October 16, 2019

# GDPR Extraterritoriality—Industry Perspectives and Best Practices for Operationalizing Global Compliance

Corey M. Dennis, PPD
Lael Bellamy, Fenwick & West
Barbara Lawler, Looker
Susan DeVane, NCR Corporation
Lauren Kitces, Squire Patton Boggs

Privacy+ Security Forum

# Speakers

**Corey M. Dennis, CIPP/US, CIPP/E, CHC**
Director of Privacy & Counsel
Pharmaceutical Product Development, LLC (PPD)

**Lael Bellamy, CIPP/US**
Director, Privacy & Cybersecurity
Fenwick & West

# Speakers

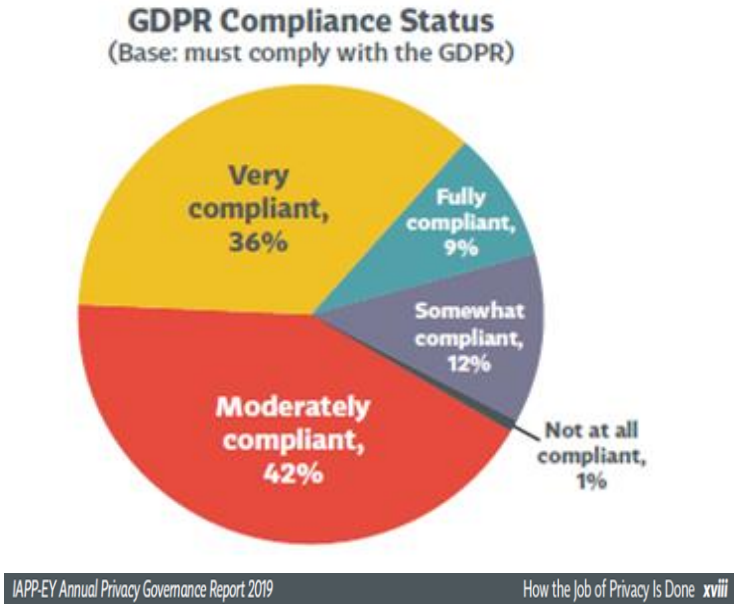
**Barbara Lawler, CIPP/US, CIPM, FIP**
VP, Chief Privacy and Data Ethics Officer
Looker

**Suzy DeVane, Esq., EnCE, CIPP/US**
IT Data Privacy Manager
NCR Corporation

**Lauren Kitces, CIPP/US, CIPP/E**
Associate
Squire Patton Boggs

# Introduction

## Why is this issue so important?




- **Compliance is complex** and **challenging**
- **Lack of understanding** of GDPR's territorial scope
- **Incorrect assumptions** made on applicability
- **Conflicts with law** (e.g., 1st Amendment, National Security)
- **Fines of up to 4% global revenue** for compliance violations
- **Potential PR issue** applying different rights globally (e.g., Facebook, Google)

# GDPR Territorial Scope and Requirements

Privacy+ Security Forum

## GDPR Article 3 (Territorial Scope)

(1) This Regulation applies to the processing of personal data ***in the context of the activities of an establishment*** of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(1) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the ***offering of goods or services***, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b) the ***monitoring of their behaviour*** as far as their behaviour takes place within the Union.

(2) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Privacy+ Security Forum

# Additional GDPR Requirements

- GDPR Article 27 (Appoint Representative)
  - where ex-EU Controller/Processor processes EU data subject personal data in many circumstances

- GDPR Article 37 (DPO)
  - additional requirements described in Articles 38 and 39

# EDPB Guidelines

## EDPB Guidelines on Territorial Scope of GDPR


- Draft guidelines (Nov. 2018) confirm expansive reach of GDPR
- Many open questions remain, e.g.:
  - "establishment" criteria
  - definitions of "monitoring" behavior and "offering goods or services"
  - Representative role/responsibilities

# Extraterritorial Application and Enforcement

- Enforcement challenges
- Google v. CNIL
  - global right to erasure rejected by EU Court of Justice
  - ability to apply rights globally permitted at a member-state level
  - case C-507/17 (24 Sept. 2019)
- Facebook CJEU ruling (Oct. 2019)
  - Facebook responsible for worldwide removal of defamatory comments
  - Freedom of speech/expression concerns

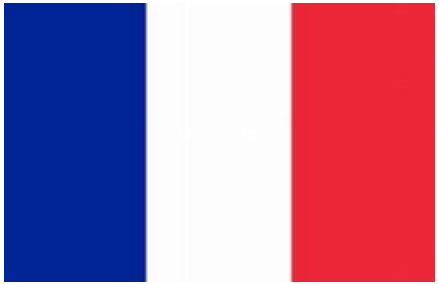
# Case Study

An e-commerce website is operated by a company based in Brazil. Data processing is exclusively carried out in Brazil, but the company has established a European office in Paris in order to lead and implement marketing campaigns aimed at EU citizens.


**Questions:**

(1) Is the company caught by the GDPR?

(2) Do Brazilian data subjects have rights to make a data subject rights request?



# Case Study

**Questions**:

(1) Is the company caught by the GDPR?

(2) Do Brazilian data subjects have rights to make a data subject rights request?

**Answers**:

(1) Yes. The organization will be caught by Article 3(1)

(2) Yes. Technically, once caught by Art 3(1) GDPR applies to ALL personal data processed (Art 3(1) is data subject blind).

# Best Practices

Privacy + Security Forum

- **Understand territorial applicability/limitations of GDPR**
- When in doubt, **assume "personal data" is subject to GDPR** and broadly defined
- **Ensure policies/procedures required by GDPR are global**
- **Implement global training** on GDPR
- **Implement** appropriate **EU data transfer mechanisms**
- **Incorporate GDPR contract requirements** (e.g., Article 28)
- **For Controllers/Processors based outside EU, appoint Representative** where required
- **Procure cyber insurance** with broad scope of GDPR considered

# Best Practices

- If seeking to avoid application of GDPR entirely, consider:
  - Not establishing physical presence/facilities in EU
  - Avoiding processing data of EU customers
  - Ensuring any such data is technically anonymized before received
  - Avoiding offering goods/services to those in the EU
  - Avoiding monitoring behavior of those in the EU
  - Not providing services (e.g., software hosting) involving EU data processing
  - Adopting position statement on GDPR inapplicability
  - Exercising care when negotiating agreements with GDPR obligations

# Industry Perspectives—Healthcare (Corey)

- EDPB Guidelines Example 5
  - pharma company based in EU (Stockholm) processes clinical trial data at company affiliate in Singapore
  - GDPR applies to processing per GDPR Article 3(1)
- multiple controller scenarios
  - e.g., EU-based pharma company and U.S. university hospital
  - potential application of EU subject rights under GDPR

# Technology/Data Analytics (Barb)

- B2B Events, professional certifications and sales/lead prospecting - contracts and DSARs under GDPR
  - multiple controller scenario
  - single controller scenario

- Data Analytics Platform - contracts, data security, DSARs under GDPR
  - controller to processor scenarios
  - data transfers and subprocessors

# Financial Services (Lauren)

- Data movement in a multiple-controller environment
  - Insurance placement example
- KYC check considerations
- Ensuring consideration of other requirements in regulated industries

# Fintech (Suzy)

- GDPR and CCPA
  - Efficiency and expediency are key: Organizations need to harmonize disparate rules and regulations to avoid redundancy and streamline compliance efforts.
  - As global companies with all data flowing worldwide how to delineate personal data from a particular country or state to be treated any differently?

# Questions + Contact

**Corey M. Dennis**
Director of Privacy & Counsel
PPD
coreymdennis@gmail.com

**Lael Bellamy**
Director
Fenwick & West
404-277-2495
lbellamy@Fenwick.com

# Questions + Contact

**Barbara Lawler**
Chief Privacy & Data Ethics Officer
Looker
barbara.lawler@looker.com

**Suzy DeVane**
IT Data Privacy Manager
NCR
678-808-5104
Susan.DeVane@NCR.com

**Lauren Kitces**
Associate
Squire Patton Boggs
202-457-6427
lauren.kitces@squirepb.com

# Resources

Privacy+ Security Forum

# Resources

Privacy+ Security Forum

## GDPR vs. Data Protection Directive

| Issue | The Directive | The GDPR | Impact |
|---|---|---|---|
| **Establishment**<br><br>**Organisations are subject to EU data protection law if they have an establishment in then EU. The word "establishment" is not precisely defined. The key question is whether there is effective and real exercise of activity through stable arrangements (e.g., a branch or subsidiary can be an "establishment", but a travelling salesperson is unlikely to constitute an "establishment").** | Rec.19; Art.4(1)(a)<br><br>The Directive (as implemented via the national law of a Member State) applied to organisations that:<br><br>· were established in one or more Member State(s); and<br><br>· processed personal data (whether as controller or processor and regardless of whether or not the processing takes place in the EU) in the context of that establishment. | Rec.22; Art.3(1)<br><br>The GDPR applies to organisations that:<br><br>· are established in one or more Member State(s); and<br><br>· process personal data (either as controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment. | The GDPR and the Directive both apply to organisations that have an establishment in the EU and process personal data in the context of that establishment. |
| **Application of Public International Law**<br><br>**EU data protection law applies to an organisation if the laws of any Member State apply to that organisation by virtue of public international law.** | Art.4(1)(b)<br><br>An organisation that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law was also subject to the Directive. | Rec.25; Art.3(3)<br><br>An organisation that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR. | The GDPR does not amend this principle. In practice, the circumstances in which the laws of a Member State apply by virtue of public international law are rare, and so this issue is unlikely to materially affect many organisations. |

# Resources

## GDPR vs. Data Protection Directive

| | | | |
|---|---|---|---|
| Activities in Member States<br><br>EU data protection law may apply to an organisation if offering goods or services is the nature of the organisation's activities in a Member State, or in relation to the individuals in that Member State. | Rec.20; Art.4(1)(c)<br><br>The Directive (as implemented via the national law of a Member State) applied to organisations established outside the EU if they made use of a "means of processing" (e.g., equipment or a processor) located in a Member State, for the purposes of processing personal data (other than mere transit of those data through the EU). | Rec.23; Art.3(2)(a)<br><br>The GDPR applies to organisations established outside the EU if they (either as controller or processor) process the personal data of individuals in the EU when offering them goods or services (whether or not in return for payment). The question of what constitutes "offering" goods or services to individuals in the EU is determined on a case-by-case basis:<br><br>· Mere website accessibility of a service in the EU is not sufficient to trigger application of the GDPR.<br><br>· Factors such as offering a service in the languages or currencies used in a Member State (if not also used in the third country), or mentioning customers or users in a Member State may trigger application of the GDPR. | For any organisation that was already using a "means of processing" in the EU to offer goods or services to individuals in the EU, these changes are unlikely to have any practical impact.<br><br>For any organisation that was not subject to the Directive (e.g., because it is established outside the EU and does not use a "means of processing" in the EU) but offers goods or services to individuals in the EU, these changes mean that such an organisation is subject to the full range of compliance obligations under the GDPR, in relation to the relevant processing activities. |

# Resources

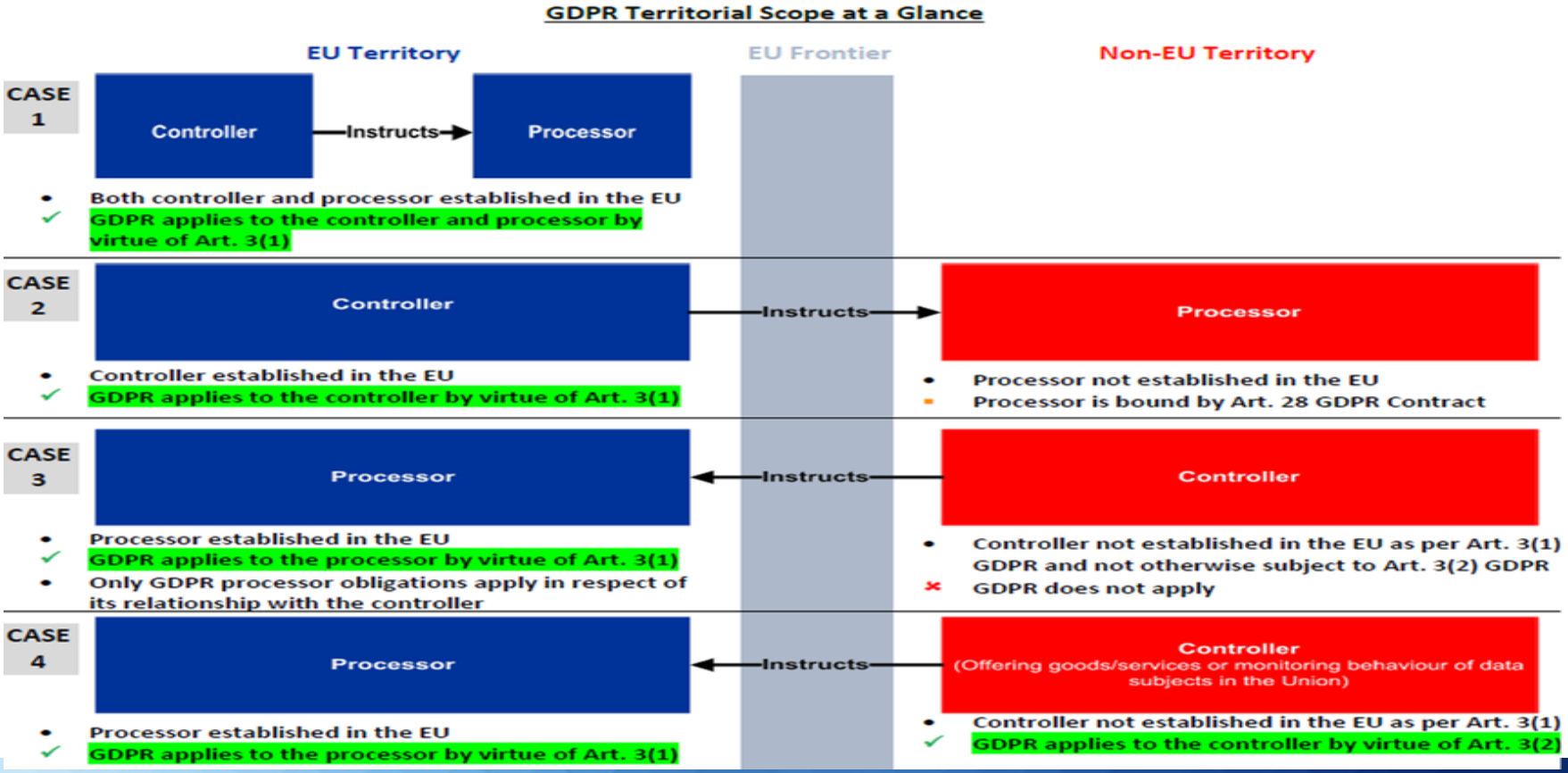
Privacy+ Security Forum

## GDPR vs. Data Protection Directive

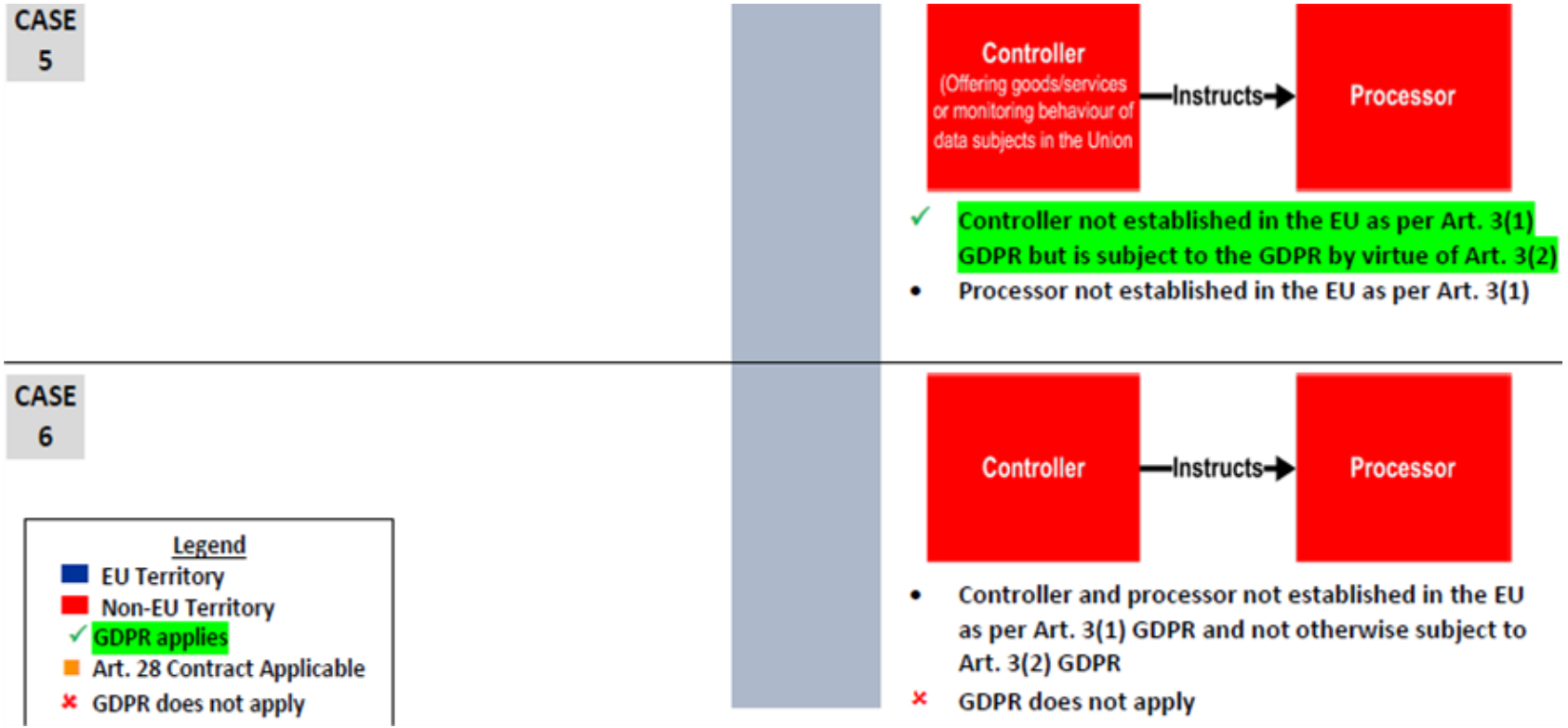
| Issue | The Directive | The GDPR | Impact |
|---|---|---|---|
| Monitoring of individuals in the EU<br><br>EU data protection law may apply to an organisation if that organisation monitors the behaviour of individuals in the EU. | N/A<br><br>The application of the Directive was not affected by the question of whether an organisation monitored the behaviour of individuals in the EU. | Rec.24; Art.3(2)(b)<br><br>The GDPR applies to organisations established outside the EU if they (whether as controller or processor) monitor the behaviour of individuals in the EU (to the extent that such behaviour takes place in the EU). The question of what constitutes "monitoring" is determined on a case-by-case basis:<br><br>· "monitoring" may include tracking an individual in the EU on the internet; and<br><br>· "monitoring" may also include the use of data processing techniques to profile individuals, their behaviours or their attitudes (e.g., in order to analyse or predict personal preferences). | For any organisation that was already monitoring the behaviour of individuals in the EU either through an establishment in the EU or a "means of processing" in the EU, these changes are likely to make little practical difference.<br><br>For any organisation that was not subject to the Directive (or applicable national laws of Member States) but monitors the behaviour of individuals in the EU, these changes mean that such an organisation is subject to the full range of compliance obligations under the GDPR, in relation to the relevant processing activities. |

**Source:** D. Gabel and T. Hickman, "Unlocking the EUGeneral Data Protection Regulation," White & Case LLP (updated April 2019), https://www.whitecase.com/publications/article/chapter-4-territorial-application-unlocking-eu-general-data-protection

# Resources


GDPR Territorial Scope at a Glance
EU Territory
EU Frontier
Non-EU Territory
CASE 1
Controller
Instructs
Processor
• Both controller and processor established in the EU
✓ GDPR applies to the controller and processor by virtue of Art. 3(1)
CASE 2
Controller
Instructs
Processor
• Controller established in the EU
✓ GDPR applies to the controller by virtue of Art. 3(1)
• Processor not established in the EU
- Processor is bound by Art. 28 GDPR Contract
CASE 3
Processor
Instructs
Controller
• Processor established in the EU
✓ GDPR applies to the processor by virtue of Art. 3(1)
• Only GDPR processor obligations apply in respect of its relationship with the controller
• Controller not established in the EU as per Art. 3(1) GDPR and not otherwise subject to Art. 3(2) GDPR
× GDPR does not apply
CASE 4
Processor
Instructs
Controller
(Offering goods/services or monitoring behaviour of data subjects in the Union)
• Processor established in the EU
✓ GDPR applies to the processor by virtue of Art. 3(1)
• Controller not established in the EU as per Art. 3(1)
✓ GDPR applies to the controller by virtue of Art. 3(2)

# Resources




**Source:** Centre for Information Policy Leadership, "Comments to the EDPB on Draft Guidelines 03/2018 on Territorial Scope" (18 Jan. 2019), https://www.huntonprivacyblog.com/2019/01/22/cipl-submits-comments-to-edpbs-draft-guidelines-on-the-territorial-scope-of-the-gdpr.