GDPR : ONE YEAR LATER

Everyone needs a trusted advisor. Who’s yours?
Rex Johnson, CISSPP, CISA, CIPT, PMP, PCIP, QSA

Director | IT Risk Services | BKD Cyber

- Over 25 years experience
- Cybersecurity governance & technical assessments
- Compliance (FFIEC, PCI, NIST, ISO)
- Help companies build or enhance cybersecurity programs
- Information & Operational Technology environments
- Retired Army Lieutenant Colonel
How has GDPR impacted your business?
Quick Recap

• General Data Protection Regulation (GDPR)

• Replaces the European Data Protection Directive, which was created in 1995

• Impacts organizations that collect & process personal data of EU data subjects

• Penalties of up to 20M € ($22.6M) or 4% of organization’s annual global turnover, whichever is higher

• Data subjects can claim compensation for damages from breaches to their personal data – which is complaint driven

• Went into effect May 25, 2018
GDPR Data Subject Rights

- **Access to data** – data subject must have access to the data that is provided to controllers/processors
- **Right to object** – challenge the legitimacy of collection of certain data
- **Correct errors & omissions** – have the right to have their data corrected
- **Restrict processing (consent)**
- **Data portability** – allow data subject to transfer their data to another data controller, e.g., a data subject should be able to transfer his/her personal data/profile from one health care provider to the other
- **Erasure** – can request their personal data be erased from controller’s database
What Has Happened Since…

• The IAPP hosted a retrospective panel in London mid-March
• More than 200,000 reported cases in the 31 countries
• 91 fines totaling €56M ($63.4M) were enforced; involving 11 countries
  • The highest fine so far is €50M, made against Google who is appealing
• Has been praised as a successful breach notification law

Sources: https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html
https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/
European Data Protection Board

- EDPR issued a report for the first 9 months
- Realized it is a massive effort to manage
- The member countries have a willingness to cooperate

Source: EDPR Report 2/25/2019
The missing information from some LEA countries SAs is due to the short timeframe to collect data and cannot be interpreted as they do not need additional resources.
Takeaways from EDPR Report

• GDPR enforcement led to extra workloads, additional time dealing with cases & has an impact on the budget of the regulators

• Still trying to figure out **One-Stop-Shop**. *The handling of cross border cases takes time*

• SA believe the workload is manageable for the moment

• Many in the EU want to consider this a transition year

Source: EDPR Report 2/25/2019
Polling Question

Which of the following is NOT true regarding GDPR:

a) There have been more than 200k cases in the EU
b) Over €50M in fines have been enforced
c) There is significant resistance in the EU over cross-border cooperation
d) It has had an impact on breach notifications
Which of the following is NOT true regarding GDPR:

a) There have been more than 200k cases in the EU
b) Over €50M in fines have been enforced

c) There is significant resistance in the EU over cross-border cooperation

d) It has had an impact on breach notifications
So, what does that mean to us*?

* us = U.S.
Impacts of GDPR

• Developed to strengthen & standardize data privacy protections
• Brought to a global stage the question of individual privacy
• Is bringing data breaches more to the forefront than before
• Created reluctance of venture capitalist firms to invest in startups impacted by GDPR
• Created reduction in online ad revenues
• Brought potential slowing of digital transformation

Privacy in the U.S.

• U.S. states are becoming more active in data protection & privacy

• Current privacy laws:
  • California
  • Vermont
  • Colorado
  • New Jersey

• All 50 states have enacted data breach notice laws

California Consumer Privacy Act (CCPA)

• Signed into law June 28, 2018; goes into effect January 1, 2020
• Grants consumers new rights in the collection of personal information
• Allows California consumer to see data a company has on them
• Applies to companies that
  • Have more than $25M in annual revenue
  • Have personal data on at least 50,000 people
  • Collect more than half of their revenue from the sale of personal data.
• Applies to more than the state of California, & even the U.S.

Sources: https://oag.ca.gov/privacy/ccpa
Colorado House Bill 1128

• Went into effect September 1, 2018
• Requires businesses that maintain personal information on Colorado residents to maintain “reasonable” security practices
  • Appropriately dispose of data
  • Protection of data when transferred to third parties
  • Notification of breaches within 30 days
  • Designation of a responsible individual (DPO)
  • Develop & maintain a DR plan & BCP, tested annually

Source: https://www.americanbanker.com/list/the-states-at-the-forefront-of-consumer-privacy-legislation
Colorado House Bill 1128

- Defines personal information as a combination of a resident’s first name or initial & last name with
  - Social security number
  - Student, military, or passport ID number
  - Driver’s license or identification card number
  - Medical information
  - Health insurance identification number
  - Biometric data

Vermont House Bill H.764

• Passed into law May 2018 to be enacted in January 2019
• Data brokers must register with the State’s AG
• Four mechanisms
  • **Transparency**: Annual registration & discloses whether consumers may opt-out, and # of breaches
  • **Duty to Secure Data**: Administrative, technical & physical safeguards
  • **No Fraudulent Collection**: Nor for purposes of harassment or discrimination
  • **Free Credit Freezes**: Consumer can lock their credit file

New Jersey Senate Bill No. 1913

• Personal Information and Privacy Protection Act

• In 2017, bill passed to limit a merchant’s ability to collect information about shoppers
  • Only used to verify identity
  • Store data securely

• May not share data with third party unless they disclose their data-sharing practices

New York Bill S00224

• “Right to Know Act of 2019”

• Consumer’s information that is being collected

• How that information is being disclosed to third parties

• Names & contact information of those third parties

Washington State Bill SB 5376

• “Washington Privacy Act”

• Confirm & provide access to the data

• Correct inaccurate data

• Delete data once no longer necessary to maintain

• Right to object processing related to direct marketing
Polling Question

What are impacts of GDPR & Data Privacy in the U.S.?

a) Every state has implemented data privacy laws
b) Breach notification laws are in all 50 states
c) The U.S. has no interest in data privacy & will not impose this
d) All of the above
Polling Question

What are impacts of GDPR & Data Privacy in the U.S.?

a) Every state has implemented data privacy laws
b) Breach notification laws are in all 50 states
c) The U.S. has no interest in data privacy & will not impose this
d) All of the above
So, now what?

The subject of privacy is not going away!
Case Study: Facebook & Privacy

2006
- Beacon, Ad Privacy
  - Purchase notifications shared without consent.
  - FB provided Opt-Out also talking with FTC on online privacy & advertising

2007
- FTC Settlement
  - Third-party apps had access to all personal data of user.
  - FB agrees to undergo biannual independent privacy evaluation

2011
- Facebook Bug
  - White Hat hacker found bug that exposed email & phone numbers of 6M users to anyone who had some connection to the person

2013
- App Restriction
  - FB cut off apps from taking all data & limited access of developers.
  - Did not stop previously downloaded data.
  - Cambridge Analytica ban

2015
- GDPR, Belgian, & Data Theft
  - FB released privacy principles to users on how to control their data.
  - Belgian court ordered to stop collecting data from its citizens & delete existing data.
  - FB faced pressure on massive data theft.
  - Developing tool for users to see what apps have access to their data

FB News Feed
- Not all users happy with details of personal life being blasted into daily feeds

Website Compliance

The following are recommendations for website developers:

• Include description of what the user is signing up for

• Ensure all forms & other data collection methods on websites are explicitly opt-in (*note: a tick-box must not be pre-ticked*)

• Make it easy for users to opt-out or unsubscribe

• Add cookie alert banner

• Update privacy policy/terms & conditions to reference GDPR or relevant privacy terminology

Source: https://www.cmdsonline.com/blog/the-looking-glass/gdpr-us-websites/
Cookies

• Make transparent, providing clear & specific information about data types & purpose

• Appear prior to any processing other than the strictly necessary takes place, also known as “prior consent”

• Position them as an affirmative, positive action

• Document them; securely stored as evidence that consent has been given

• Allow users to withdraw consent whenever they want

• Review & renew them regularly (the ePrivacy directive suggests once a year)

http://www.spryideas.com/blog/gdpr-affect-business/
Considerations for GDPR & Other Privacy

- Establish privacy policies & procedures
  - Data classification
  - Data disposal
  - Data privacy
  - Data storage

- Identify personal data types & digital data types with your organization

- Understand IT systems, files & databases that process & store personal information

- Map personal data to the business functions which collect, process & store it

- Dedicate a Data Protection Office (DPO)
Considerations for GDPR & Other Privacy

- Develop & annually test the Incident Response plan
- Consider how-to processes & respond to data requests from customers
- What third-party vendors process personal data on behalf of your organization or customers?
- What type of data transfer agreements are required?
Polling Question

What is a core element of data privacy?

a) Giving a user the right to know how information is being used
b) The ability to provide consent (opt-in)
c) Disposal of personal data when no longer needed
d) All of the above
Polling Question

What is a core element of data privacy?

a) Giving a user the right to know how information is being used
b) The ability to provide consent (opt-in)
c) Disposal of personal data when no longer needed
d) All of the above
“You have zero privacy anyway…Get over it.”

- Scott McNealy, former CEO of Sun Microsystems circa 1999

A lot has changed in the past 20 years.
Summary

• Concerns over data privacy are not diminishing
• GDPR has brought this to the forefront
• Breach awareness & notification are rising
• U.S. States are implementing privacy laws
• Organizations need to consider how they will address the subject of data privacy
How We React to Change

1. “Anything that is in the world when you’re born is normal and ordinary and is just a natural part of the way the world works.

2. Anything that's invented between when you’re 15 and 35 is new and exciting and revolutionary and you can probably get a career in it.

3. Anything invented after you're 35 is against the natural order of things.”


Questions?
Thank You!

bkd.com | @BKDCyber  @RexSecurity