



AIJA

www.aija.org

**Lost in Privacy? – How to tackle transatlantic
data protection challenges**
New York, 2-3 February 2017



The General Data Protection Regulation And Its Impact In The USA And In The Rest Of The World

February 3, 2017 New York

Tanja Jaatinen
Ministry of Justice (Finland)
Senior Specialist, LL.M., LL.B.



www.aija.org

www.aija.org

Introduction

“20 million reasons for organisations to get EU data reforms right”, ICO 14 March 2016



Rationale Behind the EU Data Protection Reform

- Currently includes the General Data Protection Regulation (EU 2016/679, 'GDPR') and Directive for the Police and Criminal Justice Sector (EU 2016/680)
- GDPR replaces the 20-year-old Directive 95/46/EC
 - Full harmonization not plausible
- Two main incentives: free flow of data and enhanced level of data protection
- Harmonization of data protection laws among the member states
- Extending EU data protection legislation to apply to data controllers and processors located outside of EU

Scope of the GDPR

- Wide material scope (broad definition of personal data)
- Article 3 on 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.
 2. **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.

[...]



Article 8 of the Charter of Fundamental Rights of the European Union

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Main Features of the GDPR

- Risk-based approach
- Higher sanctions (maximum 4 % of worldwide turnover / MEUR 20)
- From compliance to accountability
- Controller-processor relationship
- Enhanced data subject rights
- New obligations (e.g. data breach notifications, DPIAs...)
 - More obligations for processors (e.g. cloud service providers), too
- One-stop-shop

- Will be applied as of 25 May 2018 - 476 days to go!



Thank you!

Tanja Jaatinen

Ministry of Justice of Finland

Helsinki, Finland

tanja.jaatinen@om.fi



Tanja Jaatinen





The General Data Protection Regulation And Its Impact In The USA And In The Rest Of The World

February 3, 2017 New York

Federica De Santis
Goodwin Procter LLP
International Associate



www.aija.org

www.aija.org



Agenda

- Practical impacts for US businesses
- The “One Stop Shop” mechanism
- Breach notification
- Other trends to watch (proposed e-Privacy Regulation; data localization)



Practical Impact Of GDPR For US Businesses

- Intended to harmonize EU privacy laws and reduce compliance burden
- Member states will still have the authority to impose additional obligations (e.g., genetic, biometric, health data; employee data; professional secrecy; national security)
- EU-based representative
- Enforcement?

The «One Stop Shop»

- Aimed at achieving consistent application and enforcement across the EU
- Applies to “cross-border” processing activities of controllers/processors
 - Multiple establishments in the EU
 - Single establishment carrying out processing activities that “substantially affect” individuals in multiple EU States
- “Lead” Data Protection Authority (DPA) of the “main establishment” or single establishment will coordinate enforcement

The «One Stop Shop»

- Cooperation and consistency procedures
 - Lead DPA must involve “concerned” DPAs
 - European Data Protection Board will determine disputes between DPAs
- DPAs remains competent to handle “local” cases (e.g., HR data)
- Urgency procedure

Case Scenarios

1. A company has its headquarter in France and subsidiaries in other EU countries. All the EU companies use a CRM software to process customers' data. The strategic marketing decisions are taken by the French establishment and the marketing team is also located in France.
2. A company established in Ireland runs an online pharmacy that carries out marketing based on the drugs purchased by customers. It analyses this information to build up a 'health and wellbeing' profile of customers and carry out targeted marketing.

What About.....?

- Businesses with no establishment or no “main establishment” in the EU
- Businesses acting as controllers for some activities and processors for others
- Other



Data Breach Notification

- US&EU data breach notification regime
- GDPR requires “data controllers” to notify DPAs within 72 hours
- Individuals must be notified “without undue delay” if the breach is likely to result in a “high risk” for them
- Interplay with other breach requirements (e.g., Network&Information Security EU Directive)
- Key Takeaways



Other Trends

- EU Commission's proposed e-Privacy Regulation
 - Regulates providers of electronic communication to harmonize EU e-Privacy laws & ensure consistency w/ GDPR
 - Interplay with GDPR
- Data localization requirements & challenges for companies
 - E.g., Russia, China



Thank you !

Federica De Santis

Goodwin Procter LLP

United States, Boston

fdesantis@goodwinlaw.com



Federica De Santis





The General Data Protection Regulation And Its Impact In The USA And In The Rest Of The World

February 3, 2017 New York

Daniel Avila Failla
Dannemann Siemsen
Brazil



www.aija.org

www.aija.org

South America



Agenda

- Data Protection in South America
- Data Protection in Brazil
- Challenges
 - Collecting/Processing Brazilian data
 - Brazilian companies collecting/processing European data
 - Transferring data to Brazil

South America

- Civil law systems
- Heavily regulated
- Technology importers
- “Law importers”



Uruguay

- Act 18.331/2008
 - Protection of personal data is inherent to the human being (constitutional principle)
 - Applied to personal data stored in any platform in which they can be processed and all manners in which the data can be of posterior use.
- European Commission - adequate level of protection

Argentina

- Article 43 of the Federal Constitution - right to access personal information stored in public databases
- Federal Law 25.326/2000
 - Protects personal data stored in archives, registers, databases and other data processing platforms, public or private, in order to guarantee the right to privacy and correlated rights, such as honor, image and intimacy.
- Data Protection Authority with enforcement powers.
- European Commission - adequate level of protection (2003)

Chile

- Chilean Data Protection Law N° 19.628/1999.
- Basic concepts are poorly drafted, leaving ample margin for interpretation.
- Does not have a DPA
- Proof of damage
- Low fines – up to US\$ 3,500

Colombia

- Colombian Constitution provides for the fundamental rights to intimacy and data protection.
- Law 1266/08 - credit, financial and banking use of personal
- Law 1581/2012 - data protection provisions.
- Decree 1377/2013 - consent, treatment of sensitive data, how data subjects can exercise their rights and cross borders transfer of personal data.

Brazil



Brazil

- No Data Protection Law
- Therefore...
 1. Brazilian Constitution
 2. Civil Code
 - 3. Consumer Code**
 4. Federal Law 9296/96 - interception of computer and telephonic communications
 5. Access to Information Law (Federal Law 12.527/11) - access to information stored in public databases

CONTINUES...



Brazil

6. Telecommunications Act – confidentiality of telecommunication companies' clients
7. Children Protection Act – protection against the use of children's names and their protection against pornography, both on the Internet and in physical media
8. Electoral Code
9. Complementary Federal Law 105/01 – financial data
10. Labor Law
- 11. Internet Civil Rights Framework – Federal Law 12.965/14 (“Marco Civil da Internet”) regulated by Decree 8771/16**

Brazil

- Privacy and Data Protection
 - Bill of Law 52726/16
 - Bill of Law 330/133

Brazil

- BICRF, as to personal data collection, storage and use, provides for:
 - Data quality
 - Purpose
 - Consent
 - Confidentiality
 - Right to access
 - Right to be forgotten
 - Transparency

South America

Data Subject Rights	Breach Notification	Right to Access	Right to be Forgotten	Privacy by Design	Data Protection Officers	Data Portability
GDPR	Yes	Yes	Yes	Yes	Yes	Yes
Brazil Today	No	No	Yes	No	No	No
Brazil Personal Data Protection Bill	Yes	Yes	Yes	Yes	No	Yes
Argentina	No	Yes	Yes	Yes	No	Yes
Colombia	Yes	Yes	Yes	Yes	No	Yes
Chile	No	Yes	Yes	No	No	Yes
Uruguay	No	Yes	Yes	Yes	No	No



Challenges



The screenshot shows the top section of The Guardian's website. At the top, there is a dark blue navigation bar with links for "a supporter", "subscribe", a search icon, and "search". On the right side of this bar are links for "jobs" and "US edition". Below this is the "theguardian" logo in white. Underneath the logo is a horizontal menu with various sections: "opinion", "sports", "soccer", "tech", "arts", "lifestyle", "fashion", "business", "travel", and "environment". To the right of this menu is a button that says "browse all sections". Below the navigation bar, the main headline reads "Brazilian police arrest Facebook's Latin America vice-president". Underneath the headline, there are two bullet points: "● Dzodan accused of ignoring judicial order in drug crime investigation" and "● Facebook says WhatsApp is separate entity and does not store information".

a supporter | subscribe | search

jobs US edition

theguardian

opinion sports soccer tech arts lifestyle fashion business travel environment

≡ browse all sections

Brazilian police arrest Facebook's Latin America vice-president

- Dzodan accused of ignoring judicial order in drug crime investigation
- Facebook says WhatsApp is separate entity and does not store information

Challenges

According to the court, [WhatsApp](#) had been ordered for more than a month to reveal messages relating to a suspected drug-trafficking ring. After the company denied three related requests by federal police, the judge first imposed a daily fine on the US company of 50,000 reais (£9,000), then a daily penalty of 1m reais (£180,000), and finally ordered the arrest.

“In the face of repeated non-compliance, the judge Marcel Maia ordered the arrest of a representative of the company in [Brazil](#), Mr Diego Dzodan for obstructing the police investigation,” a court spokesman wrote in an email.

[Facebook](#) called the police action “extreme and disproportionate”.

It says WhatsApp - which was acquired by Facebook in 2014 and has no staff based in Brazil - operates independently so Dzodan should not be held responsible. Moreover, it notes that the WhatsApp messaging service does not store content, which is encrypted by users at either end. The courts, it says, are requesting information it does not have.

Challenges

- Whatsapp caseS
- 100 million users (80% of the cellphone owners use WhatsApp)
- 4 attempts to interrupt Whatsapp services
- 2 times blocked – 14 hours and 24 hours
- Decisions issued in criminal cases
- Facebook refused to deliver the conversation content and users data
- Criminal law enforcement x Privacy and Consumers rights

Challenges

- Challenges (Collecting/Processing Brazilian data)
 - Local laws (different regulation depending on the purpose)
 - Absence of data protection specific regulation
 - Lack of experience/knowledge of the courts
 - Criminal law enforcement current relevance
 - Turbulent political environment may difficult advances in the near future

Challenges

- Challenges (Brazilian companies collecting/processing European data):
- Lack of data protection culture - Privacy by Design or Default
- Enforcement of GDPR in Brazil:
 - Review by the Superior Court of Justice
 - (a) the parties must prove that the decision attend to all legal formalities;
 - (b) the decision must be final, with no possibility of further revision;
 - (c) it needs to be notarized by a Brazilian Consul in the country where it was delivered and translated into Portuguese;
 - (d) in addition, in order to receive the exequatur from the Superior Court, foreign decision cannot be contrary to the Brazilian public order and local practices.
- Choice of law / dispute resolution

Challenges

- Challenges (Transferring data to Brazil):
 - Did not receive approval from the European Commission
 - Binding Corporate Rules
 - Model Clauses



Thank you!

Daniel Avila Failla

Dannemann Siemsen

São Paulo, Brazil

dfailla@dannemann.com.br



Daniel Avila Failla

