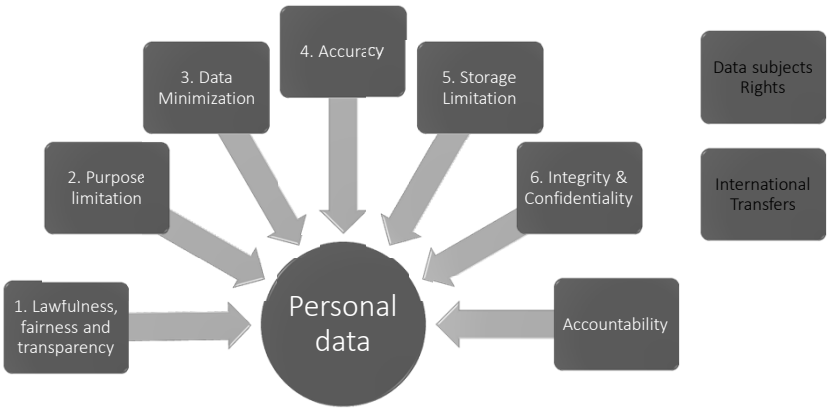
GDPR, CCPA, AND CYBERSECURITY ISSUES

SCCE Regional Conference
Chicago, May 3, 2019

John E. Black, Jr., Skarzynski Marick & Black LLP
David P. Saunders, Jenner & Block LLP

What are the Core Obligations of the GDPR?

GDPR: 6 Principles + Overarching Principle of "Accountability"



1

Key GDPR Definitions

Broad Definitions of Personal Data and Sensitive Personal Data:

- Personal Data: "Information relating to an ***identified*** **or** ***identifiable*** natural person" through "all means reasonably likely to be used". May include location data or IP addresses.
- Sensitive personal data, such as genetic data, biometric data, racial or ethnic origin and religious beliefs, receives additional protections.
- GDPR does not apply to anonymized data.

Controllers and Processors

- Controller: Person or body that determines purpose and means of processing personal data
- Processor: Person or body that processes data for controller
- Both Controllers and Processors may be subject to liability for non-compliance.

2

What Exposure Does the GDPR Present?

Broad Regulatory Oversight:

Wider investigative and corrective powers, including to conduct on-site data protection audits and issue public warnings, reprimands and specific remediation.

Wide Territorial Scope:

- Applies to Data Subjects in EU or
- Applies to offering of goods or services to, or monitoring behaviour of, Data Subjects in EU.
- **No** requirement that Data Subject be an EU national.
- Therefore, it may affect a U.S. e-commerce company with one U.S. citizen customer living in EU.

3

What Exposure Does the GDPR Present?

Significant Sanctions:

Fines based on prior year revenues of the "undertaking."

- Two categories of fines:
  - ***Up to 20,000,000 Euros or 4% of total worldwide turnover***, whichever is higher, for certain violations such as international transfer restrictions.
  - ***Up to 10,000,000 Euros or 2% of total worldwide turnover***, whichever is higher, for certain violations such as security and data breach notification.

Individual Right to Seek Compensation:

- Any person who has suffered "material or non-material damage" from a breach may seek compensation from controller or processor.
- May also require consumer protection body to bring claims on their behalf, increasing likelihood of group claims for GDPR violations.

4

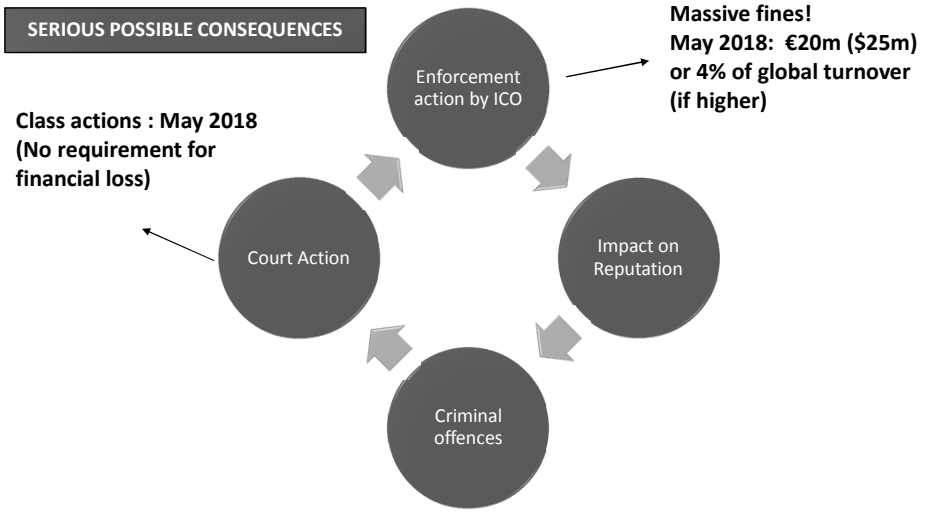
What Exposure Does the GDPR Present?

Data Breach Notification Obligations:

- Controller must notify supervisory authority of breach without undue delay, and if feasible, ***within 72 hours*** of becoming aware. If likely high risk to individual, must notify individuals "without undue delay."
- Processor must notify controller of breach "without undue delay."
- Must describe nature of breach in ***clear*** and ***plain language***
- Notification not required if:
  - implemented and applied appropriate measures (e.g. encryption)
  - subsequent measures ensure high risk no longer likely
  - disproportionate effort (only public communication required)

5

Why Care About the Impact of the GDPR on Privacy?



6

GDPR Fines to Date - 2018

October, 2018

- ***Austria – small, local business – €4,800***

  A local business had a CCTV camera that videotaped public space.

November, 2018

- ***Germany – Knuddels.de (social media / chat platform) – €20,000***

  Knuddels reported a data breach. Upon investigation, local data protection agency determined the site had been storing user passwords in plaintext without hashing. The fine was issued over the data storage practices, not the breach itself.

December, 2018

- ***Portugal – Hospital near Lisbon – €400,000***

  Staff at the hospital used bogus accounts to access patient records.

7

GDPR Fines to Date - 2019

January, 2019:

- ***France – Google – €50,000,000***

  Google was fined for lack of transparency and consent in advertising personalization, including a pre-checked option to personalize ads.

March, 2019:

- ***Poland – A Data Processor – €220,000***

  Data processor fined because it scraped the internet for public contacts for commercial contact with over 90,000 people, 12,000 of whom objected to unauthorized use of their data.

- ***Denmark – Taxa 4X35 (Taxi Company) – 1.2M DKK***

  Following random audit, company was found to have over 9 million personal records it stored but did not need. Fined for failing to delete unused contact information.

8

What is Usually Covered by Cyber Insurance?

First Party Coverages	
Personal Information breach remediation and notification:	Cost to respond to breach, including forensic and legal investigation, legally required breach notification, credit monitoring, call centers and public relations.
Digital asset replacement:	Cost to replace, restore or re-collect digital assets corrupted or destroyed by a security breach.
Extortion costs and rewards:	Expenses and ransom and reward payments to resolve a credible extortion threat to: ▪ launch or continue a computer security attack on insured; ▪ release or improperly use personal or confidential corporate information held by insurers.
Business Interruption loss:	▪ Lost net income and extra expenses due to interruption in service of computer system due to security breach or attack. ▪ Some insurers offer contingent/dependent business income loss.
Other coverages:	▪ Social engineering fraud loss ▪ Telecommunications hacking

9

What is Usually Covered by Cyber Insurance?

Third Party Coverages	
Personal data breach liability:	Defense costs, settlements and judgments from civil suits (other than regulators) for failing to prevent unauthorized use, access or disclosure of protected personal or confidential information or for violating privacy laws protecting personal information.
Regulatory proceeding liability:	Defense costs from regulatory agency investigations or proceedings arising from privacy breach. Some policies also cover fines, penalties and consumer redress funds.
Security and privacy liability:	Defense costs, settlements and judgments from civil suits for failing to prevent, virus attacks, denial of service or transmission of malware.
Multimedia Insurance:	Defense costs, settlements and judgments from civil suits over online and offline media content, including copyright/trademark infringement, libel/slander and personal injury.
Other coverages:	▪ Technology professional services. ▪ PCI DSS fines and costs

10

What are Possible Limitations of Cyber Insurance?

- No Coverage for Loss of Customers
- Limited Coverage for Loss of Brand Equity
- No Coverage for the Loss of Intellectual Property
- Potential Coverage Gaps with Standard Lines Policies
- Possible Limitations on Coverage for GDPR Fines
- Other Limitations on GDPR Coverage

11

California Consumer Protection Act of 2018 v. GDPR

Topic	GDPR	CCPA
Territorial Scope	Extraterritorial	Extraterritorial
Applicability	Controllers/Processors	Businesses/Service Providers
Internal Data Processing Limits	Significant	None
Lawful basis for use	6 lawful bases	No similar provisions
Opt out of data sale	None	Opt-in and opt/out
Enforcement	Designated DPAs	California AG, possible private right of action

- Differences as to what constitutes personal data
- No "Sensitive Data" regime under CCPA

13

California Consumer Protection Act of 2018

- Scheduled to enter into force on January 1, 2020.
- California Attorney General required to publish regulations between January 1, 2020 and July 1, 2020.
- Attorney General may not bring enforcement actions until the earlier of six months after the publication of final regulations or July 1, 2020.

14

California Consumer Protection Act of 2018 (Cont.)

Applies to for-profit businesses doing business in California and which:

(1) Have annual gross revenues over $25 million;

(2) Annually receive, sell, or share for commercial purposes personal information of more than 50,000 California consumers, households, or devices; or

(3) Derives 50 percent or more of annual revenue from selling California consumers' personal information.

Exclusion for de-identified or aggregated information, publically available information, and information regulated by federal statutes (e.g., HIPAA, GLBA, DPPA, FCRA).

15

California Consumer Protection Act of 2018 (Cont.)

- Business outside of CA who have revenues from customers in CA or provide products or service to customers in CA.
  - For example, a Japanese company, which provides goods or services to residents of CA.
- Any entity that controls or is controlled by a business who is subject to CCPA.
- Any entity that shares common branding with a business who is subject to CCPA.
  - Shared name, servicemark, or trademark.

16

Personal Information under the CCPA

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.

"Consumer" means CA residents.

Publicly available information is not personal information.

Includes, among others: IP address, cookie identifier, geolocation data, browsing history, search history, audio, electronic, visual , thermal, olfactory, or similar information.

17

California Consumer Protection Act of 2018 (Cont.)

- Notice to consumers re: information collected and purpose.
- Provide consumers with opt-out to business selling their information to third parties.
  - Affirmative opt-in for PII of individuals under the age of 16.
- Provide reports to consumers upon request as to what company is doing with consumers PII, including providing a right of access to the PII to the consumer.
- Delete consumer PII upon request.

18

California Consumer Protection Act of 2018 (Cont.)

A business that collects PII is required disclose the following information in its privacy policy:

- The categories of PII it has collected about that consumer in the preceding 12 months.
- The categories of sources from which the PI is collected.
- The business or commercial purpose for collecting or selling PII.
- The categories of third parties with whom the business shares PII.
- The specific pieces of PII the business has collected about that consumer.
- A description of a consumer's rights to disclose and not to be discriminated, financial incentives, and one or more designated methods for submitting requests.

19

California Consumer Protection Act of 2018 (Cont.)

If the business sells the consumer's PII or discloses it for a business purpose, the business is also required to disclose the following:

- The categories of PII it has sold in the preceding 12 months.
- The categories of PII that the business disclosed for a business purpose in the preceding 12 months.

Privacy policy needs to be updated at least once every 12 months.

20

California Consumer Protection Act of 2018 (Cont.)

Make available to consumers two or more designated methods for submitting requests for information required to be disclosed.

- At a minimum, a toll-free telephone number
- If the business maintains an Internet Web site, a Web site address.

The business is required to disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer.

If the business does not take action on the request of the consumer, the business needs to inform the consumer of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

21

California Consumer Protection Act of 2018 (Cont.)

Private right of action (individual or civil class action) for data breaches.

- May result in statutory damages between $100 and $750 for each California resident and incident *or* actual damages, whichever is deemed proper by the court.

Enforcement actions by California Attorney General.

- Civil actions may result in penalties of up to $2,500 per violation (not cured within 30 days) or up to $7,500 per intentional violation.

22

Cybersecurity Checklist

- ☑ Know what personal data your company collects and where it is stored
- ☑ Know with whom you share your data and for what purpose
- ☑ Use two-factor authentication methods where possible
- ☑ If you are using the cloud, make sure you know who can access your data
- ☑ Have a process for eliminating access for former employees
- ☑ Have a written data incident response plan
- ☑ Training, Training, Training
- ☑ Establish password policies

23

Questions?