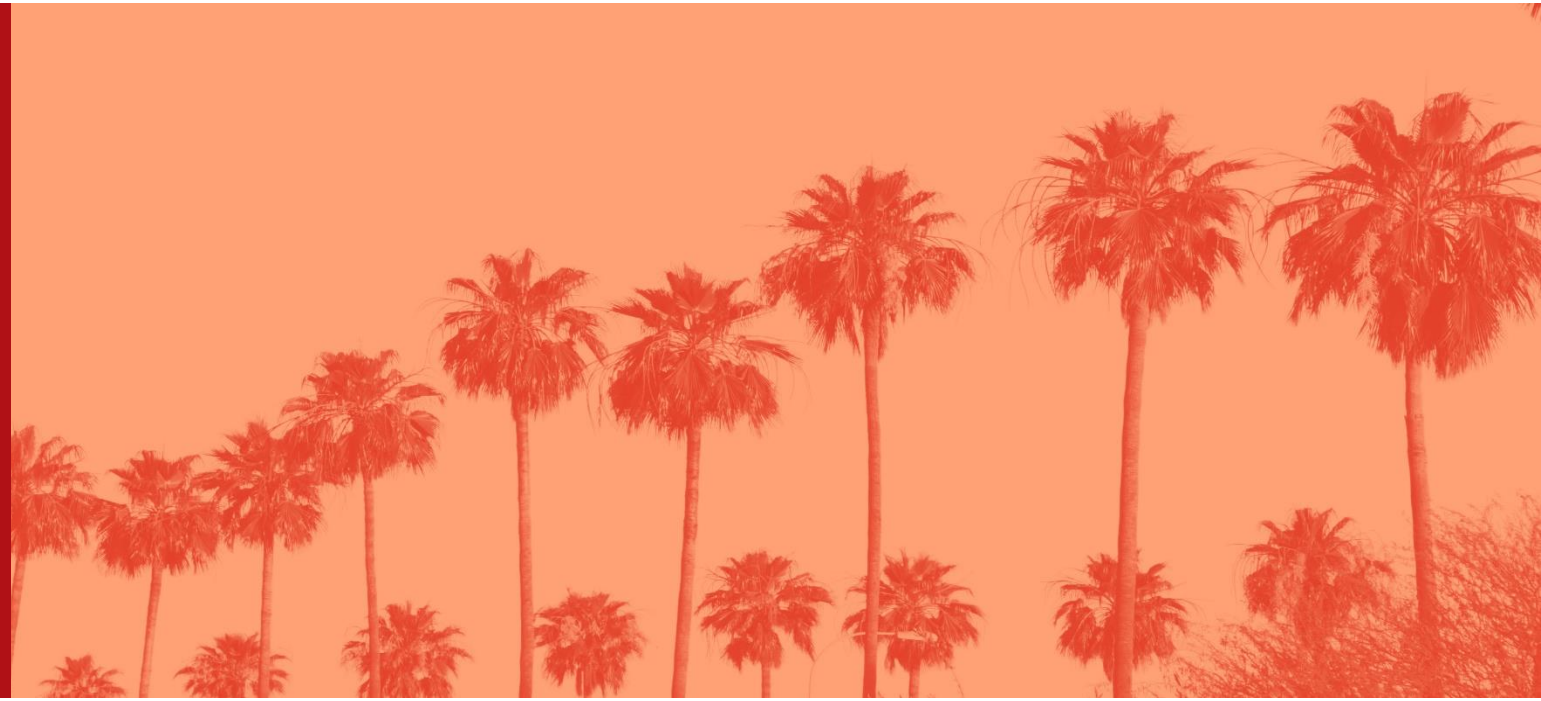
LOOKING AHEAD

> **Risa B. Boerner** (CIPP/US) – Fisher Phillips, Philadelphia

> **Danielle Urban** (CIPP/E) - Fisher Phillips, Denver



2019 FISHER PHILLIPS INSIDE COUNSEL CONFERENCE

MARCH 6-8 | SCOTTSDALE, AZ

The Future of Data Security for Employers

Overview

- Global trends in data privacy
- General Data Protection Regulation (GDPR) – overview and update
- Other recent international data privacy laws enacted/amended
- California Consumer Protection Act (CCPA)
- Anticipated trends in U.S. data privacy laws and regulations in 2019 and beyond

Global Trends in Data Privacy

- Focus on individual rights to control collection and dissemination of personal data
- Expansion of protection to data exceeding scope of "PII" in most U.S. data breach notification laws
- Implementation of controls and regulations on manner in which data is collected, stored, used, maintained
- Emphasis on notice/consent to collection and use of personal data

Global Trends in Data Privacy

- Data privacy regulation in the United States is piecemeal and lagging behind many other countries (the California Consumer Privacy Act, set to go into effect January 1, 2020 is a notable exception)
- In addition to the General Data Protection Regulation (GDPR), which went into effect May 25, 2018, several other countries have their own data protection regulations
- China, India, Mexico, Canada are just a few examples

Practical Implications:
The Big Picture for Multi-National Employers

- Applicant data
- Employee data
- Compensation data
- Race, gender, age, ethnicity
- Diversity
- Home address and family
- Raises
- Starting compensation
- Performance management

International Privacy Challenges

- Complex international data privacy and general laws affecting employers
- Stricter and broader global laws
- Extraterritorial application
- HR databases and processes
- Enforcement and penalties

Other International Employee Privacy Issues

- Varying privacy protections in different countries and regions
- Constitutional guarantees for private employees
- Facebook and other social media
- Background checks; use of criminal conviction information
- Substance abuse testing
- Medical tests
- Pre-employment inquiries

GDPR – The Big Picture

- (Potentially) Massive fines (4% of global revenue or 20 million Euros, whichever is bigger, worst case
- Extra-territoriality – Covers any company doing business in the EEA
- Explicit consent – Opt IN not opt OUT, can be withdrawn at any time
- Right to access your data
- Right to a copy of your data in an interchangeable format

GDPR – The Big Picture

- Breach notification – within 72 hours
- Privacy by design
- Right to be forgotten – applies to third parties you share with
- (Maybe) Requires that you have a data protection officer:
  - DPO cannot be held personally liable
- Not clear what will happen in Britain after Brexit

GDPR – Get Expert Advice

- The effective date for compliance WAS May 25, 2018
- EU Authorities are following up on thousands of complaints:
  - Anyone can file a complaint with a supervisory authority
  - Who may coordinate with other country's SAs
- Some small number of fines have already been issued
- Austria alone has 115 investigations in the pipeline
- Expert advice is recommended

GDPR IN NUMBERS

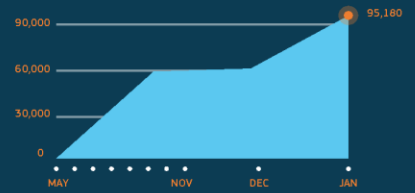
The General Data protection Regulation (GDPR) applies since 25 May 2018. Reports of massive data breaches and the mishandling of personal data by, large online platforms remind us what is at stake: from preserving our private life to protecting the functioning of our democracies and ensuring the sustainability of our increasingly data-driven economy.

On the occasion of Data Protection Day we take a close look at compliance, enforcement and awareness of the new rules.

COMPLYING WITH THE RULES

Number of complaints to Data Protection Authorities (DPAs) under the GDPR*

Complaints can come from any individual who believe their rights under GDPR have been violated, but the GDPR also introduced the possibility for an organisation mandated by individuals to introduce such complaints. This possibility has been used immediately after the entry into application of the GDPR.



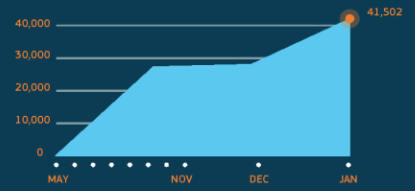
Accumulated number over time.**
From all data protection authorities in Europe.

Most common type of complaints*

These are the activities in which most complaints have been reported so far.

Number of data breach notifications*

When personal data for which a company is responsible is accidentally or unlawfully disclosed, that company is obliged to report this data breach to their national DPA within 72 hours after finding out about the breach.

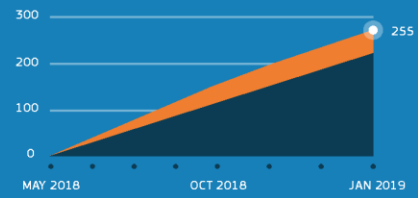


Accumulated number over time.**
From all data protection authorities in Europe.

ENFORCING THE RULES

Cross-border cases*

Many companies, such as social media platforms, provide their services in more than one EU country. The GDPR provides that in most cases one national data protection authority takes the lead to investigate a case process ("one-stop shop"), while the other concerned authorities support the investigation. If there is a disagreement between authorities, the European Data Protection Board will arbitrate.



- Investigations initiated by Data Protection Authorities.
- Investigations by Data Protection Authorities on the basis of individual complaints.

Fines issued under GDPR*

Several high level cases are ongoing and could cause fines up to 4 % of the annual of a business, if there is a serious infringement. So far three fines have been issued.

- A social network operator for failing to secure users' data **EUR 20,000**
- Sports betting café for unlawful video surveillance **EUR 5,280**
- Google for lack of consent on Ads **EUR 50,000,000**

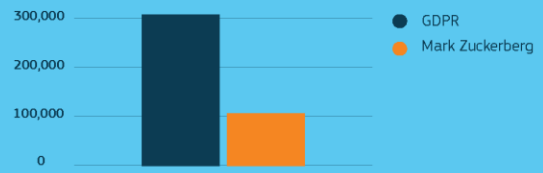
Adaptation of the national laws in the Member States

Being an EU Regulation the GDPR is directly applicable in all EU countries. However, it also requires countries to adapt their national legislation. Whilst 23 Member States have adopted the required national legislation, five are still in the process of doing so (Bulgaria, Greece, Slovenia, Portugal, Czechia).

AWARENESS OF THE RULES

Media coverage

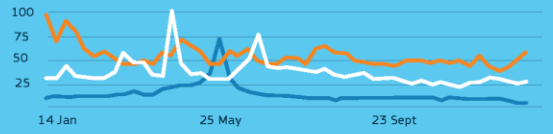
GDPR received a lot of attention in **2018**. So much than even some celebrities had to stand in its shadow.



Annual worldwide mentions in the media
Source: Factiva

Google searches

During the peak month of May 2018 GDPR was searched more often on Google than American superstars Beyoncé and Kim Kardashian.



Interest rated between 0-100, based on number of searches on Google.
Source: Google trends

European Commission

europa.eu/dataprotection

***Source:** The European Data Protection Board.

****Disclaimer:** We were not able to verify if all the reported figures relate to cases post 25 May, when GDPR entered into application. Some of them can also relate to the former data protection directive.

Source: European Commission 25 January 2019

Principles

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Use limited to the purpose it was collected
- Accurate and, if needed, kept up to date
- Kept only for as long as needed for the purpose collected
- Processed with appropriate security including:
  - Confidentiality, Integrity and Availability

Legal Issues

- Fines of up to 4% of revenue for willful neglect or 2% in other cases (or 20 mil €s/ 10 mil €s, whichever is greater)
- Covers countries outside the 31 countries of the EEA
- Burden of proof is now on businesses not victims
- New requirements for privacy notices which must be clear and conspicuous
- Consent must be freely given and can be withdrawn at any time

Technical Issues

- Must report breaches within 72 hours
  - Must understand who and what happened
- Encryption is a get out of jail free card (sort of)
  - Can't be weak encryption
  - No exemption if means to decrypt stolen also
    - As would be the case with malware acting as an authenticated user
- Users can opt out of online profiling
  - Automated profiling illegal in many cases
  - Not just for web sites
- Privacy by Design is legally required

Technical Issues

Data Protection Impact Assessment (DPIA)

- New requirement to ensure that companies document the privacy issues associated new uses of data
  - Systems and paper

Legal + Technical Issues

Data Inventories

- What data do you have
- Where do you have it
- Including shared with third parties
- Only used for pre-consented purposes
- New purposes require new consent
- MUST BE MAINTAINED

Legal + Technical Issues

Right to be Forgotten

- With limited exceptions
  - Companies must cease all processing and
  - Delete all data
  - On a data subject
- A variant of this is the right to request cease processing
- Ties back to data inventory
- And business processes

Legal + Technical Issues

Right to Know What Information You Have

- Must know what data you have about a data subject
- Including where it is located
- Have limited time to produce the data
- How to deliver it is not clear
- Does it include, for example, recordings of customer service calls
- Tied to next requirement

Legal + Technical Issues

Right to a Copy of Data That You Hold

- Called data portability
- In electronic format
- Designed for data exchange:
  - For example, with a competitor of yours
- Google, Microsoft, Facebook and Twitter PARTNER on new data interchange format

  https://www.theverge.com/2018/7/20/17589246/data-transfer-project-google-facebook-microsoft-twitter

Legal + Technical Issues

Expanded Definition of Personal Data

- Added the concept of pseudo anonymous data
- But that is a very slippery slope:
  - Can you ensure that it cannot be reversed?
- Personal data may include a person's IP address(es)
- "'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject')."

Breach Reporting

- Event leading to the destruction, alteration, unauthorized disclosure or access to personal data
- Must notify the SA within 72 hours unless breach is unlikely to result in a risk to the rights and freedoms of the data subject
- Must notify data subjects "without undue delay" if data breach is likely to result in a ***high*** risk to their rights and freedoms
- The UK ICO has seen an 800% increase in reporting
- 2/3rds of which they consider legit (some over reporting)

Transfer of Data to Other Countries

GDPR restricts transfer of data outside of the EEA unless:

- The commission says that other countries have adequate level of protections
- Or there are adequate safeguards (US Privacy Shield)
  - Privacy Shield is the subject of several lawsuits at the CJEU and to be reviewed soon by the EC – stay tuned

Canada: Personal Information Protection and Electronics Documents Act (PIPEDA)

- 2001: Regulates collection, use, disclosure and management of personal information by organizations that recognizes privacy. Originally applied only to Federal sector and private entities selling personal information across Provincial or country boundaries.
- 2004: Applies to all private organizations unless covered by specific Provincial laws (such as Alberta, British Columbia and Quebec). Personal information broadly defined: (ex: performance, salary, seniority, marital status, religion, race, personal interests)
- 2018: Mandatory data breach notification requirements take effect

Canada: Personal Information Protection and Electronics Documents Act (PIPEDA)

- Personal information may not be collected, used or disclosed without person's consent (unless express exception)
- Organizations: limited to collected information only for reasonable purposes identified at or before time of collection
- Safeguarding privacy of information; access by individuals, inaccuracies corrected; disagreements noted; procedures for people to challenge compliance

Examples of Other Notable International Data Privacy Laws

- Mexico
  - Federal Law for the Protection of Personal Data in Possession of Private Parties (2010)
- India
  - Information Technology Act (2000; Amended 2008)
  - Indian Telegraph Act (consumer privacy)
  - Banking Regulation Act
  - Right to Information Act
  - Health industry laws
  - Citizenship Act (breaches)
  - Draft Data Privacy Bill

Examples of Other Notable International Data Privacy Laws

- China
  - Cyber Security Law – effective June 1, 2017
  - Non-binding guidelines went into effect May 1, 2018
  - Breach notification: 24 hours
- Vietnam (Jan 1, 2019)
  - Store 36 months of local user data in country
  - Bans the usage of social networks to spread false information, create difficulties for authorities or organize anti-state activities
  - Gave Google, Facebook and similar organizations one year to comply

Examples of Other Notable International Data Privacy Laws

- Japan (May 30, 2017)
  - Similar to GDPR in scope but no concept of data controller or data processor
  - Includes publicly available data such as phone numbers and business contacts
- Spain (draft published)
  - Covers what happens to personal data after death and conflicts between heirs, relatives, and spouses
  - Creates concept of digital wall

Other Countries with “Adequate” Protections

The European Commission has so far recognized:

- Andorra
- Canada
- Guernsey
- Israel
- Jersey
- Switzerland
- United States (W/ Privacy Shield)
- Argentina
- Faroe Islands
- Isle of Man
- Japan
- New Zealand
- Uruguay

Other Countries with “Adequate” Protections

- Adequacy talks are ongoing with South Korea
- These adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the "Police Directive" (article 36 of Directive (EU) 2016/680)

CCPA: The Basics

- Signed into law June 28, 2018
- Takes effect January 1, 2020
- Compromise – tech industry and consumer lawyers – to convince Allistair McTaggart to drop ballot initiative
- Rushed through legislature in June

To What Organizations Does the CCPA Apply?

- Entities that have annual gross revenues in excess of $25,000,000 –OR-
- Annually buy, receive, sell, or share for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices -OR-
- Derive 50 percent or more of annual revenues from selling consumers' personal information.

Whose Information is Protected?

All California residents including:

- Customers
- Employees
- Visitors to a company Internet site or building
- Contractors and independent contractors
- Vendors

What is Personal Information?

> "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 of Personal Information

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
- Any categories of personal information described in subdivision (e) of Section 1798.80.
- Characteristics of protected classifications under California or federal law.

Examples of Personal Information

- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

Examples of Personal Information

- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act

But wait . . . there's more

- Personal information also includes inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

What's Not Personal Information?

- "Personal information" does not include publicly available information or information that is lawfully made available from federal, state, or local government records
- As long as it is used in a manner consistent with the purpose for which it was collected

Carve-out for Certain Data and Organizations

- This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the Driver's Privacy Protection Act.
- Does not apply to a provider of health care or another entity governed by HIPAA.

Individual Rights Conferred

- Right to know and access
- Right to deletion
- Right to opt out of sale of personal information
- Right to be free of discrimination (right to equal service and price, even if individual exercises privacy rights)
- Private right of action (limited)

Financial Incentives

- A business may offer financial incentives for the collection, sale, and deletion of personal information.
- Must notify consumers and obtain opt-in consent.
- Must not discriminate against consumers that do not opt-in or who exercise their rights.

Transparency

Businesses will have to inform consumers, at or before the point of collection, of categories of personal information they collect and the business purpose in collecting that information.

- Categories of data
- Categories of sources of data
- Purpose for collecting or selling the data
- What PI was "sold" or disclosed (must be distinguished), for what purpose and to whom
- Specific pieces of personal information the company has collected

Do Not Sell My Data

- A business must provide a clear and conspicuous link on the homepage titled "Do Not Sell My Personal Information," which links to a section of the privacy policy that provides the required disclosures.

Record Keeping

- Need to be able to track:
  - "Do not sell" requests
  - Opt in authorizations (for under 16s)
  - Deletion requests
  - Access (copies) requests

Enforcement

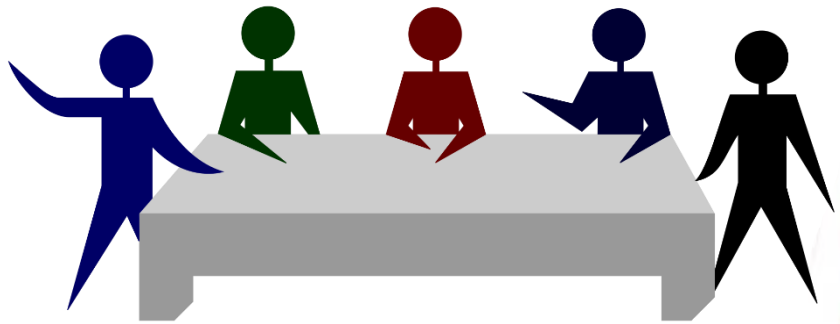
- Consequences for failure to comply include:
  - Civil penalties from an AG action up to $7,500 per violation. Technical amendments before Governor Brown would change to $2,500, only $7,500 for willful.
  - Private right of action in case of a breach up to $750 per record without having to show damages.
  - 30 day right to cure a violation

CCPA v. GDPR: Key Differences

	CCPA	GDPR
Do Not Sell My Information	Button on website	Right to object to processing for marketing purposes but not explicit right to demand that information not be sold
Transparency Requirements	Requires that disclosures distinguish between information sold and information disclosed for business purposes	No such distinction – just requirement to disclose all data sharing of any kind and the purposes for same
Financial Incentives	Permissible as long as not discriminatory	No such concept or allowance for financial incentives for sharing data
Enforcement	AG and private right of action (class actions)	Data Protection Authorities and individual representative actions (e.g., Max Schrems' privacy lobby group None of Your Business)

What Companies Can Do to Prepare for CCPA

- Start planning for implementation by 1/1/2020; enforcement begins July 1, 2020, in some cases sooner (privacy provisions)
- Start budgeting for the implementation
- Update privacy notices
- Identify personal information in the company's possession and create strategies for complying with consumer requests
- Non-Discrimination: review practices to ensure compliance



Anticipated Trends in Data Protection in 2019 and Beyond

- U.S. federal data privacy legislation:
  - The "Data Care Act"
  - Tech industry lobbying for uniform federal regulations (Google, Facebook, Microsoft, etc.)
- Continued expansion of existing U.S. state data breach notification laws
- Ongoing focus on notice/consent to collection and use of personal data
- Greater regulation of security measures to safeguard personal information

FINAL QUESTIONS

Fisher Phillips

Inside Counsel Conference 2019

Fisher Phillips

Inside Counsel Conference 2019

THANK YOU

FOR JOINING US

Risa B. Boerner (CIPP/US)
rboerner@fisherphillips.com
610.230.2132
Radnor, PA

Danielle Urban (CIPP/E)
durban@fisherphillips.com
303.218.3650
Denver, CO