# Lessons Learned After One Year of GDPR

Justin P. Webb, CIPP/US
Co-Chair, Data Privacy & Cybersecurity, CISO
FIRMA 2019 Orlando Conference

# THE GDPR PANIC HAS SUBSIDED!

- In the run up to May 25, 2018, there was:
  - Misinformation about GDPR applicability
  - Late attempts at compliance
    - Client – “Can you make me GDPR compliant by tomorrow?”
    - Me – “It’s good to dream big.”
  - Widespread use of privacy policies copied from other sites, without proper vetting
  - Misunderstanding of GDPR requirements due to:
    - Lack of regulatory guidance
    - Nervous privacy professionals

# GDPR Basics – Overview

- Became effective May 25, 2018
- Gives individuals (Data Subjects) rights over their information
- Protects personal data
  - Any information relating to an identified or identifiable natural person
- Fines up to 4% of global turnover
- Extra-territorial applicability (*i.e.* applies to US and other non-EU entities)
- 72 hours to notify a supervisory authority of a data breach
- Required notification rights
- Contracting requirements between Controllers and Processors
  - Data processing agreements
- Cannot transfer data between E.U. and U.S. without meeting certain requirements
  - Standard contractual clauses
- Requires legal basis for processing

# GDPR Basics
# Extraterritorial Applicability

| Established in the EU | Offering Goods or Services in the EU | Monitoring of Data Subjects in the EU |
|---|---|---|
| • A company with an office in the Paris<br>• A hosting provider located in Ireland<br>• Sales representatives located in Germany | • A US company that sells widgets to people in France through its online store that is provided in French and accepts Euros | • Canadian company that tracks the online behavior of people in Ireland<br>• A US technology company with an app that provides restaurant recommendations to people in Italy based on their geo-location |

# GDPR Basics – Relationships

- It's all about Controllers and Processors
  - Critical to understand the relationship between the parties
  - Who is the Controller?
    - The party that has ultimate say over the use of the data
  - Who is the Processor?
    - The party who acts only at the direction of the controller
  - Can be Controller-Controller relationships
  - Typical relationship is Controller-Processor
    - Example

# GDPR Basics
# Data Subject Rights

- GDPR provides Data Subjects with rights:
  - Right of Access
  - Right to Rectification (Correction)
  - Right of Erasure (the “Right to be Forgotten”)
  - Right of Data Portability
  - Right of Restricted Processing
    - Only use information for limited purposes
  - Right to Lodge a Complaint

# GDPR Basics
# Data Subject Rights (cont'd)

- Data Subject rights, operationally
  - Entities should have a process to deal with requests by data subjects to exercise their rights
  - Must respond within 30 days, unless extension is necessary
  - Must answer Data Subject request from any medium
  - Must vet the Data Subject
    - This allows companies to slow down the process
  - Are there ways to achieve the data subject request, without causing operational difficulties?
  - Is there a valid exception to the right?

# GDPR Basics – Lawful Basis

- Cannot process “Personal Data” without a lawful basis, including:
  - Consent
    - Over-reliance on consent caused early GDPR problems (more on that)
  - Necessary for pre-contractual or contractual purposes
  - Legal obligation (*i.e.*, AML/KYC)
  - Legitimate interest
    - The “squishiest” basis
    - Typically the preference for processing

# GDPR Basics – Notice & Consent

- Notice and consent regime
  - Where consent is necessary, must provide, clear, concise, transparent notice (cannot be layered, or multi-part)
  - Describe what you are going to do with the data
  - Who you will share it with, and for what purpose
  - Whether data will be transferred outside the country
  - How long you will retain data
  - Inform Data Subjects of their rights

# GDPR Basics – DPAs

- Data Processing Agreements
  - Any sharing of Personal Data under GDPR requires written contractual terms between the parties, pursuant to Article 28(3), with various specific requirements
  - Operationally, this is where companies have seen a lot of the GDPR legwork
  - Up to May 25, 2018, companies were rushing out with DPAs
    - Since then, companies have been revising those DPAs to modify the risk allocation between the parties, especially the allocation of risk related to GDPR fines

# One Year Into GDPR

- Partial compliance is still the norm, outside the EU (and in the EU to some extent)
- Continued focus on progress, not perfection
- Regulators have taken a soft hand to fines, and want to see progress
- Regulators have closed a lot of data breach cases
- Surveys show data breach over-reporting (more on that later)

Photo credit to http://career-intelligence.com/networking-target-company/

# One Year Into GDPR (cont'd)

- EU regulators are **still** putting out guidance – so metes and bounds of law are unclear
- Some supervisory authorities are not yet fully up and running, or are short staffed
- As of September 2018, a survey by Talend reported 70% of surveyed businesses could not address a data subject request in one month
- Large global companies with large breaches are getting EU regulators' attention
  - Facebook
  - Google
  - British Airways

Photo credit to http://career-intelligence.com/networking-target-company/

# How are companies approaching the GDPR?

- Risk-based approach
  - Common with all clients
  - Implementing compliance for impacted company sectors or specific data
  - Many publicly traded companies still working toward entity-wide compliance
- Some mid-market companies are electing to purge EU data and block European IP addresses or block cookies for those addresses
  - *E.g.*, Los Angeles Times
- Even for entities not subject to the GDPR, legally, obligations arise under contract with E.U. or U.S. entities subject to the GDPR

# Mistakes So Far: Consent

- Many companies mistakenly rely on consent as their legal basis for processing, because of misunderstandings regarding “legitimate interest” basis for processing
- Should not use consent if there is another basis; if the documented basis is consent then a data subject may revoke his/her consent and this could cause process or business impact if the data is required
- Legitimate interests include:
  - Processing pursuant to contract
  - Legal obligations
  - Some marketing
  - Anything else that would be reasonably asserted as a legitimate interest, based on a balancing of the company’s interests vs. the Data Subject’s interests

# Mistakes So Far: Misunderstanding GDPR vs. Data Transfer

- To transfer data outside the EU, need a valid “transfer mechanism”
- Companies misunderstood Privacy Shield vs. GDPR compliance
- Valid Transfer Mechanisms
  - Standard Contractual Clauses (Most Common)
  - EU-US Privacy Shield Program
  - Binding Corporate Rules
- Member of Privacy Shield ≠ GDPR Compliance

# GDPR Breach Stats & Thoughts

- From May 25, 2018, to January 28, 2019, the European Commission reported 41,502 data breach notifications so far
- DLA Piper Report from Feb. 2019 put the number at 59,430
- Breach reporting includes:
  - Minor errors like emails to wrong recipient
  - Major problems like global hacking incidents involving Data Subjects internationally
- Companies and regulators still attempting to strike a proper balance between breach over-reporting, and failing to meet regulatory obligations
- When does a company become “aware” of a breach?

# Enforcement So Far

- To date, 91 reported fines have been imposed under GDPR
  - Source: DLA Piper Data Breach Survey Feb. 2019
- Highest fine imposed to date: 50M Euros
  - Against Google for processing of personal data for advertising purposes without authorization
- “The majority of fines are relatively low in value”
  - This is inconsistent with much of the GDPR hysteria
- GDPR regulators have a significant backlog of reports, so “we expect that 2019 will see more fines for tens and potentially even hundreds of millions of euros as regulators address the backlog”

# Fine Examples and Regulatory Guidance

- One of the first fines under GDPR involved breach of social media platform that compromised 330K records
  - Fined **only 20,000 euros**
  - Low fine because the organization “made demonstrable efforts to proactively notify” the German DPA and customers in due time
  - Also, company engaged in “exemplary cooperation” with the DPA to implement changes, and to provide information to regulator
- Take-Home Message:
  - Notify early
  - Cooperate fully (unless there is reason not to)

# Fine Examples and Regulatory Guidance

- Google's 50M Euro Fine
  - Failed to obtain valid consent to obtain and process data because required disclosures (*i.e.,* essential information under GDPR) were split up between multiple documents and privacy policies, violating various GDPR principles including notice and transparency
  - Used "blanket consent" rather than granular, freely given, informed, and unambiguous consent through affirmative action
  - Had "pre-ticked" or opt-out signups
- Take-Home Message:
  - Must take consent seriously
  - Must have true opt-in consent that is not over inclusive
  - Must get rid of pre-ticked boxes
  - Ensure that privacy policy is clear and conspicuous, and easy to understand and read

# Fine Examples and Regulatory Guidance

- AggregateIQ – First Extraterritorial Fine
  - UK's ICO fined Aggregate IQ for activities related to Brexit
  - Accused Candian Company of using Personal Data – names and email addresses – of UK individuals to target them with political advertising messages on social media
  - Did so "in a way that the data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for that processing"
- Take-Home Message:
  - EU regulators are willing to fine entities wholly outside of the EU
  - But, it is likely to require significant interactions with the EU
  - Ensure that if you obtain Personal Data from third parties, you obtain representations and warranties regarding the lawfulness of the data and proper notice & consent

# Fine Examples and Regulatory Guidance

- Most important regulatory guidance since May 25, 2018:
  - Guidelines 3/2018 on Territorial Scope of the GDPR
- In November 2018, finally received EDPB guidance on how and when GDPR applies outside the EU
  - Take-Home Message:
    - Need more than random EU individuals accessing a website
    - Need targeting of EU individuals, through various means or modalities
    - Tangential relationships to EU are insufficient
    - High-exposure area of website tracking likely requires something more like targeting, as well
    - GDPR does not apply to everyone

# What does the future hold?

- GDPR has influenced legislation internationally and in the US
- US Legislation
  - CCPA
  - Washington Privacy Act
- Companies should be focused on building out a comprehensive privacy program, regardless of GDPR or CCPA applicability
- Expect more and higher fines from DPAs as they staff up
- Expect more consumers exercising Data Subject rights, as more laws providing those rights materialize
- Watch for a Federal Privacy Law
  - Preemption?

GODFREY & KAHN S.C.

MILWAUKEE | MADISON | WAUKESHA | GREEN BAY | APPLETON | WASHINGTON, D.C.

# Thank You


Justin P. Webb, CIPP/US

414.287.9527
jwebb@gklaw.com