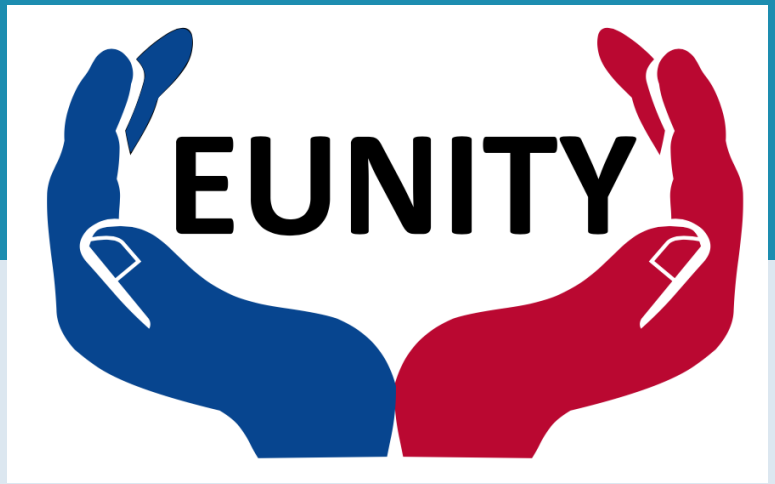
KU LEUVEN

CENTRE FOR IT & IP LAW

imec

European privacy landscape:

GDPR and others



EUNITY Project meeting

Tokyo, 11/12 October 2017

KU LEUVEN

CENTRE FOR IT & IP LAW

imec

KU Leuven Centre for IT & IP Law (CiTiP) – imec

Stefano Fantin

Policy Researcher

www.law.kuleuven.be/citip

Summary

Background and context

What is GDPR?

International transfers and NIS

Conclusions

Japanese Landscape

Background and context

The Digital Single Market

Announced in 2015 with the purpose of fostering the role of the EU as a global leader in the digital economy.

Aims at creating **the right environment and conditions for digital networks and services***.

Developing stronger data protection rules is part of such a policy area.

State of the European Union 2017

(Strasbourg, 13/09/2017)

Two out of five* Commission's priorities for the next year explicitly mention privacy and data protection as a main driver.

The General Data Protection Regulation and EU privacy reform

To start with:

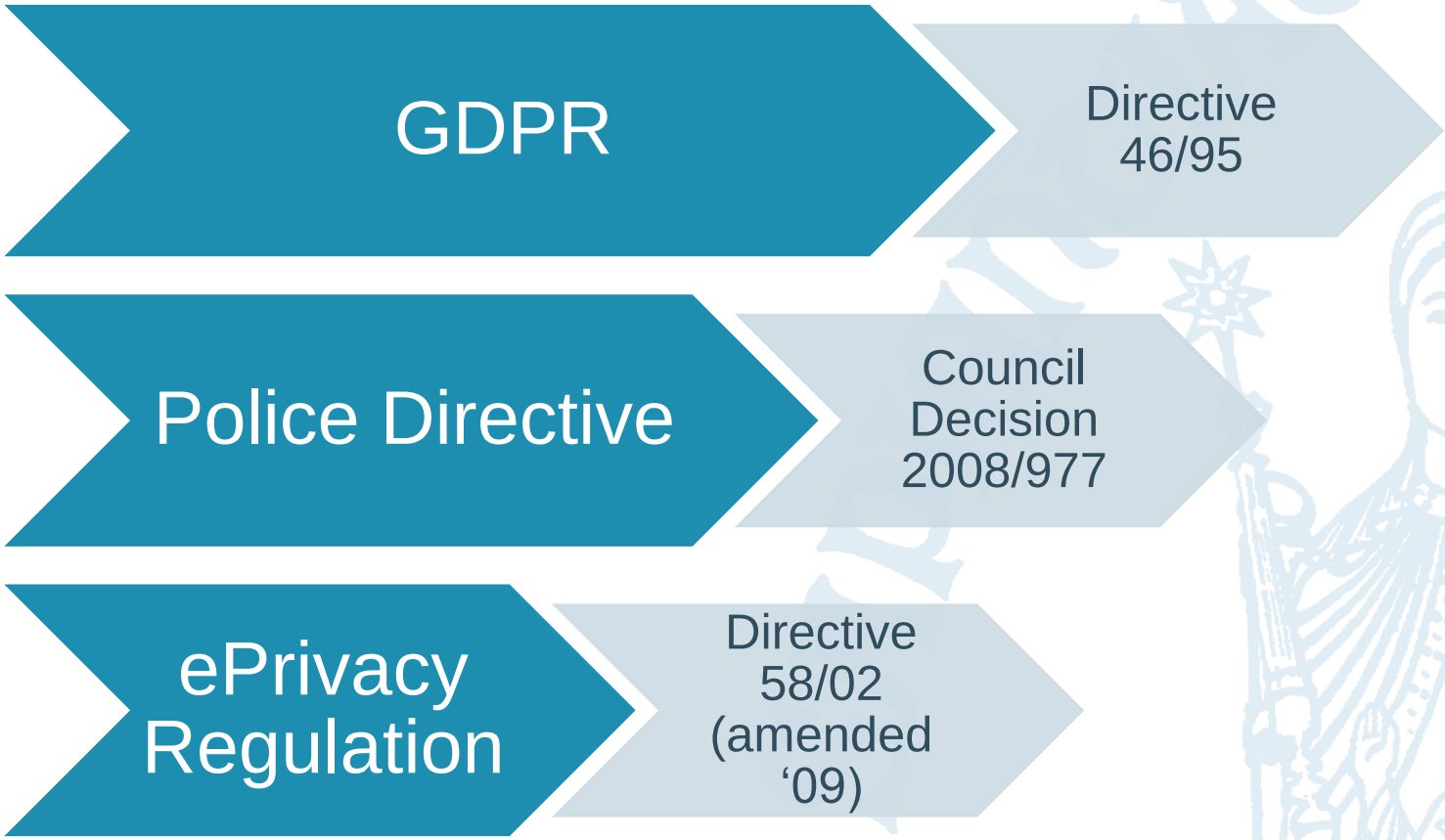
It is not **only** about GDPR!

The new reform is more comprehensive:

- GDPR
- Directive on data protection in the Police and Justice Sector (“Police Directive”)
- Proposal for a new ePrivacy Regulation (currently work in progress)

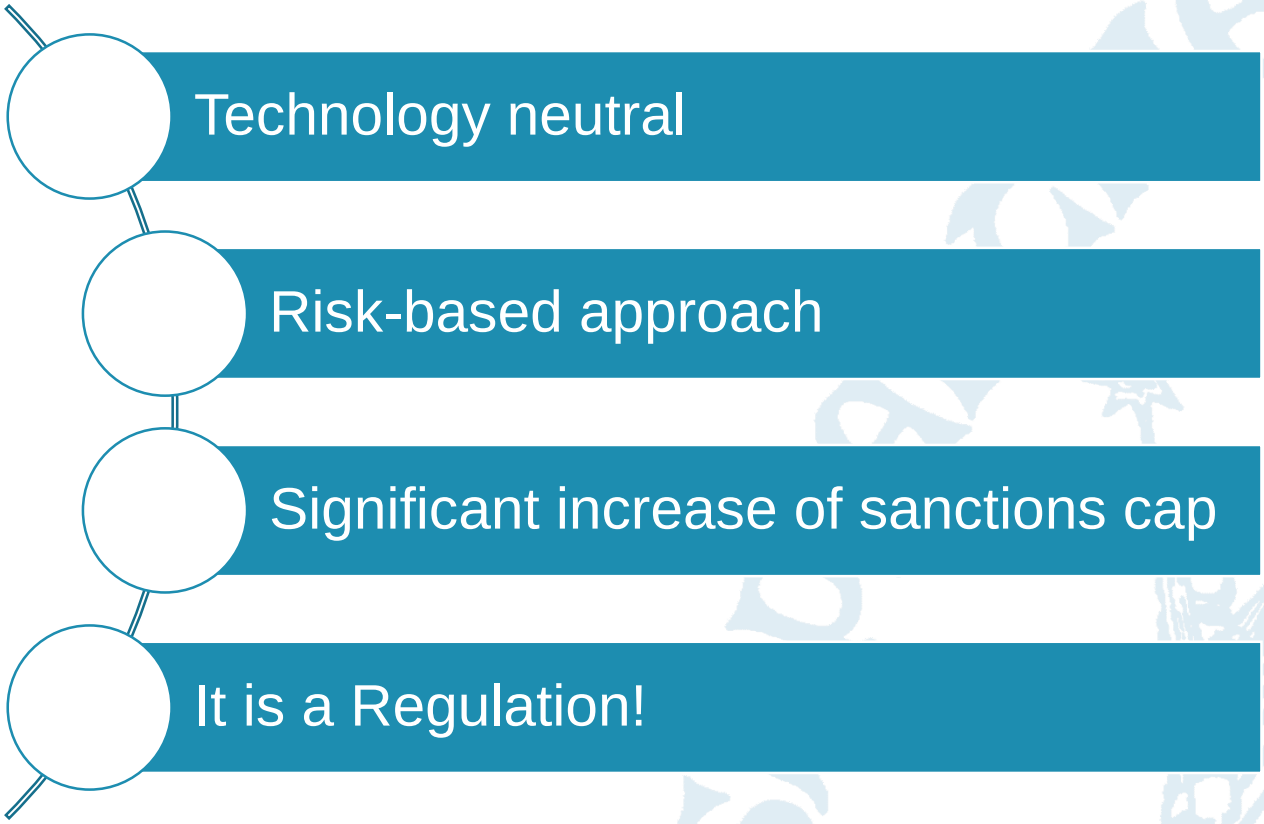
What do we leave behind?

The three acts of the reform repeal previous legal texts:



Let’s talk about GDPR

Among the main themes…



Application

It will apply as of **May 25th, 2018.**

It will apply to the processing of personal data:

- **by** controllers established in the EU (regardless of whether the processing takes place in the Union or not).
- **of** data subjects who are in the Union by a controller or processor not established in the Union

(GDPR, Art.3)

More protective towards individuals' rights

Right to access

Right to transparent information

Right to rectification

Right to object

Right to be forgotten*

Right to data portability*

(GDPR, Ch. III)

More reactivity required

In the event of a **data breach**, organizations need to:

- Inform the data subject if there's a high risk
- Notify the breach to the data protection authority
- React promptly (72 hours)

(GDPR, Art. 34)

More accountability and transparency requirements for data controllers

Obligation to keep records of processing activities and to appoint a Data Protection Officer *(Art.30 and 37)*

Stricter rules on consent, lawful processing, data minimization and purpose limitation *(Art. 5, 6 and 7)*

Data protection by design and by default* *(Art.25)*

More security

Demonstrating compliance with GDPR through security of personal data processing and of the systems;

Controllers will have the obligation to implement technical and organizational security measures such as PETs (encryption, pseudonymisation) and other actions aimed at ensuring CIA. *(Art. 32)*

Such measures will have to be duly documented *(R78, 81 and 83)*

Consent by children

art 8 GDPR

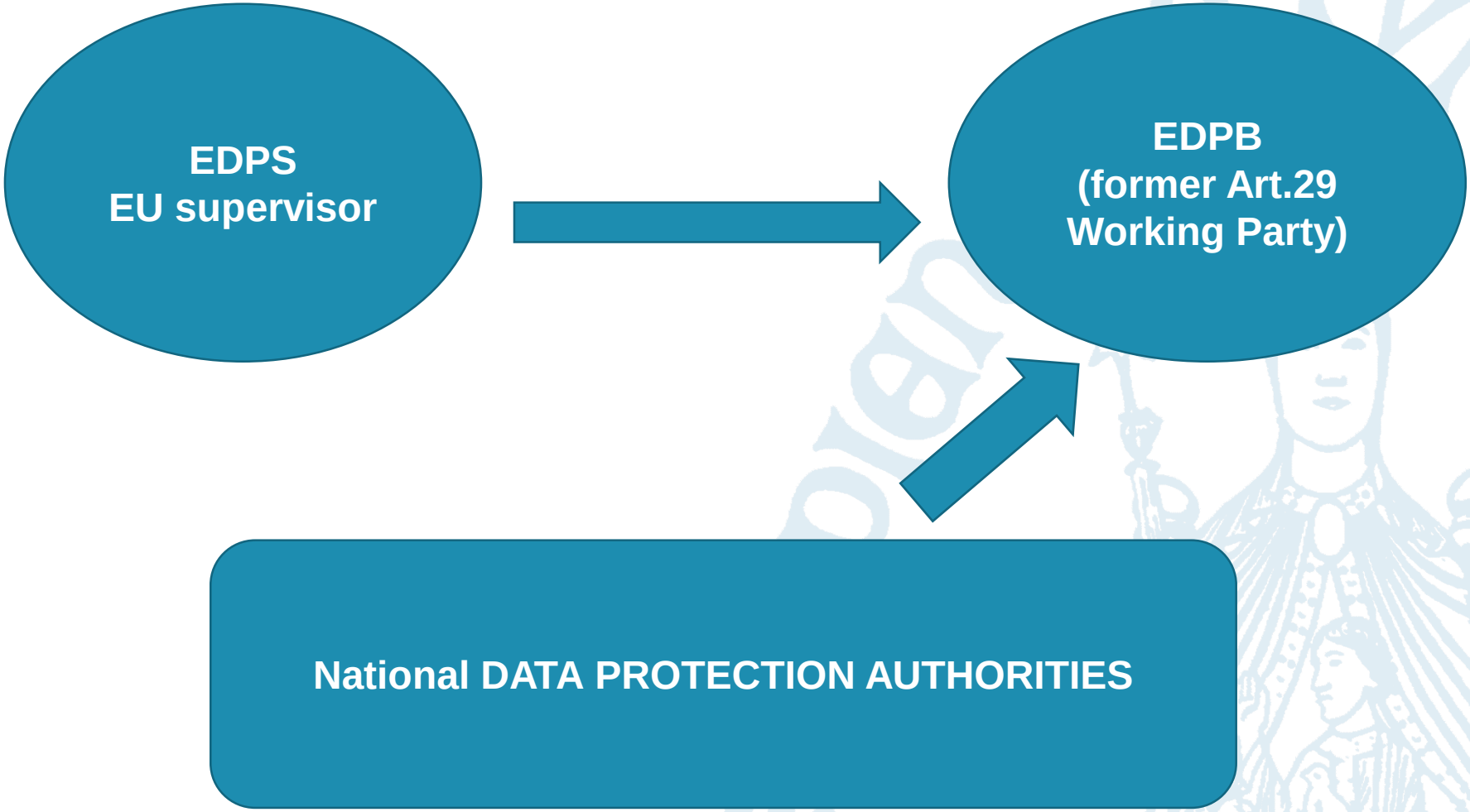
Consent by children under 16 must be given by parent.

BUT Member States may lower the age to 13.

- So far, the UK & Ireland: 13, Spain: 14
- Other MS with plans to change age: Sweden & Poland

KU LEUVEN

Key regulatory bodies: the model as from May 2018



GDPR readiness

Are organizations ready?

Not fully: two examples…

- In the United Kingdom, 33% of Local Government Authorities still don't do privacy impact assessments (source: ICO, 3/2017).

- Globally, 47% of companies claim that all of their critical data is securely stored (source: NTT, 8/2017).

International transfers

State of play

The EU is **not only** reviewing its internal data protection rules.

This is in fact a crucial period for several relationships with international **partners** with regard to cross-border personal data flows.

Some examples…

United States: Privacy Shield is suffering delays in its full implementation

United Kingdom: GDPR standards will still apply regardless of its withdrawal from the EU (“Brexit”)

Japan and South Korea: ongoing negotiations with the European Commission aimed at an adequacy decision

GDPR and NIS Directive

GDPR and NIS Directive

	Security of Networks and Information Systems Directive	General Data Protection Regulation
Date of Adoption/Application	6 July 2016 (10 May 2018)	27 April 2016 (25 May 2018)
Objectives	• Ensure common security level across EU • National CS Strategy • National single point of contact • Incident Response Team (& Network) • Cooperation Group • Security and Breach Notification Requirements	• Protection of Personal Data Processing • Data Protection Officer • Controller/Processor Agreements • Data Protection by Design (T&O Measures, PIA) • Breach Notification • Etc....
Scope of Application	• Member States • Operators of Essential Services (energy, transport, banking, financial market, health, etc.) • Digital Service Providers (online search engines, online market place, cloud computing)	• Member States • Data Controllers • Data Processors

Post-Scriptum: the NIS Directive

The different legal instruments used to codify reveal two major considerations:

- Different stages of progress at EU policy level between privacy and cyber security
- Different strategies. Cyber security in the EU requires active intervention by Member States: it aims at boosting cooperation, rather than imposing strict and readily-enforceable rules (different from GDPR).
- Different models: PPPs (public-private partnership) vs EDPB (regulatory/advisory intergov. authority)

Conclusions

GDPR is part of a broader EU policy initiative:

- It is part of the **DSM** strategy
- It is a milestone of a bigger **reform package**
- It influences the setting up of **international** personal data transfers
- It is about protecting **individuals**
- It aims at shifting corporate behaviors into a more transparent **mentality**

The Japanese privacy landscape: Introducing our guest

Prof. **Hiroshi Miyashita**

(Associate Professor of Law, Chuo University)

Thank you.

Reach out at the following contacts:

Stefano Fantin
stefano.fantin@kuleuven.be

KU Leuven Centre for IT & IP Law
(CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip