GDPR vs. the California Consumer Privacy Act (CCPA) and Handling GDPR Personal Data Breaches

Laura Jehl, Partner (Washington DC), BakerHostetler
Stephanie Malaska, Associate (Washington DC), BakerHostetler
Elizabeth (Betsy) Dellinger, General Counsel, Park Place Technologies

November 1, 2018
“In comparing various authors with one another, I have discovered that some of the gravest and latest writers have transcribed, word for word, from former works, without making acknowledgment.”

- Pliny the Elder
New and Ongoing Challenges

NEW

**The California Consumer Privacy Act**
- How does GDPR compliance intersect with CCPA requirements?

ONGOING

**Reporting personal data breaches under the GDPR**
- Initial considerations (data transfer mechanisms, vendor DPAs, privilege issues)
- Notifying regulators (when, where, how, in what language?)
- Notifying data subjects (determining what poses a risk to "rights and freedoms")
- Security incidents involving unstructured data

**Recent GDPR Enforcement Actions**
GDPR Snapshot

• **Became Effective May 25, 2018**
• Applies to organizations that:
  – Are “established” in the EU;
  – Process personal data of EU “data subjects” when offering them goods or services (whether or not for payment); or
  – Monitor behavior occurring in the EU.
• Key terms:
  – “Personal data”
  – “Processing”
  – “Controller” and “Processor”
• Max fine: greater of €20 million or 4% of worldwide annual turnover
CCPA Snapshot

- Effective July 1, 2020
- Compliance begins January 1, 2020
- Broad scope and application
- Protects “personal information” of “consumers”
- Greatly enhances rights of consumers
- Fines
  - AG can impose up to $2,500 for each violation or $7,500 per each intentional violation. Violating entity will be subject to an injunction.
- Private right of action
  - Consumer may bring an action for a business’s alleged failure to “implement and maintain reasonable security procedures and practices” that results in a data breach.
CCPA Applicability

• Any for-profit “Business” doing business in California, that:
  1. Has $25 million+ in revenue;
  2. Annually buys, receives for the business’s commercial purposes, sells or shares for commercial purposes the Personal Information (PI) of **50,000 or more “Consumers”** households or devices; or
  3. Derives 50%+ of its annual revenues from selling Consumers’ PI.

• OR, an entity that:
  – Controls or is controlled by a covered business

• Some application to “Service Providers” as well
CCPA Does NOT Apply To:

- Commercial conduct taking place wholly outside of California
- Non-pseudonymously identifiable or aggregated information
- Compliance with legal obligations
- Other categories of non-application
  - Certain health information and healthcare entities
  - Clinical trial information
  - Information processed, collected, sold, or disclosed pursuant to GLBA
CA residents enjoy expanded rights, similar to those under GDPR:

1. The right to know what PI is being collected about them
   - Sources from which it is collected
   - Purposes for collection or sale of data
   - Types of data
   - Categories of third parties with whom it is shared
2. The right to access and download PI in a transferrable way
3. The right to refuse to allow companies to sell their PI (opt-out)
   - Opt-in for those under 16
4. The right to deletion
   - Some exceptions
CCPA Covered Business Obligations

- Recordkeeping obligations *in advance* of effective date
- Privacy provisions must be included in service provider contracts
- Update privacy policies & notices
- Implement internal processes
  - Map data flows
  - Procedures for responding to consumer requests
  - Non-discrimination and incentive programs
GDPR vs CCPA: Similarities

- Extra-territorial reach
- Broad definition of personal information / personal data
- Data subject rights of access, deletion, and portability
- Requirement to notify consumers of privacy practices prior to or at time of data collection
- Notify consumers of changes to privacy practices
- Certain rights for children
- Time limits for fulfilling data subject requests
  - GDPR allows 30 days
  - CCPA allows 45 days
- Penalties for data breaches
GDPR vs CCPA: Differences

Found Only in CCPA

- Right to opt-out only covers the sale of personal information
- Establish specific communication channels for consumers
  - Toll-free phone number and conspicuous link on website
- Extend “personal information” protections to information about devices and households
- Recordkeeping on a 12-month basis. You are only required to provide information once per year
- Private right of action for data breaches
GDPR vs CCPA: Privacy Notices

- Does not need to be online
- Purposes of processing
- Legal basis for processing
- Legitimate interests of controller or third party
- Recipients or categories of recipients
- Any cross-border transfers and legal mechanisms
- Data retention period or criteria used to determine that period
- Whether data subject is obliged to provide the personal data and possible consequences of failure to provide such data
- Existence of automated decision-making, including profiling

- Must be online
- Must update notice every 12 months
- Categories and specific pieces of personal information collected, its sources, and its intended use of the personal information.
- Categories of third parties with whom business shares information Description of consumer’s rights to request
- If selling data, a “Do Not Sell My Personal Information” link on its website’s homepage and online privacy policy that functions as an opt-out link
- Whether information is sold and a list of categories of information that are sold
- Whether information is disclosed for business purposes and a list of categories of information disclosed
CLE CODE #1

Privacy 1
Data Breaches & GDPR
What is a “personal data breach?”

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

GDPR Article 4(12)
Initial Considerations (First 72 Hours)

- Investigations
- Data Processing Agreements (DPAs) among parties involved
- Preservation of privilege
- Notification obligations
  - Who reports?
  - Where to report?
  - Data subject notification?
Investigation & Analysis

- Determine whether entity is subject to GDPR
- Determine whether the incident constitutes a “personal data breach”
  - Types of personal data affected
  - Sensitive or “special categories” of data
- Determine & manage reporting obligations across jurisdictions
  - Special considerations (languages)
  - Controller or processor? Both?
Third Party Data Processing Agreements

• What entities will be accessing personal data?
• Who is a controller and who is a processor?
  – Law firms as joint controllers
• Will personal data be transferred out of the EU?
  – Privacy Shield or Model Clauses
• Structure engagements to protect privilege
Breach Notification

Clock starts ticking when you become aware

“Brief” investigative period allowed to determine if incident actually is a “personal data breach”
Notification, at a glance

**Notify regulator**: unless the breach is unlikely to result in a “risk to the rights and freedoms of natural persons”

– *Supervisory authority* = the data protection authority in each EU jurisdiction

**Notify data subjects**: if the breach is likely to result in a “high risk to the rights and freedoms of natural persons”
Notifying Regulators

• Requirements
  – Online portals
  – Specific language
  – 72 hour window

• Lead Supervisory Authority
  – Benefits of having an LSA
  – If no LSA, notify every Supervisory Authority impacted
    ▪ Location of data subjects?

• Can be done in phases

*Remember:* reporting may result in further scrutiny of privacy and data security practices
Who should do the notification?

• Not every organization will have a DPO (may have an Article 27 Representative)

• Privilege considerations relevant to the involvement of DPO in a multinational investigation

• The practicalities of reporting an incident
Notifying Data Subjects

• Contents
  – Accessible, in “clear and plain language” and local language
  – Nature of the data breach
  – Contact details (DPO)
  – Likely consequences and measures to be taken to mitigate breach

• Method
  – Direct communication, if possible
  – Otherwise, public communication

• Confer with Supervisory Authority, if needed
Unstructured Database Breaches

O365 Incident

- Business is established in the EU or otherwise subject to GDPR
- Custodian mailboxes compromised
- Unknown contents, which may include PII (US) and personal data (EU), as well as “sensitive” data

WHAT TO DO NOW?
Recent GDPR Enforcement Actions

UK (ICO)
• First enforcement action against a Canadian analytics company for breaches of Article 5 and 6 of the GDPR for “processing personal data in a way that data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for processing.”
• Company ordered to cease processing personal data of UK or EU citizens for the purposes of data analytics, political campaigning or any other advertising.

Portugal (CNPD)
• CNPD fined a Portuguese hospital 400,000 euros for GDPR violations related to the principles of integrity and confidentiality and data minimization, including the hospital’s failure to put in place appropriate technical and organizational measures

Austria (DSB)
• DSB fined an establishment 4,800 euros for use of its CCTV camera in violation of GDPR.

France (CNIL)
• Last week CNIL gave formal notice to a data marketing company, citing the company’s failure to obtain valid consent for the processing of geolocation data for advertising targeting purposes and the failure to implement a data retention policy and ensure the security and confidentiality of personal data.
• Company has three months to remedy the violations or they will face a fine.
CLE CODE #2

Privacy2
Question & Answer

Betsy Dellinger
T +1.202.861.1588
bdellinger@parkplacetech.com

Laura Jehl
T +1.202.861.1588
ljehl@bakerlaw.com

Stephanie Malaska
T +202.861.1716
smalaska@bakerlaw.com
These materials have been prepared by Baker & Hostetler LLP for informational purposes only and are not legal advice. The information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional counsel. You should consult a lawyer for individual advice regarding your own situation.