volume: 5 Issue: 7 (July 2018).
- "Life Sciences and the AI Revolution," Chambers and Partners, (June 2018).
- "What Congress's First Steps Into AI Legislation Portend," Bloomberg Law (May 8, 2018).
- "Should the government regulate artificial intelligence? It already is," The Hill (February 26, 2018).
- "When and How Cos. Should Address Cyber Legal Compliance," Law360 (October 24, 2017).

Kate received her J.D. from Yale Law School and her B.A. from Yale University.

Full biography: <https://www.sidley.com/en/people/h/heinzelman-kate>

ANDREW CLEARWATER



Director of Privacy

CIPP/US

+1 207-766-6654

aclearwater@onetrust.com

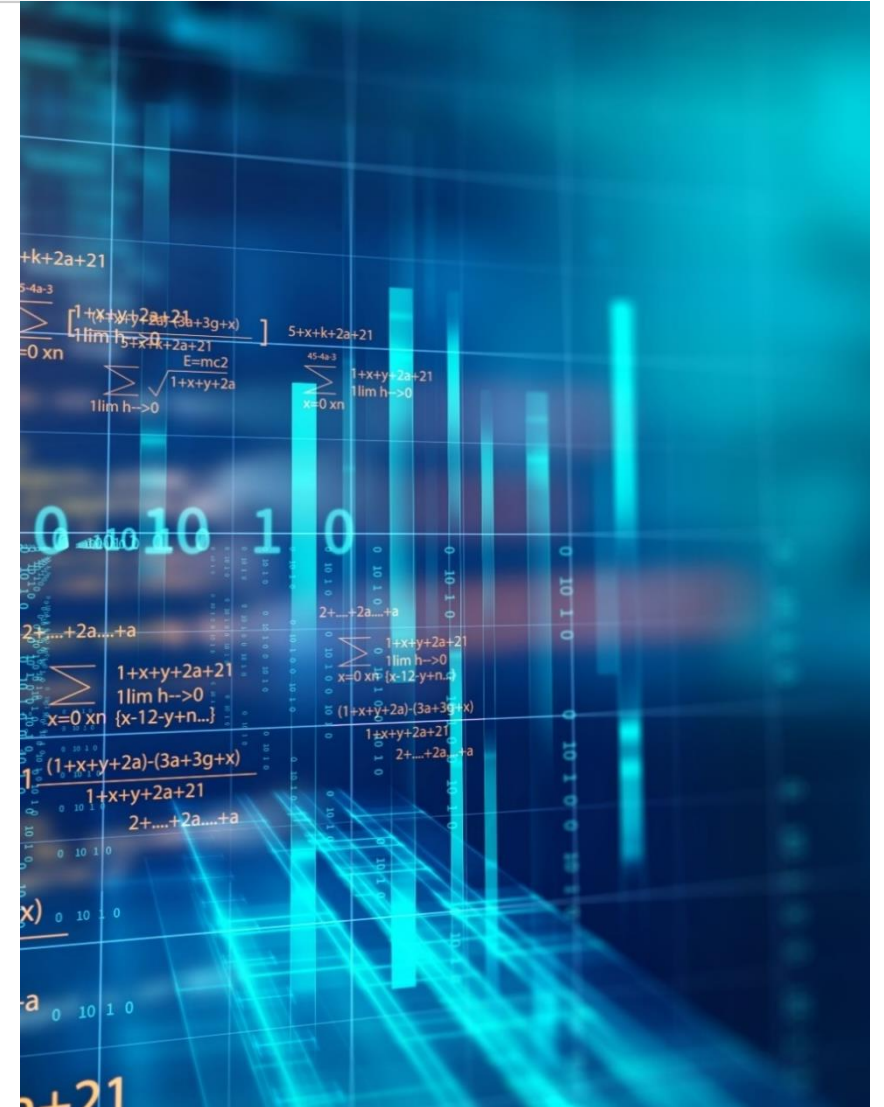
Andrew Clearwater serves as Director of Privacy at OneTrust. Mr. Clearwater is a Certified Information Privacy Professional (CIPP/US), holds an LLM in Global Law and Technology and is a licensed attorney. In his role as Director of Privacy, Clearwater provides counsel, leadership, and guidance on data protection. He is also responsible for providing public policy analysis in the areas of privacy, data security, information policy, and technology transactions.

Before joining OneTrust, Mr. Clearwater was the Privacy Officer for RxAnte. Clearwater also held privacy roles at the Future of Privacy Forum, as well as the Network Advertising Initiative. In addition, he made contributions to the NTIA mobile application transparency discussion, helped launch a privacy seal program for companies that use consumer energy data, participated as a member of the W3C Tracking Protection Working Group, and taught as an adjunct professor of privacy and technology law at the University of Maine.

Clearwater has been published in several of the top industry publications on privacy, including the IAPP Privacy Advisor and CPO Magazine. He is a frequent speaker at leading industry events, including the IAPP Global Privacy Summit, The International Privacy + Security Forum and SecTor.

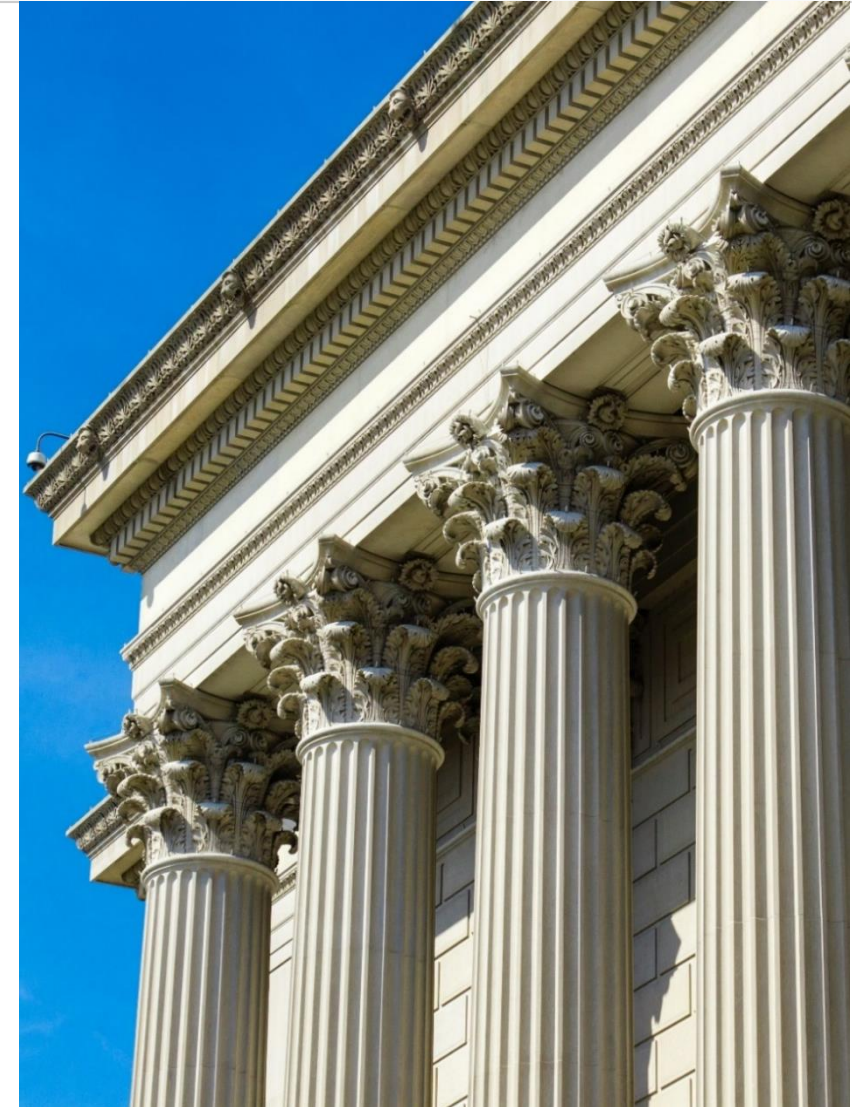
Agenda

- 1 How has the privacy landscape changed in the last year?
- 2 GDPR and CCPA Overview
- 3 Comparing the CCPA and the GDPR
- 4 10 Practical Preparation Steps
- 5 Regulatory Enforcement and Civil Litigation



Agenda

- 1 How has the privacy landscape changed in the last year?
- 2 GDPR and CCPA Overview
- 3 Comparing the CCPA and the GDPR
- 4 10 Practical Preparation Steps
- 5 Regulatory Enforcement and Civil Litigation



GDPR: The Global Privacy Catalyst



- **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**

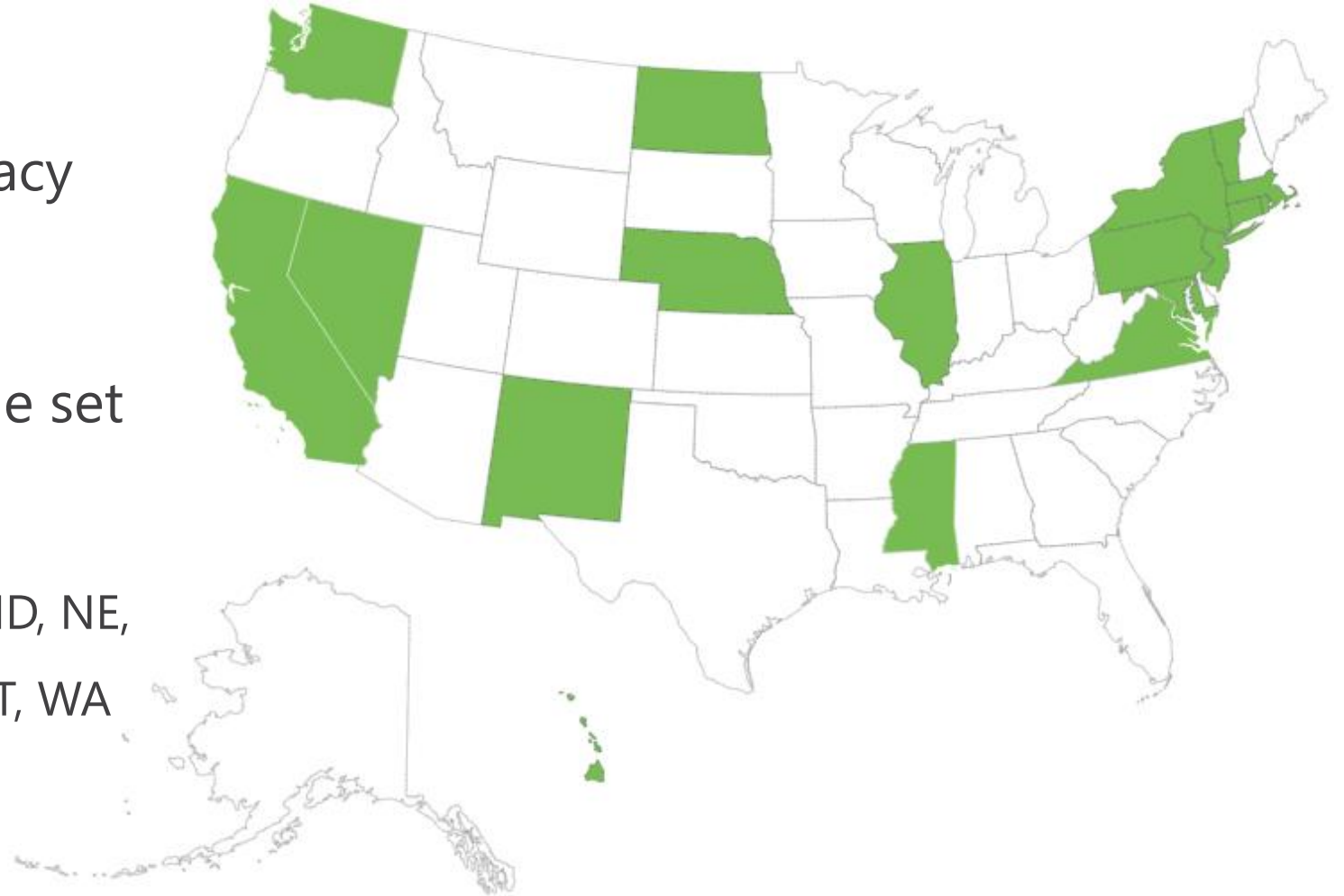
Global Laws - Summary



visit onetrust.com for whitepapers and additional resources on these and other global privacy laws

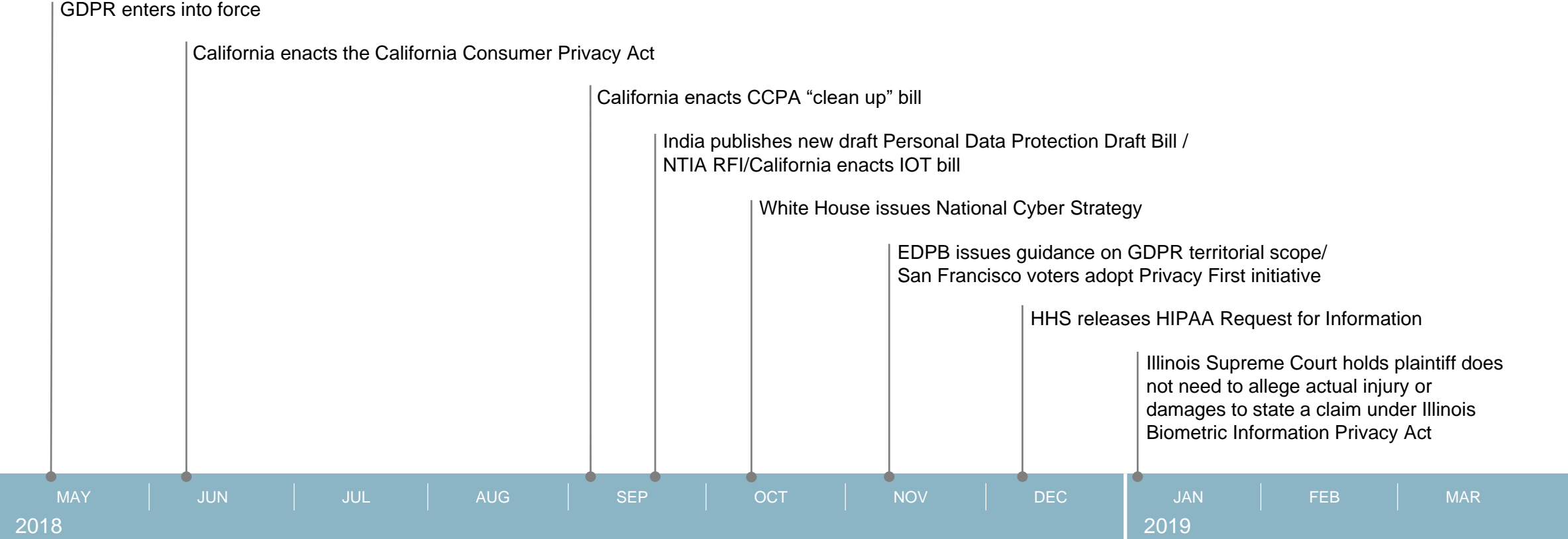
U.S. Federal Privacy Law

- Countless proposals for comprehensive federal privacy legislation
- States following the example set by California (CCPA)
 - CA, CT, HI, IL, MA, MD, MS, ND, NE, NJ, NM, NV, NY, PA, RI, VA, VT, WA



Backdrop

High-profile data breaches, privacy incidents, and foreign privacy laws have focused global attention on these issues



Will Congress enact preempting legislation?

Privacy at a Crossroads

The New York Times

Internet Users in China Expect to Be Tracked. Now, They Want Privacy.

Ant Financial, an affiliate of the e-commerce giant Alibaba Group, has apologized for automatically enrolling users in a program that tracks personal relationships and behavior patterns. *Imaginechina*, via Associated Press

The New York Times

Just Don't Call It Privacy

Amazon, Google and Twitter executives are heading to Congress. Should legislators give consumers control over the data companies have on them?

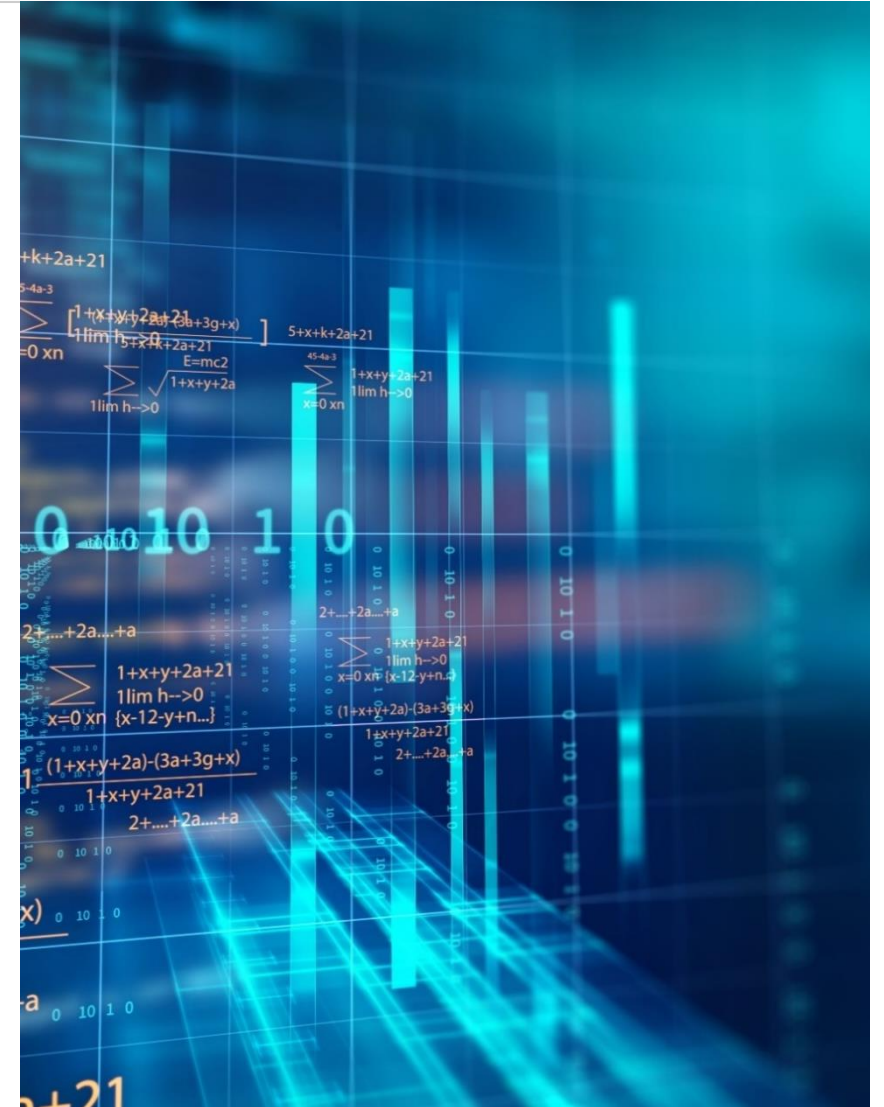
The Washington Post

Our privacy regime is broken. Congress needs to create new norms for a digital age.

By Editorial Board
January 5

Agenda

- 1 How has the privacy landscape changed in the last year?
- 2 **GDPR and CCPA Overview**
- 3 Comparing the CCPA and the GDPR
- 4 10 Practical Preparation Steps
- 5 Regulatory Enforcement and Civil Litigation



What is GDPR?

- GDPR is broad personal data privacy, security and breach notification law
- GDPR applies to US organizations that offer goods or services or monitor individuals located in European Union (EU) even if they lack physical presence in EU
- GDPR applies to all individually identifiable information (Personal Data), not just HIPAA protected health information (PHI) or sensitive categories of information
- GDPR provides more expansive individual rights than HIPAA, e.g., right to deletion of Personal Data or data portability unless exception applies
- Unlike HIPAA, individuals have private cause of action and class action rights
- Regulators may assess penalties (up to greater of 20M EUR and 4% of revenues)

Key GDPR Requirements

- Ensure there is a “**legal basis**” (*i.e.*, an exception to general rule of privacy) for processing Personal Data
 - When relying on consent as the legal basis, ensure consent is freely given, specific, informed and unambiguous
- Provide clear and transparent **notice** to data subjects about how Personal Data is used, collected, disclosed, and otherwise processed
- Perform privacy impact assessments for high risk activities
- Demonstrate accountability, *e.g.*, by maintaining records of Personal Data processing activities

Key GDPR Requirements (cont'd)

- Honor **individual privacy rights** (erasure, restriction, portability, objection, access, and rectification) to data subjects related to the Personal Data maintained about them (except in certain circumstances)
- Appoint processors (and subprocessors) who can guarantee compliance with the GDPR and put in place written data processing agreements with them
- Appoint a Data Protection Officer and/or an EU Representative if certain criteria are met
- Notify the data protection authority (DPA) in the event of a Personal Data breach involving **risk** to individual and notify individual if **high risk**

What Is the CCPA?



Increased salience of commercial data practices: high-profile breaches, government access debates, etc., etc., etc.



Meanwhile, the EU General Data Protection Regulation enters into force



Consumer privacy initiative qualifies for November ballot



Difficulty in amending laws passed by initiative leads to push for legislative replacement



Legislature enacts CCPA and ballot initiative is withdrawn; original legislation is amended

What Is the CCPA?

The CCPA is a far-reaching data protection and privacy regime that grants consumers new rights over data collected about them and creates new mechanisms for enforcing those rights.



Adopted in 2018 and will come into force in 2020



Grants consumers rights to, among other things, access, delete or stop the sale to third parties of data collected about them



CCPA applies to certain for-profit entities doing business in California and defines personal information very broadly



Private cause of action for data breaches with damages permitted without proof of harm (although companies are given a chance to cure violations)



Broad privacy policy disclosure requirements



California Attorney General authorized to enforce provisions with statutory fines of up to \$7,500 per violation

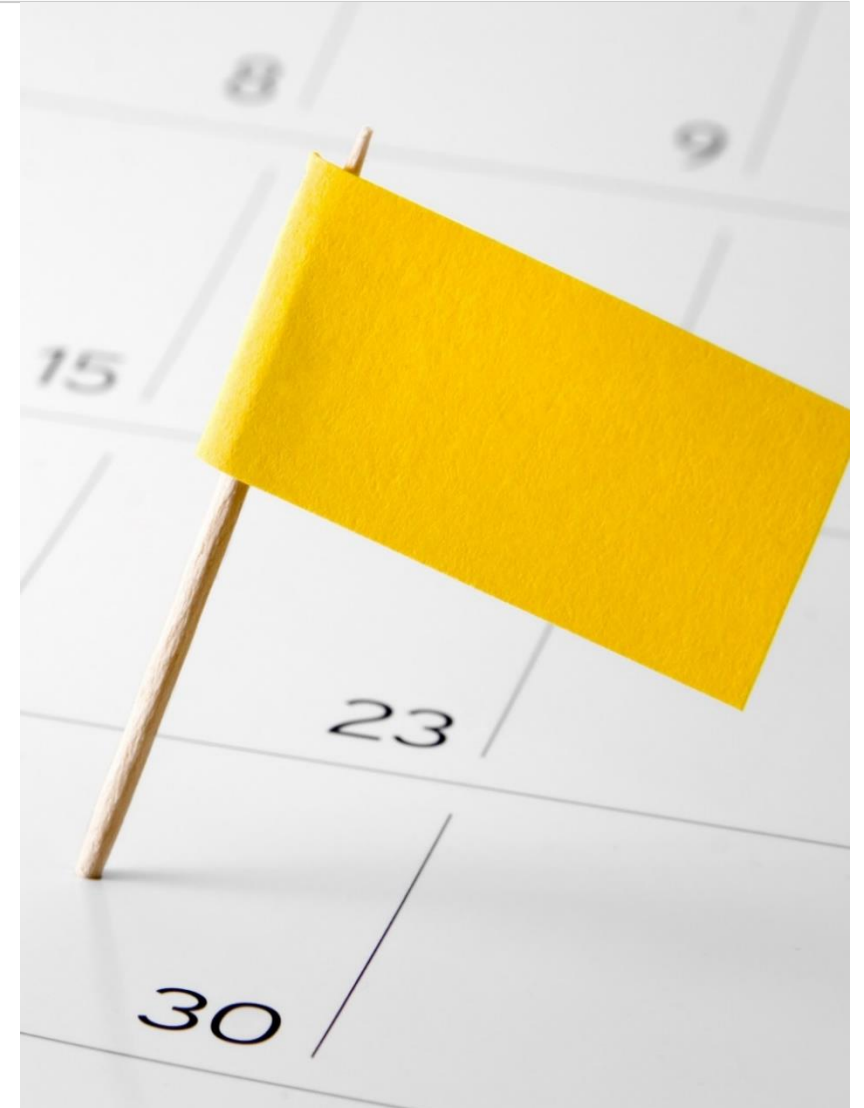
September 2018 “Clean-Up” Amendments – Effective Date

Delayed deadline for regulations and enforcement

- AG has until July 1, 2020, to issue regulations
- Enforcement cannot begin until July 1, 2020, or six months after final regulations are published

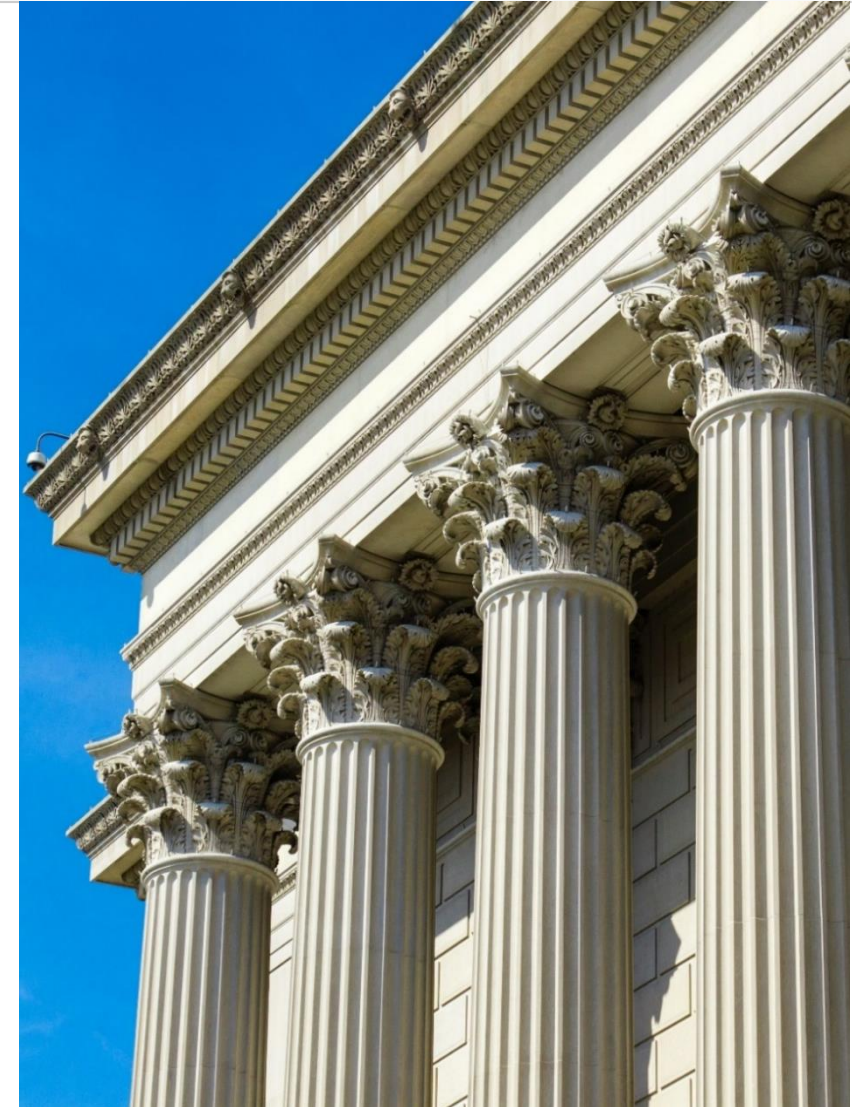
Compliance deadline remains the same, which means

- Businesses must invest in compliance programs without regulatory guidance.
- Could be immediately subject to enforcement actions once regulations are published



Agenda

- 1 How has the privacy landscape changed in the last year?
- 2 GDPR and CCPA Overview
- 3 Comparing the CCPA and the GDPR**
- 4 10 Practical Preparation Steps
- 5 Regulatory Enforcement and Civil Litigation



Territorial Scope

GDPR

- GDPR applies to US Company that is a controller or processor **established in the EU in the context of the activities of the EU establishment**, whether or not processing takes place in the EU
- GDPR applies to entities not established in the EU if the processing is related to the
 - **Offering of goods or services** to individuals in the EU
 - **Monitoring the behavior** of individuals in the EU

CCPA

- CCPA applies to a for profit entity that “**does business in California**”
 - California Franchise Board provides guidance on phrase for other CA laws
- CCPA does **not** restrict ability to collect or sell a consumer’s personal information if
 - the business collected PI while the consumer was outside of California,
 - no part of the sale of the consumer’s PI occurred in California, *and*
 - no PI collected while the consumer was in California is sold.

EDPB Guidance on Territorial Scope

- European Data Protection Board (EDPB), which provides authoritative guidance on GDPR, issued guidance on territorial scope of GDPR in November 2018
- EDPB advises that processing by a company outside EU may be “inextricably linked” to the company’s EU establishment and thereby subject to GDPR
- Example 9: “A U.S. citizen is traveling through Europe during his holidays. While in Europe, he downloads and uses a news app that is offered by a U.S. company. The app is exclusively directed at the U.S. market. The collection of the U.S. tourist’s personal data via the app by the U.S. company **is not subject to GDPR.**”

Covered Businesses (CCPA)



Scope: Applies to “businesses ... do[ing] business in the State of California” that satisfy one of the following (or entities “that control[] or [are] controlled by” such businesses)

- Have annual gross revenues in excess of \$25 million;
- annually buy, sell, receive or share for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers or devices; or
- Derive 50 percent or more of annual revenues from selling consumers’ personal information

Covered Businesses (CCPA) (Cont'd)



CCPA distinguishes between “service providers” and “third parties.”

- A “service provider” is a for-profit entity “to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract,” provided that the contract limits the retention, use, and disclosure of the data.
- A “third party” is an entity that is not a business or an entity to whom the business discloses information pursuant to a contract.
- Implications (among other things):
 - Different liability rules
 - Third parties may not sell personal information that has been sold to them unless the consumer receives explicit notice and opportunity to opt out.

GDPR – Controllers and Processors



Controller

Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.



Processor

Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

CCPA v. GDPR– Personal Information



Personal Information – CCPA

Defined extremely broadly – *i.e.*, to include “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” and “inferences drawn from any [personal information] ... to create a profile about a consumer.”



Personal Data – GDPR

“any information relating to an identified or identifiable natural person ('data subject'); 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”

Questions about Personal Information



- Must it be “identifiable”?
- Employee information
- Inferences
- CCPA exceptions, including
 - GLBA
 - HIPAA/CMIA

Medical Information Exception (CCPA)



Cal. Civ. Code § 1879.145(c) provides that the CCPA shall not apply to:

- (1)(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules [under HIPAA]
- (B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules . . . established pursuant to [HIPAA], to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.
- (C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

Hypothetical – Personal Information

A business records storage company in the U.S. holds PHI on behalf of a national health insurance company. It also holds PII on behalf of numerous national grocery chains. It applies the same data protections to the PHI and PII.

Is it exempt from the Act?



Lawful Use of Personal Data/California Consumer PI

GDPR

- GDPR begins with general rule of confidentiality and then specifies multiple “legal bases” that provide lawful grounds to process personal data or SPD
- Data subject’s consent is one legal basis
- Consent is required to offer “information society services” directly to a child below 16 (or age between 13-16 set by Member State)
- Data subject has right to object to processing on basis of “legitimate interests” or “performing a task in the public interest”

CCPA

- CCPA does not have a list of legal bases like GDPR or HIPAA Privacy Rule
- Consumers age 16+ may “opt-out,” *i.e.*, ask businesses not to sell their PI
- Business needs opt-in consent to sell PI about a minor under age 16
 - Minor can consent from age 13-16
 - Parent/guardian must consent if younger than 13

Legal Bases for **non-SPD** Under GDPR

- For processing that does not involve Sensitive Personal Data, legal bases under GDPR Article 6 apply such as:
 - Processing is necessary for the **performance of a contract**
 - Processing is necessary for the performance of a **legal obligation to which controller is subject**
 - Processing is for the purposes of the **legitimate interests** pursued by the controller, except where interests are overridden by data subject's rights
- May receive Personal Data under Data Processing Agreement with controller

Legal Bases for Processing SPD Under GDPR

- Medical Care
- Public Health
- Scientific Research
- Consent

GDPR Article 9(2)(h) Medical Care Basis

- Article 9(2)(h) basis is available if SPD processing is:
 - **necessary** for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
 - **on basis of Union or Member State law** or pursuant to contract with health professional; and
 - by or under the responsibility of a professional subject to the obligation of **professional secrecy** under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
- “Professional secrecy” means data is obtained and processed by an appropriate qualified medical professional

GDPR Article 9(2)(i) Public Health Basis

- Article 9(2)(i) basis is available if SPD processing is:
 - **Necessary** for reasons of public interest in area of public health, such as ensuring high standards of quality and safety of health care and of medicinal products or medical devices; *and*
 - On the basis of **Union or Member State law**, which must provide “for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.”

GDPR Article 9(2)(j) Research Basis

- Processing is
 - **necessary** for archiving purposes in the public interest, **scientific** or historical **research purposes** or statistical purposes
 - subject to appropriate **safeguards** to protect rights of individuals in accordance with Article 89(1) (e.g., data minimisation)
 - based **on Union or Member State law**
 - which shall be **proportionate to the aim pursued**, and
 - respects essence of the right to data protection and provide for suitable and specific measures to **safeguard** the fundamental rights and the interests of the data subject
- **Recital 159 interprets scientific research purposes broadly** to include, for example, technological development and demonstration, fundamental research, applied research and privately funded research

Requirements for Consent Under GDPR

- **Freely given:** Individual must have a realistic choice, or the realistic ability to refuse or withdraw consent without detriment
- **Specific:** Consent must include a specific, transparent statement of each purpose, including, without limitation, purposes other than treatment
- **Informed:** Individual must be informed of the nature and extent to which individual is consenting
- **Unambiguous:** Consent must include a statement or “clear affirmative act” that indicates the individual has agreed to the proposed processing activities
 - *E.g.*, checking an unchecked box in an online context

Additional “Explicit” Consent Requirement for SPD

- For the processing of health data or other Sensitive Personal Data, individual’s consent must be **explicit**, which is a higher standard than unambiguous
- Article 29 Data Protection Working Party examples of explicit consent:
 - Hand-written signature – Electronic signature - Uploaded scanned signed document
 - Two-stage verification of consent requiring individual to click on a verification link sent by email or text message after initially consenting
- Informed consent to participate in research under EU Clinical Trial Directive or other human subjects protection laws is distinct requirement from privacy consent

Notice Requirements

GDPR Privacy Notice Content

- Identity and contact details of controller
- Purposes and legal basis of processing
- If processing based on legitimate interests, controller's legitimate interests
- Recipients or categories of recipients of the Personal Data, if any
- If controller will transfer Personal Data to a third country, the existence of an adequacy decision or reference to the appropriate safeguards and means to obtain
- Period for which data will be stored or criteria used to determine period

CCPA Privacy Policy Content

- PI collected
- Categories of sources of PI
- Purposes for collecting or selling
- Whether PI is being sold/disclosed
- To whom PI is being sold/disclosed

Data Subject Rights

| Topic | CCPA | GDPR |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Right of access | <p>Right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.</p> <p style="text-align: center;"><u>plus</u></p> <p>Right of portability (similar to Art. 20 GDPR)</p> | <p>Right to obtain from the controller confirmation as to whether or not personal data . . . Are being processed and . . . To the personal data as well as other information (Art. 15)</p> <p>Right to receive the personal data 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 (Art. 20)</p> |

Data Subject Rights

| Topic | CCPA | GDPR |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Right to be forgotten | Right to request that a business delete any personal information about the consumer which the business has collected from the consumer. | Right to obtain from the controller the erasure of personal data . . . Without undue delay where one of several grounds applies (.e.g., data are no longer necessary in relation to the purposes for which they were collected, withdrawal of consent) (Art. 17) |
| Right to “opt out” for third party sale | Right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information. | Right to withdraw consent to processing at any time (Art. 7) |
| Right to object to processing | N/A | Article 21 |
| Right not be subject to automated processing | N/A | Article 22 |

Hypothetical – Subject Access Requests

“A consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.”

Cal. Civ. Code 1798.100

A fitness wearables company receives a request from an individual on January 5, 2020 seeking all information that the company has on him. Must the company produce the information?

- Is the company a “business”?
- Does the company “collect” the data?
- Is this a verifiable consumer request?
- Is this covered activity or wholly outside of California?



10 Practical Preparation Steps

1

Data and System
Inventory

2

Review and
Update External
Privacy
Policies/Notice

3

Consumer
Rights Requests
Internal Process
and Checklist

4

Review and
Incorporate
Applicable
Exceptions

5

Review and
Incorporate
Modalities for
Requests

6

Train Your
Employees

7

“Do not sell my
personal
information”
button

8

Children’s
Personal
Information

9

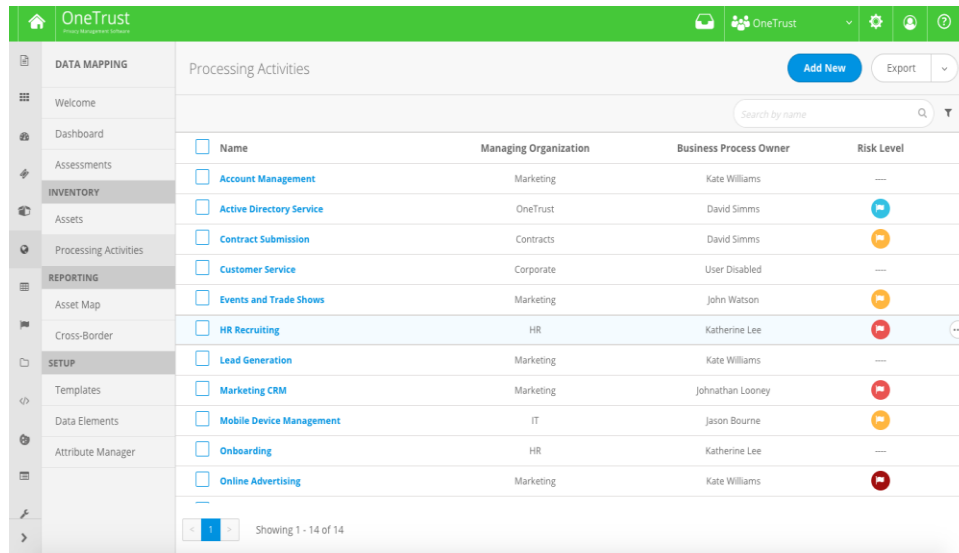
Process to honor
“Do not sell my
PI” requests

10

Reporting and
Metrics

1 | Conduct a Data and System Inventory

- Starting point to understand **where personal information resides and flows** within the organization
- Necessary to answer and implement **consumer rights requests** properly
- Ensure that systems allow for **easy access and retrieval** of data sets
- Be able to identify where personal information **associated to an individual** is located



The screenshot displays the OneTrust Privacy Management System interface. The left sidebar shows a navigation menu with categories like DATA MAPPING, INVENTORY, REPORTING, and SETUP. The main content area is titled 'Processing Activities' and contains a table with the following data:

| <input type="checkbox"/> | Name | Managing Organization | Business Process Owner | Risk Level |
|--------------------------|--------------------------|-----------------------|------------------------|------------|
| <input type="checkbox"/> | Account Management | Marketing | Kate Williams | --- |
| <input type="checkbox"/> | Active Directory Service | OneTrust | David Simms | + |
| <input type="checkbox"/> | Contract Submission | Contracts | David Simms | + |
| <input type="checkbox"/> | Customer Service | Corporate | User Disabled | --- |
| <input type="checkbox"/> | Events and Trade Shows | Marketing | John Watson | + |
| <input type="checkbox"/> | HR Recruiting | HR | Katherine Lee | + |
| <input type="checkbox"/> | Lead Generation | Marketing | Kate Williams | --- |
| <input type="checkbox"/> | Marketing CRM | Marketing | Johnathan Looney | + |
| <input type="checkbox"/> | Mobile Device Management | IT | Jason Bourne | + |
| <input type="checkbox"/> | Onboarding | HR | Katherine Lee | --- |
| <input type="checkbox"/> | Online Advertising | Marketing | Kate Williams | + |

At the bottom of the table, it indicates 'Showing 1 - 14 of 14' items.

2 | Review and Update External Privacy Policies/Notices

- CCPA requires businesses to **disclose to consumers specific information**
- Other **mandatory disclosures** to be made in the online privacy policy
- GDPR requires to provide data subjects with information where personal data are collected directly from the DS and slightly different ones where the data has not been collected from the DS (Article 13 & 14)

The screenshot shows the top portion of a privacy notice page. At the top, a dark grey header contains the text "Privacy Notice" in white, with "Effective December 13, 2018" in green below it. Below the header is a light grey navigation bar with four links: "Privacy Notice", "Cookie Notice", "Cookie Preferences", and "Exercise Your Rights". The main content area is divided into two columns. The left column is titled "Table of Contents" and lists several sections in green: "Introduction", "Information We Collect", "How We Use Information", "Third Parties", "Information Security", "Cookies and Website Tracking", "Your Privacy Rights", "Data Subject Rights", and "International Data Transfer". The right column is titled "Introduction" and contains a paragraph of text followed by a bulleted list of two items.

Privacy Notice
Effective December 13, 2018

[Privacy Notice](#) [Cookie Notice](#) [Cookie Preferences](#) [Exercise Your Rights](#)

Table of Contents

- [Introduction](#)
- [Information We Collect](#)
- [How We Use Information](#)
- [Third Parties](#)
- [Information Security](#)
- [Cookies and Website Tracking](#)
- [Your Privacy Rights](#)
- [Data Subject Rights](#)
- [International Data Transfer](#)

Introduction

OneTrust ("OneTrust," "we" or "us") offers software for privacy management and web marketing compliance, and hosts and attends events globally. We also own and operate several websites (e.g. onetrust.com and privacy.pedia.onetrust.com) (individually, "Website" and collectively the "Websites"). This privacy notice aims to inform you about how we collect, use, disclose and store information about you when you:

- interact or use our Websites, including downloading materials from our resources page or requesting a demo,
- register and/or attend any of our events (e.g. Privacy Connect), webinars, or the

3 | Draft and Implement Consumer Rights/Data Subject Requests Internal Process and Checklist

✓ How does the business enable consumer rights?

- ✓ Must include at a **minimum a toll-free telephone number and a website address** (if the business has a website)

For example: Companies may offer **standardized web forms** on their website

✓ What employees who receive request are expected to do

✓ Process for the **privacy office to review** each request and determine what action should be taken

- ✓ Verify the legitimacy of the request

- ✓ Verify the consumer's identity

 - ✓ Only "verifiable requests" must be honored

✓ How to **implement the request** within the organization

- ✓ Obtain the data

- ✓ Delete the data from all systems

✓ An effective and **secure way of responding** to the consumer

Intake Requests

Assign Tasks

Record Completion

Communicate Securely

Uniform Responses

4 | Review and Incorporate Applicable Exceptions

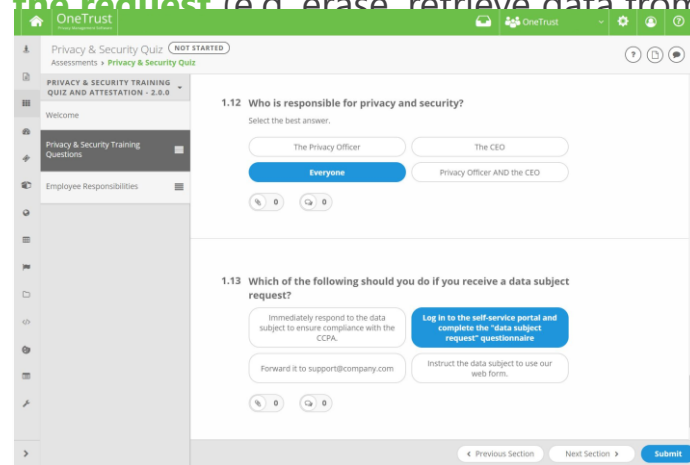
- Nine **exceptions** to the right of deletion (*summarized below*) for CCPA
 1. Complete the transaction
 2. Detect security incidents
 3. Debug to identify and repair errors
 4. Exercise free speech
 5. Comply with the California Electronic Communications Privacy Act
 6. Engage in research in the public interest
 7. Reasonably aligned with consumer expectations based on relationship with the business
 8. Comply with a legal obligation
 9. Otherwise a lawful manner that is compatible with the context it was provided
- GDPR: Pay attention to scope for each right and some exceptions
- Need step in your process to **verify whether exception applies**

5 | Review and Incorporate Modalities for Requests

- Make available to consumers **two or more designated methods** for submitting requests including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address
- Honor requests **free of charge**
- Honor requests (meaning disclosing and delivering the required information) within **45 days of receipt** of a verifiable consumer request
- Disclosure has to cover the **12-month period preceding** the receipt of the request
- The disclosure must be **in writing**
- If the consumer has an account with the business, through that account (business **cannot require consumer to create an account** for this purpose)
- If the consumer does not have an account, in a **readily usable format** that allows consumer to transmit the information to another entity

6 | Train Your Employees

- Mandatory training under CCPA
 - Businesses are responsible for ensuring that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA are **informed of all requirements** and how to direct consumers to exercise their rights
- Not mandatory under GDPR but necessary in practice
- Key employees to train
 - Employees who are likely to **receive the requests** (support personnel for example)
 - Employees who will have to **"implement" the request** (e.g. erase, retrieve data from an application)
 - The privacy team



7 | “Do not sell my personal information” button

- Businesses need to provide a **clear and conspicuous link** on the business’ Internet homepage, titled “Do Not Sell My Personal Information”...
- ...to an Internet Web page that enables a consumer to **opt out of the sale** of the consumer’s personal information
- Work with the **IT/website team** to implement link on organization’s website

8 | Implement process and/or tool to collect “prior affirmative authorization” before selling children’s personal information

- Business cannot sell the personal information of consumers the business has actual knowledge are below 16 unless:
 - It has received **affirmative authorization from the child** for children between 13 and 16
 - It has received **affirmative authorization from the parent or guardian** for children below 13

9 | Process to honor “Do not sell my PI” requests

- Need to **know the third parties** you are selling personal information to
- Process to **alert third parties** to stop processing as soon as the request is received

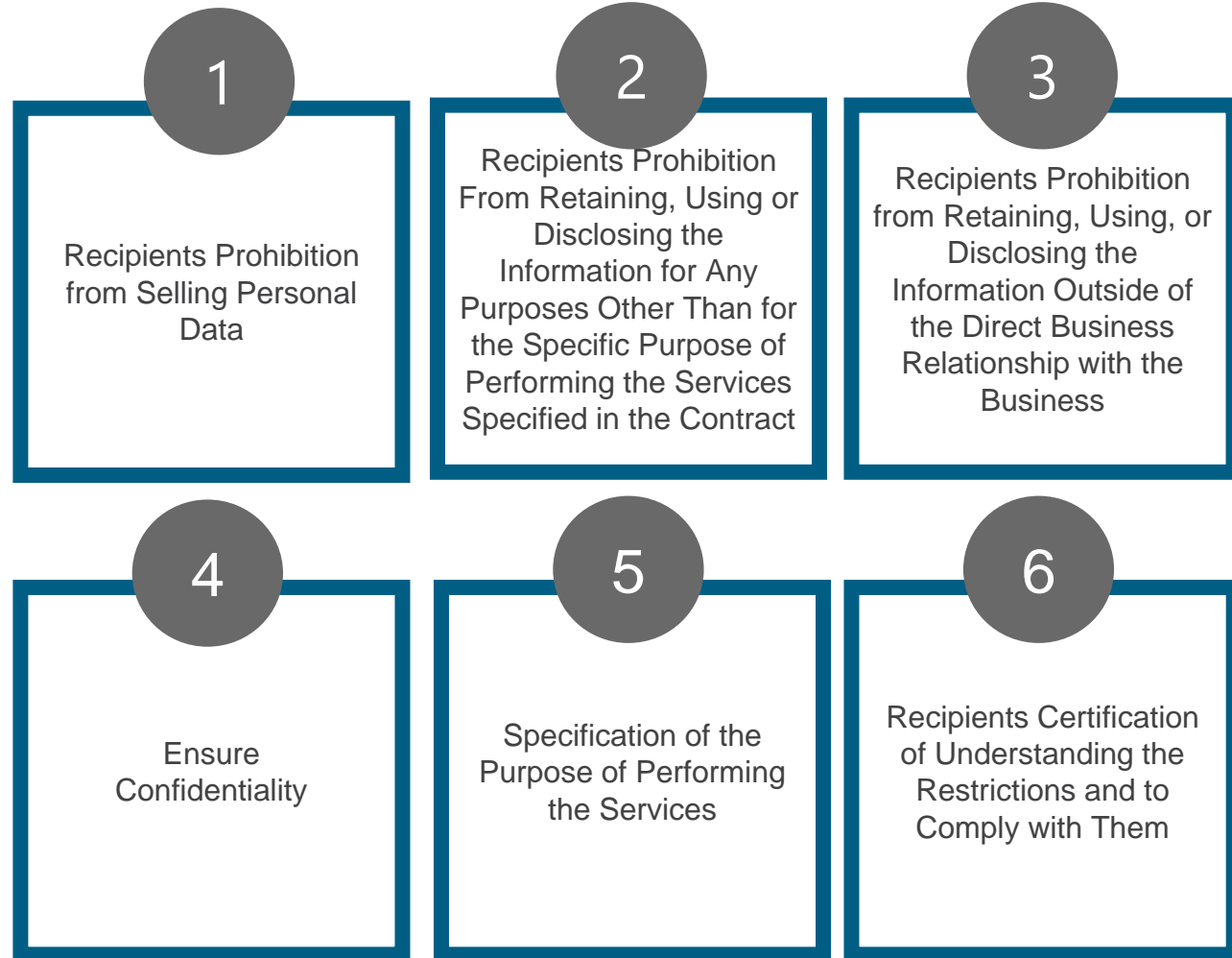
10 | Reporting and Metrics

- Keeping **evidence** of consumer requests
- Monitor **incoming requests**
 - Request volume
 - Fulfilment status
 - Aging/outliers

Bonus Content - Vendor Management - GDPR



Bonus Content - Vendor Management - CCPA



We've Seen this Movie Before

Side-by-side listing of both GDPR and HIPAA requirements for processing agreements and business associate agreements

<https://iapp.org/news/a/gdpr-vendor-management-we-seen-this-movie-before/>

Under the GDPR, the processing agreement must:

Under HIPAA, the Business Associate Agreement must:

set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller;

establish the permitted and required uses of PHI by the business associate;

require the processor to act only on the written instructions of the controller;

provide that the business associate may not use or further disclose the PHI other than as permitted or required by the contract or by law;

require the processor to ensure that people processing the data are subject to a duty of confidence;

require the use of appropriate safeguards to prevent unauthorized uses or disclosures of PHI;

require the processor to take appropriate measures to ensure the security of processing in accordance with Article 32;

require reporting any unauthorized uses or disclosures to the covered entity;

require the processor to only engage a sub-processor with the prior consent of the data controller and a written contract, and impose the same data protection obligations on the sub-processor:

require the business associate to ensure that any subcontractors that will have access to PHI agree to the same restrictions and conditions that apply to the business associate;

We've Seen this Movie Before

Side-by-side listing of both GDPR and HIPAA requirements for processing agreements and business associate agreements

<https://iapp.org/news/a/gdpr-vendor-management-we-seen-this-movie-before/>

Under the GDPR, the processing agreement must:

Under HIPAA, the Business Associate Agreement must:

require the processor to assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

require the disclosure of PHI where necessary to satisfy the covered entity's obligations with respect to individual (data subject) access or amendment requests;

require the processor to assist the controller in ensuring compliance with their obligations with respect to security, breach notification, and data protection impact assessments;

require the business associate to comply with applicable requirements under the HIPAA Privacy Rule to the extent that the covered entity has delegated the carrying out of an obligation under the HIPAA Privacy Rule;

require the processor delete or return all personal data to the controller upon request at contract termination; and

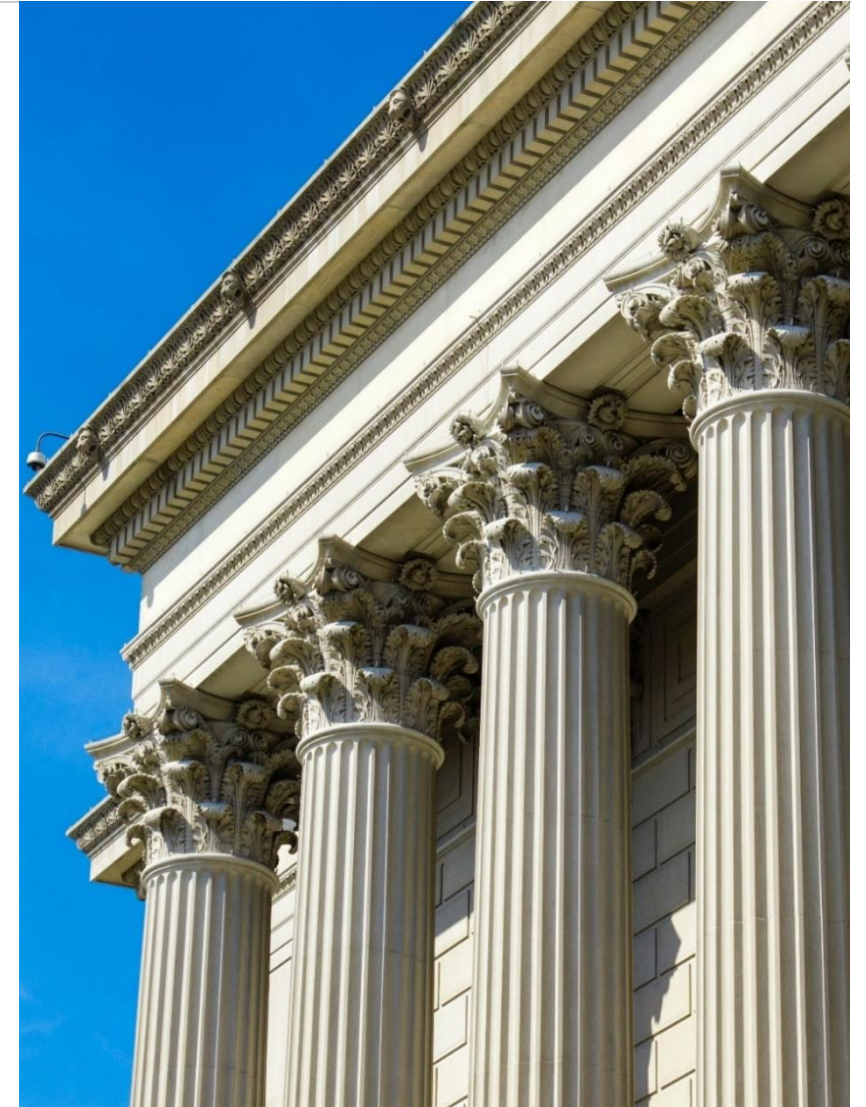
require the return or destruction of PHI at the termination of the contract, where feasible;

require the processor to make available to the controller all information necessary to demonstrate compliance with Article 28 obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

require the business associate to make available its internal practices, books and records relating to the use and disclosure of PHI available to HHS;

Agenda

- 1 How has the privacy landscape changed in the last year?
- 2 GDPR and CCPA Overview
- 3 Comparing the CCPA and the GDPR
- 4 10 Practical Preparation Steps
- 5 Regulatory Enforcement and Civil Litigation**



Enforcement: The CCPA

Only the Attorney General is allowed to bring an action against businesses for improperly selling, storing or sharing personal information, or violations of the Act's transparency requirements. Businesses have 30 days to "cure."

- AG-brought civil actions can subject companies to civil penalty of not more than \$2,500 for each violation of \$7,500 for each intentional violation.

Consumers are only allowed to bring a private right of action (including class-actions) due to a security breach and may recover damages in an amount not less than \$100 and not greater than \$750 per consumer per incident – or actual damages, "whichever is greater."

Consumers are also required to give businesses 30 days to cure before filing suit



CCPA Enforcement

"Attorney General Becerra noted that the CCPA did not provide resources for the AGO to carry out the rulemaking nor its implementation thereafter; the Attorney General called the existing deadline "simply unattainable."

— Attorney General Becerra
California Attorney General's Office



Administrative Fines

- Data subject may lodge complaint with DPA
- EU Member State DPAs investigate and enforce GDPR
- GDPR establishes a tiered approach to administrative penalties:
 - Greater of **20,000,000 EUR** for certain severe infringements (e.g., data subjects' rights violations) or **4% of annual worldwide revenue** for undertakings
 - Greater of **10,000,000 EUR** for other specified infringements, including data breach notification violations, or **2% of annual worldwide revenue** for undertakings
- “Undertaking” pulls revenues of parent/subsidiaries into calculation

Recent Administrative Enforcement Actions

- French DPA (CNIL) assessed a EUR 50 million fine against Google for lack of transparency, inadequate notice and lack of valid consent regarding the personalization of advertisements (January 2019)
- Portuguese DPA assessed EUR 400,000 fine against **Portuguese hospital** with false user profiles and 985 active physician user accounts even though only 296 physicians worked at hospital (July 2018)
- DPA of Baden-Wurttemberg Germany assessed EUR 20,000 fine against chat platform that stored users' passwords in an unencrypted form (September 2018)
- Austrian DPA assessed EUR 5,280 fine against a sports betting cafe that installed a CCTV that recorded a public sidewalk and parking lot in front of cafe without a lawful basis and in violation of its notice obligations (September 2018)

Private Remedies

- Data subject may lodge complaint with DPA or **sue the data controller or processor** in EU Member State courts for monetary and non-monetary damages if GDPR rights are infringed
- Statute of limitations are those of EU Member States, e.g., 6 years in UK (unless extended if claim hidden and only later discovered)
- GDPR **reverses burden of proof**, *i.e.*, controller or processor must prove that it complied with GDPR and is not responsible for event causing damages
- GDPR provides for **joint and several liability** if more than one person is involved in Personal Data processing

Right to Claim – Distress as Damages

- *Vidal-Hall v. Google Inc.* [2015] EWCA Civ 311
 - The Claimants’ claims were based on the distress suffered from:
 - learning that their personal characteristics formed the basis for Google’s targeted advertisements; or
 - having learnt that such matters might have come to the knowledge of third parties who had used or seen their devices.
 - The Claimants’ claims were **exclusively** for distress and anxiety, not financial damage
- Art. 82(1) – any person who has suffered “**material or non-material damage**” as a result of a breach of the GDPR has the right to receive compensation from the controller or processor
- Section 168(1) UK Data Protection Act 2018 – expressly states that “**non-material damage**” includes distress

Right to Claim – Vicarious Liability

Various Claimants v. WM Morrisons Supermarket plc [2017] EWHC 3113

- Personal data of approximately 100,000 employees subject to a breach in early 2014 by rogue employee anonymously posting the information on a file-sharing website and then sent to three newspapers
- Group claim brought by 5,518 claimants
- No concrete harm had been caused to the data subjects – claim was brought based on the distress suffered
- Morrisons was held **not to be directly liable for the data breach**
- However, Morrisons was held to be **vicariously liable**
- Morrisons to appeal the decision on the vicarious liability finding

Class Action Claims by Not-for-Profits

- Data subject has right to mandate a **not-for-profit body, organization or association** active in the field of the protection of data subjects' rights with regard to the protection of their Personal Data to
 - **lodge a complaint with DPA on subject's behalf,**
 - **exercise the rights** to pursue remedies (under Articles 77, 78 and 79) and
 - **exercise the right to receive compensation** (under Article 82) where provided by Member State law
- Not-for-profit can be created by a concerned group or a law firm to represent a class of individuals and bring claims on their behalf

Will there be an explosion of GDPR class actions?

Argument For No

- GDPR does not provide statutory damages
- No right to attorneys' fees
- Europe does not have same litigation culture as United States

Arguments for Yes

- GDPR provides for recovery of distress and other non-monetary damages
- GDPR reverses burden of proof

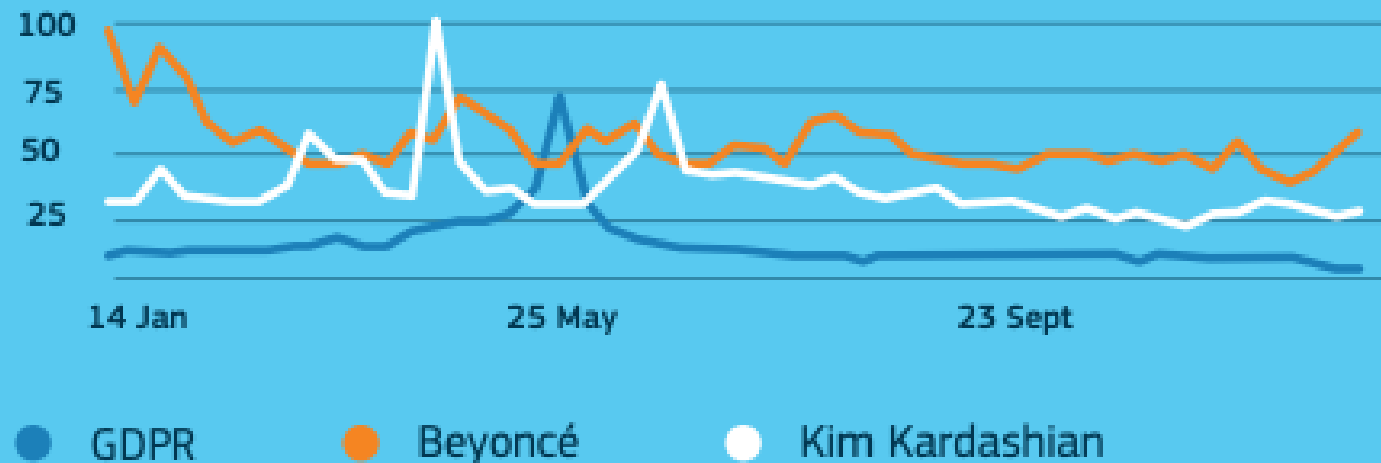
Is GDPR Enforceable against US Companies?

- DPA or data subject may enforce GDPR and recover fines/judgments from US company with any of following in EU:
 - establishment/assets
 - EU representative (for company without an establishment in EU)
 - Affiliate with establishment/assets in EU
- Absent enforcement mechanism in EU, potential mechanisms include:
 - US company has agreed contractually to comply with GDPR and/or to indemnification obligations and contract is enforceable in US court
 - Complex international law surrounding enforcement of foreign (*i.e.*, EU country) judgments in US courts and extradition of criminals

GDPR in Numbers

Google searches

During the peak month of May 2018 GDPR was searched more often on Google than American superstars Beyoncé and Kim Kardashian.

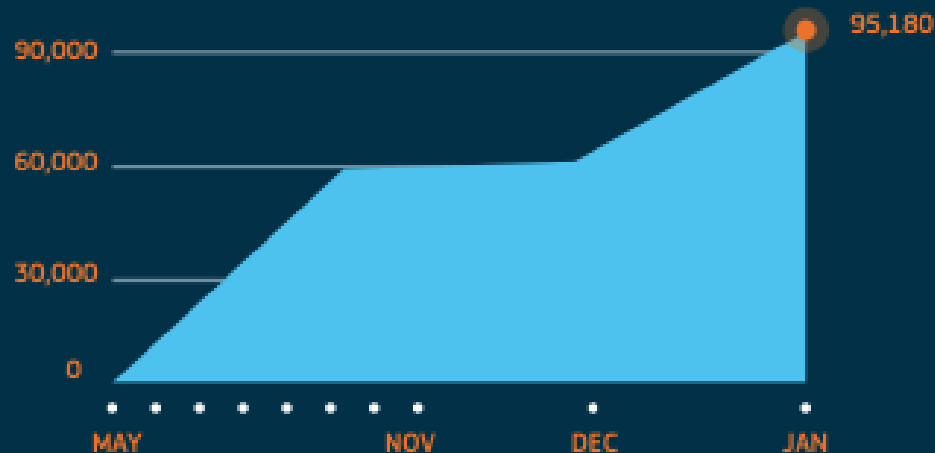


Interest rated between 0-100, based on number of searches on Google.
Source: Google trends

GDPR in Numbers

Number of complaints to Data Protection Authorities (DPAs) under the GDPR*

Complaints can come from any individual who believe their rights under GDPR have been violated, but the GDPR also introduced the possibility for an organisation mandated by individuals to introduce such complaints. This possibility has been used immediately after the entry into application of the GDPR.

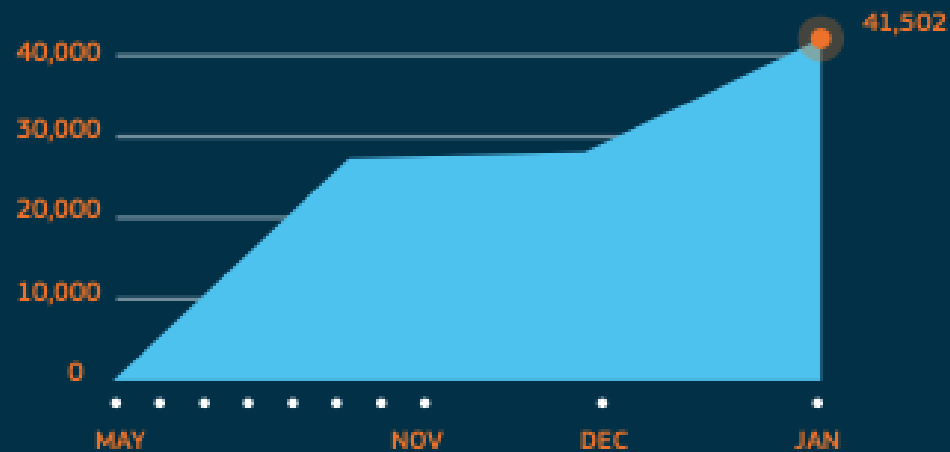


Accumulated number over time.**
From all data protection authorities in Europe.

GDPR in Numbers

Number of data breach notifications*

When personal data for which a company is responsible is accidentally or unlawfully disclosed, that company is obliged to report this data breach to their national DPA within 72 hours after finding out about the breach.



Accumulated number over time.**
From all data protection authorities in Europe.

GDPR Enforcement

"Our first priority will be to be **responsive** to the risks and trends we identify in relation to **complaints** lodged."

— Helen Dixon, Irish DPA
2018 IAPP Global Summit Washington, DC



Coimisiún
Cosanta Sonraí
Data Protection
Commission



Republik Österreich
Datenschutz
behörde

"It's not our first task to fine, it's our first task to see if you're **compliant**, and if you're not compliant it will be a problem. There are **no grace periods** because the grace period was already two years."

– Andrea Jelinek, Austrian DPA; Chair, A29WP

Sidley Disclaimer

Parts of this presentation (where so noted) were prepared by Sidley Austin LLP and Affiliated Partnerships (the Firm) for informational purposes and is not legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. You should not act upon this information without seeking advice from a lawyer licensed in your own jurisdiction. The Firm is not responsible for any errors or omissions in the content of this presentation or for damages arising from the use or performance of this presentation under any circumstances.

Do not send us confidential information until you speak with one of our lawyers and receive our authorization to send that information to us. Providing information to the Firm will not create an attorney-client relationship in the absence of an express agreement by the Firm to create such a relationship, and will not prevent the Firm from representing someone else in connection with the matter in question or a related matter. The Firm makes no warranties, representations or claims of any kind concerning the information presented on or through this presentation.

Attorney Advertising – For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, +1 212 839 5300; One South Dearborn, Chicago, IL 60603, +1 312 853 7000; and 1501 K Street, N.W., Washington, D.C. 20005, +1 202 736 8000. Prior results do not guarantee a similar outcome. Some images on this presentation are of actors and not of clients or Firm personnel.

McDermott Disclaimer

Parts of this presentation (where so noted) were prepared by McDermott Will & Emery LLP (the Firm) for informational purposes and is not legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. You should not act upon this information without seeking advice from a lawyer licensed in your own jurisdiction. The Firm is not responsible for any errors or omissions in the content of this presentation or for damages arising from the use or performance of this presentation under any circumstances.

Do not send us confidential information until you speak with one of our lawyers and receive our authorization to send that information to us. Providing information to the Firm will not create an attorney-client relationship in the absence of an express agreement by the Firm to create such a relationship, and will not prevent the Firm from representing someone else in connection with the matter in question or a related matter. The Firm makes no warranties, representations or claims of any kind concerning the information presented on or through this presentation.

March 5, 2019

GDPR and New California Privacy Law Update

Andrew Clearwater, OneTrust

Daniel Gottlieb, McDermott Will & Emery

Kate Heinzelman, Sidley Austin

SIDLEY

Kate Heinzelman

+1 202 736 8416

kheinzelman@sidley.com

OneTrust

Andrew Clearwater

+1 207-766-6654

aclearwater@onetrust.com

**McDermott
Will & Emery**

Daniel F. Gottlieb

+1 312 984 6471

dgottlieb@mwe.com