



FOLEY  
HOAG AARPI

# Understanding GDPR and Its Impact on You, Your Company and Your Customers

**MassBIO Forum**

Colin J. Zick, Esq.

[czick@foleyhoag.com](mailto:czick@foleyhoag.com)

July 31, 2018



- Counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions.
- Advises on issues involving the transfer of data between jurisdictions, including GDPR, EU-US Privacy Shield, and other relevant data privacy and security laws, cloud security, cyber insurance, the Internet of Things, and data breach response.
- Co-founded the firm's Privacy and Data Security Group (which he currently chairs) and regularly contributes to its "Security, Privacy and the Law" blog, [www.securityprivacyandthelaw.com](http://www.securityprivacyandthelaw.com). Serves as a member of Law360's Privacy & Consumer Protection editorial advisory board.
- Selected by his peers for inclusion in THE BEST LAWYERS IN AMERICA in the field of Healthcare Law (2015-2018)
- Ranked by CHAMBERS USA: AMERICA'S LEADING LAWYERS FOR BUSINESS as one of Massachusetts' leading Healthcare attorneys (2010-2018)

# Special thanks to my partner, Catherine Muyl, who helped develop these materials.



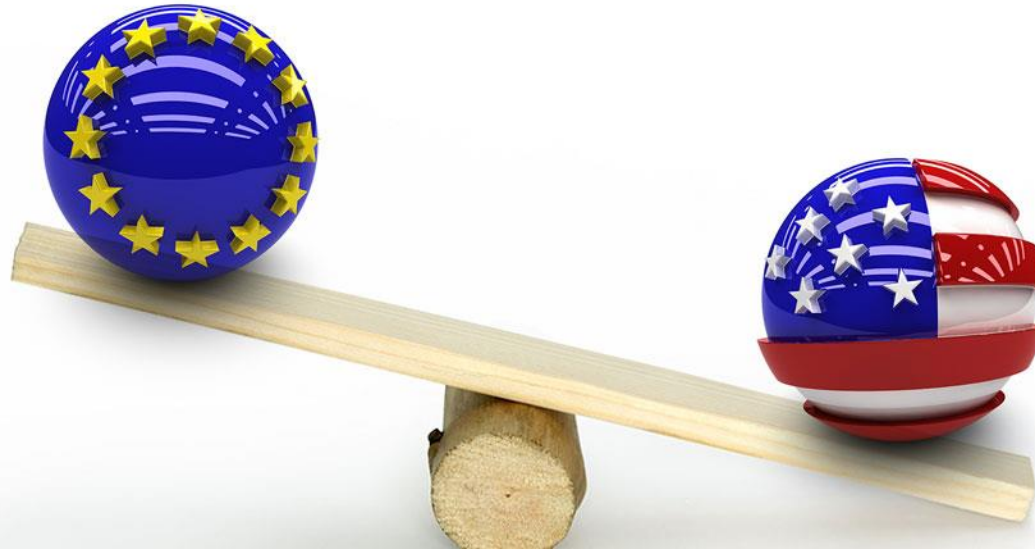
## Catherine Muyl

*Partner, Head of the French IP/IT Practice*




Paris | +33 1 70 36 61 30 | [cmuyl@foleyhoag.com](mailto:cmuyl@foleyhoag.com)

- Head of the Paris IP/IT practice.
- Works for French public entities and US and European private entities (ranging from start-ups to major international groups) on IT contracts and data protection issues, including GDPR and the transfer of data from the EU to the US. Regularly contributes to the firm's "Security, Privacy and the Law" blog, [www.securityprivacyandthelaw.com](http://www.securityprivacyandthelaw.com).
- Represents State-owned companies and private entities in IP and IT disputes before the French courts and the EUIPO (European Union Intellectual Property Office).
- Experience working on cross-border litigation.
- Native language French, fluent in English, proficient in German.

# To understand GDPR, you must see the cultural gap between EU and US



## Why should you care about those rules?

-  They aren't going away: in fact, similar rules will start coming from within the US
-  Fines: Supervisory Authorities are able to impose administrative fines of up to 20 million Euros, or 4% of total worldwide revenues of the preceding financial year, whichever is higher.
-  Contracts: Your business partners will expect you to be compliant and you'll have to confirm that compliance in contracts.

## Sensitive data (special categories of personal data):

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, [...] genetic data, biometric data for the purpose of uniquely identifying a natural person data concerning health or data concerning a natural person's sex life or sexual orientation.

## Controller:

- The person or body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

## Processor:

- The person or body which processes personal data on behalf of the controller.

## Who has to comply?

### Before May 25, 2018

- Controller has an establishment in the EU; or
- Controller uses equipment, automated or otherwise, situated in the EU.

### Now

- Controller or processor established in the EU; or
- Controller or processor not established in the EU where processing activities relate to:
  - the offering of goods or services in the EU; or
  - the monitoring of data subjects in the EU.

## What kind of data is covered?

### ■ 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 to one or more factors specific to his the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

## What kind of activity is covered?

### ■ Processing

Any operation or set of operations which is performed upon on personal data or on sets of personal data, whether or not by automatic automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking restriction, erasure or destruction.



## EU Data Subjects' Rights

Applies to anyone in the EU

**(not just residents or citizens)**, and includes

- Limits on information that can be collected
- Who has access to personal information
- Rectification of information
- Erasure (“the right to be forgotten”)
- Restrictions on use of information
- Data portability
- Objections to use of information



## What information does the data controller have to provide to data subjects?

- ❑ **Identity and contact details of the controller** and (if not established in EU) its representative,
- ❑ Contact details of the **Data Protection Officer**, where applicable,
- ❑ **Purposes** of the processing,
- ❑ If the controller intends to **transfer** personal data to a third country : the existence or absence of an adequacy decision by the Commission, which safeguards have been put in place and how to get a copy,
- ❑ **Period** for which the personal data will be **stored**,
- ❑ **Existence of the data subject's rights** (access, rectification, erasure, restriction, objection or data portability).



## EU-Based Representative:

- Controllers and processors not established in the EU must appoint a representative in the Union.

## Data Protection Officer:

Under GDPR, DPO must be appointed where :

- Processing is carried out by a **public** authority or body; or,
- Core activities consist of processing operations which by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring of data subjects on a large scale**; or,
- Core activities consist of **processing on a large scale of sensitive data**.

Some EU jurisdictions go further and require a DPO in all circumstances.

## Notification of data breach is required:

### To the Supervisory Authority

**Level:** where it is likely to result in a risk to the rights and freedoms of individuals.



Without undue delay, no later than 72 hours

#### Content of notification:

- Nature of the breach
- Name and contact details of the DPO
- A description of the likely consequences of the breach
- Description of the measures taken

### To Data Subjects

**Level:** where a breach is likely to result in a high risk to the rights and freedoms of individuals.



Without undue delay

#### Content of notification:

- Nature of the breach in clear and plain language
- Name and contact details of the DPO
- A description of the likely consequences of the breach
- Description of the measures taken

## Agreements between controllers and processors

- Heavier obligations and potential liabilities for processors.
- Contracts between controllers and processors are now mandatory and must include:
  - the subject matter and duration of the processing;
  - the nature and purpose of the processing;
  - the type of personal data and categories of data subjects;
  - the obligations and rights of the controller;
  - a list of minimum terms, obligations of the processors to ensure that both the controller and the processor comply with GDPR.

## Mandatory record of processing activities

- Obligation to maintain a **record of processing activities** containing the answers to the following questions:
  - Who?
  - Where?
  - What?
  - Until when?
  - Why?
  - How?



## Data Protection Impact Assessment

- Required where a processing likely to result in a high risk to the rights and freedoms of natural persons, for example:
  - processing on a large scale of sensitive data,
  - systematic monitoring of a publicly accessible area on a large scale (in particular CCTV),
  - automated processing on which decisions are based that produce legal effects.

## Transfers to countries which do not provide an adequate level of protection (including the US) :

- Current transfer tools :
  - to the US: Privacy Shield (but this might not last much longer).
  - Standard Contractual Clauses (SCC) issued by the Commission.
  - Binding Corporate Rules.
  - Consent.
  
- Additional transfer tools as from May 2018:
  - SCC issued by a Supervisory Authority.
  - Code of Conduct approved by the Supervisory Authority with binding and enforceable commitments from data importer.
  - Certification with binding and enforceable commitments from data importer.



## Similar Changes are Coming in the US

- The [California Consumer Privacy Act of 2018](#) (“CCPA”) was signed into law on June 28, 2018. Although it is a state law, it has national and international ramifications. Here are some key aspects to be aware of.
- The law is slated to go into effect on January 1, 2020.
- CCPA begins from the starting point of data privacy as a fundamental right (rather than, in most cases in U.S. law, as a balance between consumer and business interests).
- Applies to an entity doing business in California that: (1) has annual gross revenues over \$25 million, (2) annually buys, receives, sells, or shares the personal information of 50,000 or more California residents, households, or devices, or (3) derives 50% or more of its annual revenue from selling personal information of California residents.
- CCPA vests enforcement authority in the California Attorney General, which can impose a fine of \$2,500 per negligent violation (violations go beyond data breaches and include not complying with an individual’s data privacy rights), and \$7,500 per intentional violation, and also provides a limited private right of action to individuals for data breaches (which can include actual damages or set damages of up to \$750 per consumer per incident).

- Provides for the following individual data privacy rights:
- The right to know the purpose of data collection and what categories of personal data are being collected before the collection takes place.
- The right to object a company's sale of a consumer's personal information.
- The right for additional information regarding the personal information being collected.
- The right to have one's personal information deleted (with exceptions).
- The right to know whether one's personal information is disclosed to a third parties (and to know which third parties information is disclosed to).
- The right to not be discriminated against in terms of the price of a company's services in the event an individual chooses to exercise his or her privacy rights.



FOLEY  
HOAG AARPI



Thank you!

**FOLLOW US: @FoleyHoag**

Stay updated with our blog:

**[www.securityprivacyandthelaw.com](http://www.securityprivacyandthelaw.com)**