Baker McKenzie.

NATIONAL APARTMENT ASSOCIATION

GDPR/CCPA Privacy Primer

Michael Egan, Partner
Baker McKenzie, Washington, D.C.

January 31, 2019

Agenda

1. GDPR Primer
2. California Consumer Privacy Act Primer
3. Questions

1 GDPR Primer

EU General Data Protection Regulation (“GDPR”)

What is it?

- ✓ Regulation v. directive
- ✓ First major update since 1995
- ✓ Repeals 1995 directive
- ✓ Applies directly in member states
- ✓ Comprehensive set of requirements with broad application to any “personal data”

EU GDPR

What is “personal data”? (Art. 4(1))

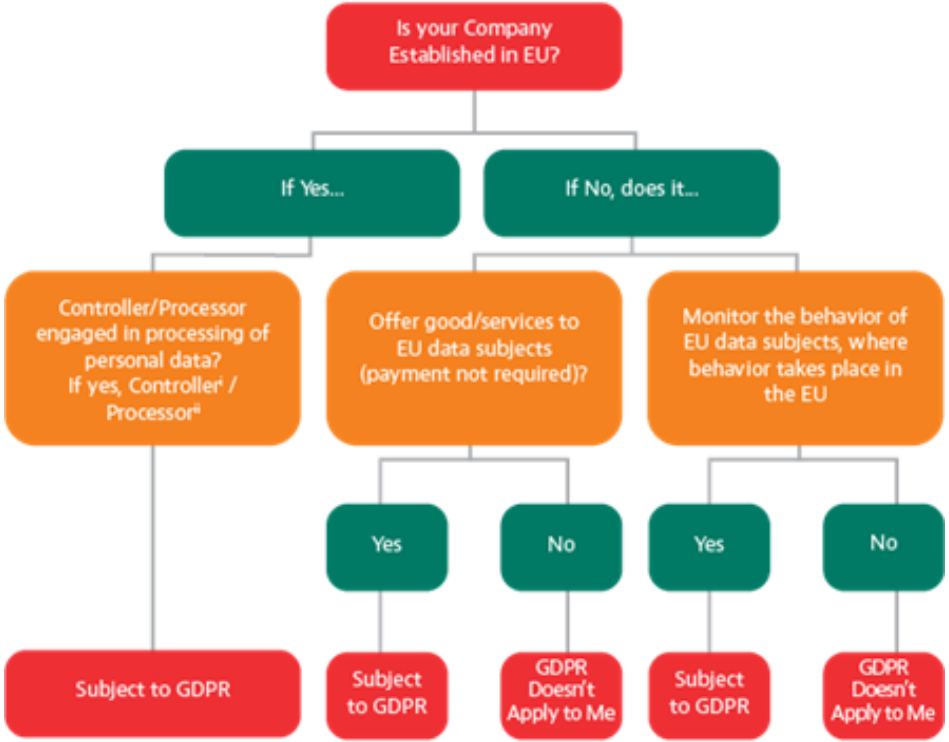
Personal data

“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 by one or more factors specific to . . . that natural person”

- **wide range of individuals covered** – consumers, end users, customer contacts, patients, employees, contractors, business partner contacts, supplier contacts, and more
- **wide range of data covered** – any data linked or linkable to a natural person (even if company does not actually link) – name, email, IP address, cookie data, device identifiers, and more

To Whom Does it Apply?

Does the General Data Protection Regulation (GDPR) Apply to You?



EU GDPR

Administrative Fines by DPAs

Maximum fine of

€20M / ~ $24M

Or **4%** of global annual turnover of prior year

(whichever is greater)

Failure to meet obligations of Articles 5-7, 9, 12-22, or 44-49

- Examples: Failure to adhere to core principles of data processing, infringement of personal rights, failure to meet data subject rights demands, or the transfer of personal data to countries that do not ensure an adequate level of data protection

Maximum fine of

€10M / ~ $12M

Or **2%** of global annual turnover of prior year

(whichever is greater)

Failure to meet obligations of Articles 8, 11, 25-39, or 42-43

- Examples: Failure to comply with technical and organizational requirements (e.g., appropriate data security, data protection by design/default, data protection impact assessment, breach communications)

"Administrative fines are a central element in the new enforcement regime introduced by the Regulation, being a powerful part of the enforcement toolbox of the supervisory authorities"

– Guidance from the European Authorities

EU GDPR

13 Game Changing Elements

1. Data Protection Officers - DPOs

2. Data breach reporting

3. Cross-border data transfer

4. Consent

5. Data mapping

6. Data Processor obligations

7. Rights for data subjects

8. One-Stop-Shop

9. Enforcement & Sanctions

10. PIAs

11. PbD

12. Profiling Restrictions

13. Accountability

Customer-Specific Elements

Customer terms	– Corporate customer standard terms and playbook for contracting
Privacy Statement	– Customer-facing privacy statement(s) for websites, mobile apps, and other sites and features
Procedures for managers	– Direct marketing procedures, data sharing rules, rules on responding to access requests/rights of data subjects
Other customer deliverables	– Statements for information collection points, consent terms, contracts for onward transfers to business partners

Data Breach Response

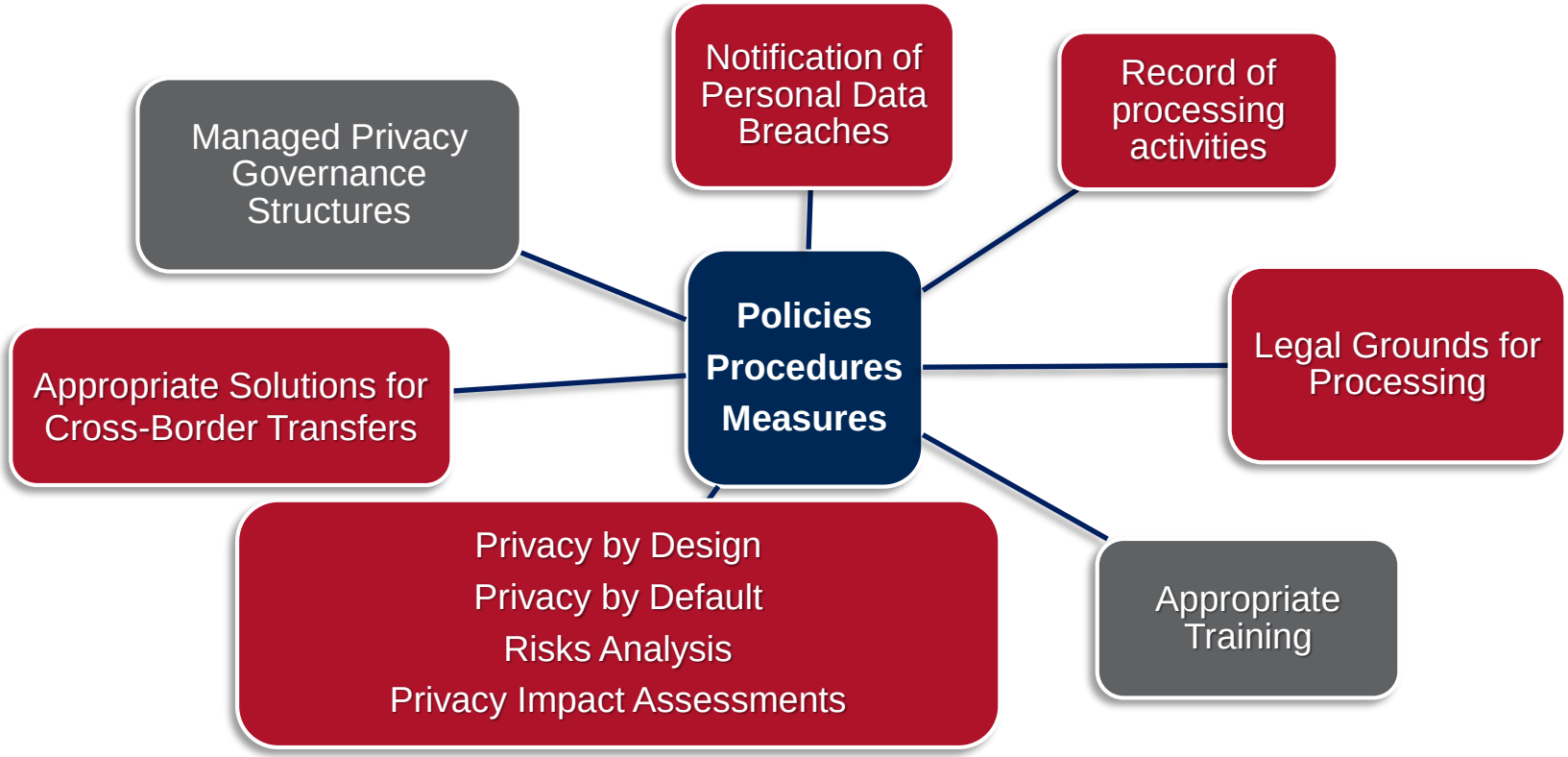
Personal data breach

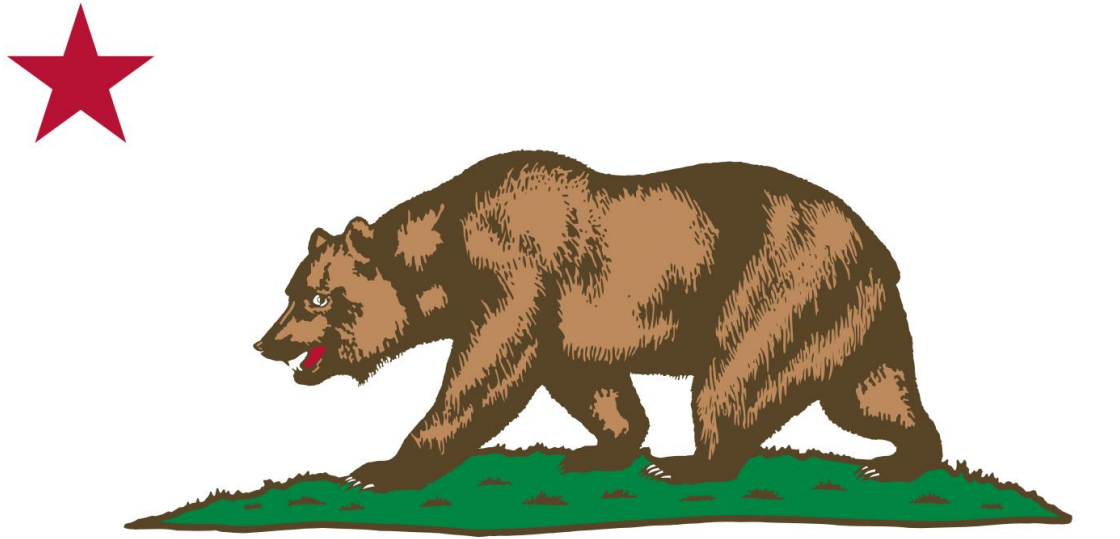
"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

- Not related to the quality / adequacy of the security measures
- Any incident impacting the Confidentiality, Integrity, Availability of personal data
- Must notify supervisory authorities within **72 hours**

EU GDPR

End Game Goal





2 California Consumer Privacy Act

California Consumer Privacy Act

CCPA Timing and Scope

The California Consumer Privacy Act (CCPA) of 2018 was passed into law by California state legislature on June 28, 2018. The CCPA will become operative on January 1, 2020. The Act will grant California consumers privacy rights and increased control over the collection of their personal information.

Redefined Language

Consumer: a natural person who is a California *resident.**

Sell, selling, sale or sold: 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 one business to another business or a third party for monetary or other valuable consideration.

Personal Information (PI): 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***. Examples include:

- Unique device identifier
- Inferences drawn about individuals from the data associated with them
- Browsing history, search history
- Excludes PI that is ***deidentified*** or ***aggregated***.
  - "cannot *reasonably* identify, *relate* to, describe, *be capable of being associated with*, or be linked, directly or *indirectly*, to a particular consumer."
  - business using it must adopt technical and procedural safeguards to prevent its re-identification, have business processes to prohibit re-identification, and not make any attempt to re-identify it.

*The term "resident," as defined in the law, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents.

CCPA Consumer Rights and Enforcement

Consumer Privacy Rights Under CCPA

- Right to Information
- Right to Access
- Right to Data Portability
- Right to Deletion (exceptions apply)
- Right to Opt-Out of the sale of Personal Information to Third Parties
- Right to Equal Service (No Discrimination)
- Explicit consent for selling personal information of minors under 16 (in the case of consumers under 13, consent must be obtained from the consumer's parent or guardian)

Enforcement

- Private Right of Action
  - Limited to data breach violations
  - Recovery of damages ($100-$750)
- Civil penalties
  - Violations (up to $2,500)
  - Intentional violations (up to $7,500)

California Consumer Privacy Act

CCPA Requirements

Consumer PI Asset Inventory

- Consumer Database
- Consumer interface including websites, mobile games, social media
- Digital Marketing Landscape

Privacy Policy and Other Notices Management

- Policy and other privacy notice updates to reference new consumer rights
- Consent management
- Annual updates

'Do Not Sell' (DNS) Link Deployment

- Deploy DNS Link
- Re-Opt-In Management (12 month opt-out)
- Cookie Management

Vendor Management

- Vendor contract updates to ensure compliance with CCPA consumer rights and potentially to avoid the "sale" of consumer PI

Operational Processes

- Consumer PI asset inventory management and maintenance
- Consumer Right's Request process implementation (e.g., authentication, honoring "Do not Sell" requests" and re-opt-in management)
- Incident management process
- Information Security compliance control management (e.g., encryption)

3 Questions?

Baker McKenzie.

Michael Egan

Partner

Baker McKenzie

Washington, D.C.

michael.egan@bakermckenzie.com

Thank You

www.bakermckenzie.com