Deloitte.

Link'n Learn
General Data Protection Regulation

16 March 2017

Georges Wantz
Director – Technology & Enterprise Application
Deloitte Luxembourg
E: gwantz@deloitte.lu
T: +352 45145 4363

Jessica Lavery
Senior Consultant – Data Privacy Services
Deloitte Ireland
E: jlavery@deloitte.ie
T: +353 1 417 2839

Table of contents

GDPR Presentation

The General Data Protection Regulation (GDPR)

Why does it matter?

The General Data Protection Regulation (GDPR)

The GDPR presents both major risks and opportunities

Risks	▪ **Financial :** Penalties of up to 4% of annual revenues or EUR 20 million, whichever is higher ▪ **Reputational :** Fines and privacy violations can create negative press that erode customer confidence and brand equity ▪ **Operational :** Unless properly designed and implemented, patchwork efforts at GDPR create risks to the efficiency and reliability of operations ▪ **Extra-Territorial :** The GDPR extends beyond the EU to other jurisdictions ▪ **Global Trend**: Other countries and regions (e.g. APAC, Canada, Switzerland) have also been revising their privacy laws
Opportunities	▪ Impetus to get control over data and enable effective analytics ▪ Gain the trust and confidence from customers, employees, and partners ▪ Create a stable legal environment for technology adoption (cloud, big data, etc.)

The General Data Protection Regulation (GDPR)

What is the GDPR?

1995

In 1995, the European Union released the **European directive 95/46/CE** relative to personal data protection. Unlike regulations, directives should be transposed into national to be applicable.

2009

The Charter of Fundamental Rights of the European Union became legally binding across the EU with the entry into force of the Treaty of Lisbon on 1st December 2009 introducing the "Protection of personal data" as a fundamental freedom (art. 8)

2016

On 4 May 2016, the **EU Regulation on Data Protection (GDPR)** has been published in the Official Journal of the European Union. The GDPR has entered into force on 24 May 2016 and will replace the former 1995 EU Data Protection Directive and create a unified data protection law

2018

The General Data Protection Regulation will apply as from **25 May 2018** directly across all 28 EU Member States after a two years implementation period. Under the new Regulation, Data Protection Authorities (DPAs) have investigative, corrective, advisory and authorization powers. They are entitled to impose **administrative fines ranging from 2 to 4% of the groups worldwide annual turnover of the preceding financial year or EUR 10 to 20 million**, whichever is higher for infringements of data subject rights, non-compliance with an order of the DPA or the obligations of the controller and processor.

The General Data Protection Regulation (GDPR)

How did we get to the GDPR?

Need for improvement of the current frameworks

➢ **Unsatisfactory EU data protection framework:**

- Divergence and inconsistency in the current data protection rules across the EU's 28 member states
- Fragmented legal environment with legal uncertainty and unequal protection for individuals causing unnecessary costs and a significant administrative burden for businesses
- Not enough empowerment for data subjects regarding the control of their personal data
- Not enough enforcement of the current frameworks

Legal needs

➢ **Outdated requirements and new needs:**

- Necessity to catch up with the digital age
- Necessity to take into account that personal data has acquired enormous economic significance by offering flexibility to businesses while protecting individuals' fundamental rights

Through a long process

➢ **Great deal of lobbying:**

- The most lobbying for any piece of European legislation: 4 years of debate, negotiation and lobbying
- Even countries outside EU (e.g. the United States) had been very active in the new Regulation lobbying, to protect the interest of US companies operating in the EU

Striking points within the GDPR adoption journey

➢ **Some requirements of the GDPR raised debates involving important time for getting to a common agreement. Ex:**

- Personal data breach notification
- Unambiguous consent
- Data Protection Officer
- etc.

The General Data Protection Regulation (GDPR)

What is a personal data?

"Any information relating to an identified or identifiable natural person".

Relating

- Content
- Purpose
- Result

Identification

- Direct
- Indirect

Data subject

- Not deceased persons
- Not legal persons

Reference

- Name
- ID number
- Location data
- Online identifier
- Etc.

The vast majority of organizations deal with personal data.

The General Data Protection Regulation (GDPR)

What is processing personal data?

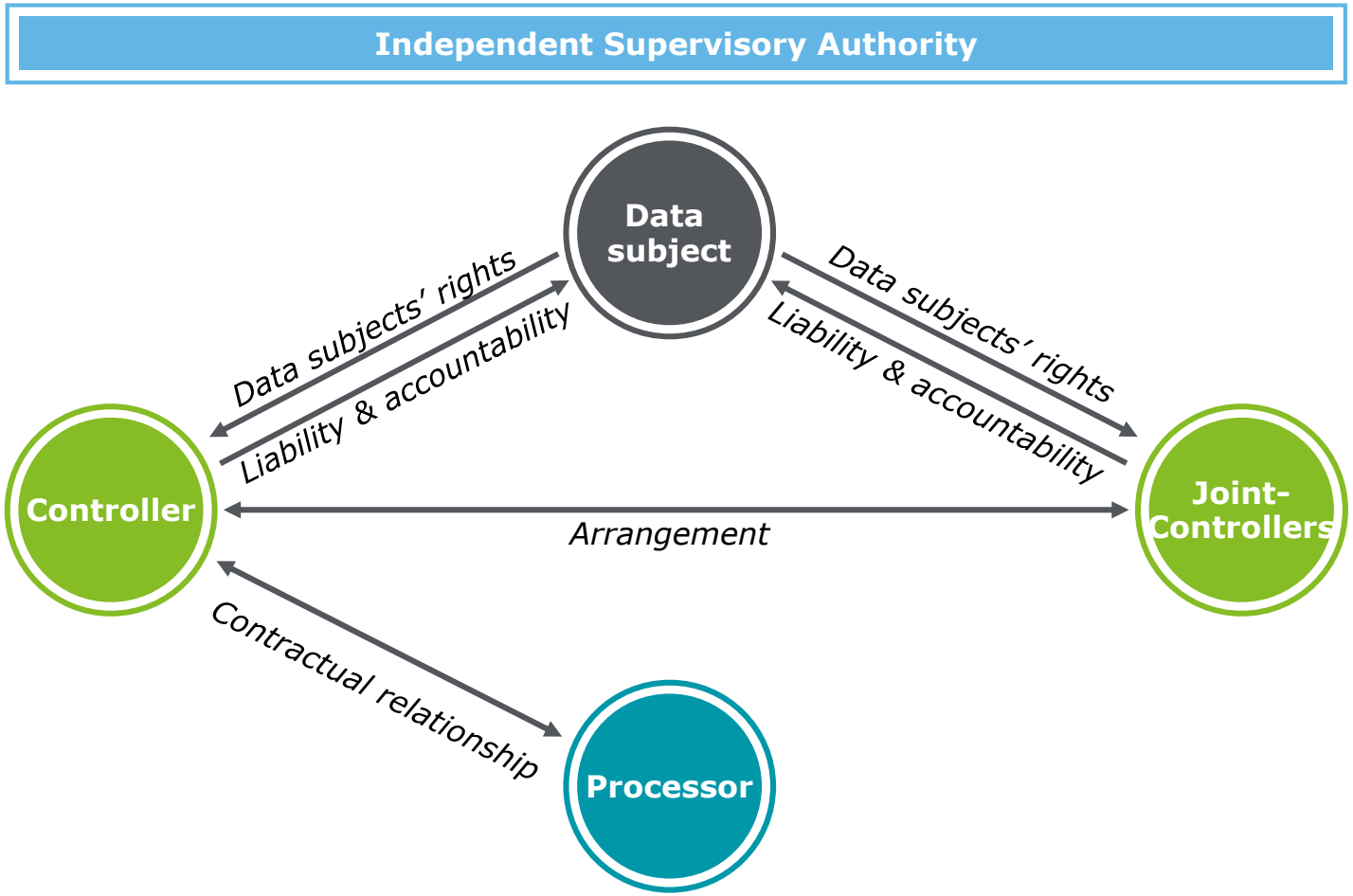
"Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means".

Personal data lifecycle

Collection	Storage	Use	Transfer	Retention & Destruction
				
• Collection • Recording	• Structuring • Storage	• Adaptation or alteration • Retrieval • Consultation • Use • Combination • Alignment	• Disclosure by transmission • Dissemination	• Destruction • Erasure • Restriction

The General Data Protection Regulation (GDPR)

What are the key roles defined in GDPR?



Data subject

An identified or identifiable natural person (e.g. private clients, employees, external consultants, etc.).

Controller

The natural or legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data (e.g. when processing employees data, employers are acting as controllers in the meaning of the GDPR).
Where two or more controllers jointly determine the purposes and means of processing, they are joint controllers.

Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (e.g. IT providers hosting personal data for their clients are acting as processors in the meaning of the GDPR).

Independent Supervisory Authority

An independent public authority which is established by a Member State to be responsible for monitoring the application of the GDPR.

The General Data Protection Regulation (GDPR)

What does the GDPR bring?

Controller and processor

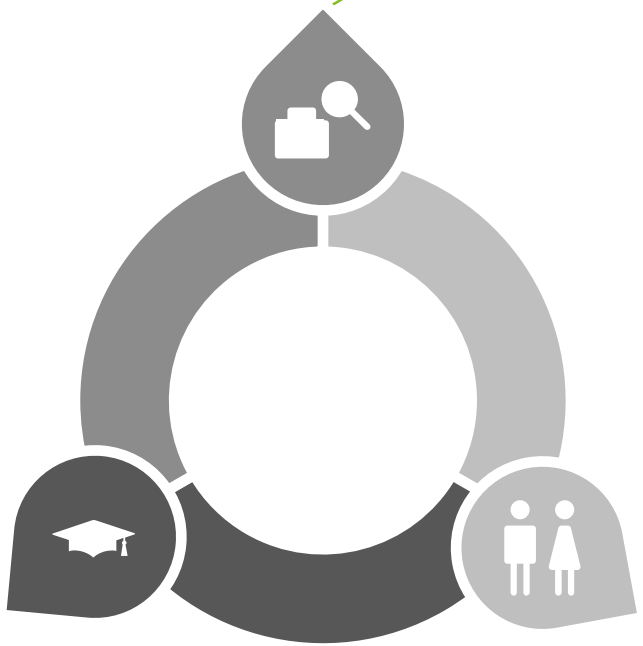
Chapters : Controller and processor, transfers of personal data to third countries or international organisations

- Accountability
- Data protection framework
- Data protection by design / by default
- Data breach notification
- Data protection impact assessment
- International data transfers

Independent supervisory authority

Chapters : General provisions, Cooperation and consistency, Independent supervisory authority

- Broader territorial scope
- One stop shop
- Enforcement



Data subject

Chapters : Principles, Rights of the data subject

- Consent
- Data subject rights
- Profiling
- Right to be forgotten
- Data portability

The General Data Protection Regulation (GDPR)
Controller and processor

Requires Documentation

Accountability
New obligation for controllers and processors to be able to demonstrate and therefore to document their compliance with the GDPR.
Companies will have to appoint a Data Protection Officer in specific situations (e.g. public authorities, large scale monitoring, special categories of data).

Data Protection Framework/Documentation
Companies should document the measures implemented.
All the measures required by the GDPR, when put together, will result in a data protection related framework : DP policy, DP by design and by default, impact assessments, data breach notifications, privacy notices, etc.

Data Protection by design/by default
Companies should implement appropriate technical and organizational measures to integrate the necessary safeguards into the processing of personal data.
By default, only necessary personal data should be processed. This requires control over : data collection, extent of processing, retention period as well as access to personal data.

International data transfers
BCRs as tools for data transfers outside the EU and EEA are now embedded in law.
Approved codes of conduct and certifications could be relied on by entities not subject to the GDPR to provide adequate safeguards for transfers of personal data.

Data breach notification
Notify data breach to the data protection authority no later than 72h after becoming aware of it.
Notify data breach to affected data subjects without undue delay when likely to result in a high risk for their right to data protection.
Processors should report to respective customer-controllers.

Data Protection Impact Assessment
Where a processing is likely to result in high risks to the rights and freedoms of natural persons, a DPIA is to be performed.
Controllers should consult their supervisory authority where a DPIA indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk.

The General Data Protection Regulation (GDPR)

Data subject

Requires Documentation

Consent

Consent is spelled out more clearly as it should be given through a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement.
Ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance will be considered as satisfactory.
Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Data subject rights

Existing rights are reinforced (access, rectification, deletion, objection to the processing).
The GDPR introduces the rights to erasure, restriction of processing, data portability and the right not be subject to data profiling.

Profiling

The GDPR strictly frames profiling activities and empowered data subjects with the right not to be subject to decisions based on profiling as well as the right to object to profiling and notably profiling for marketing purposes.

The General Data Protection Regulation (GDPR)

Independent supervisory authority

Enforcement

DPAs already have investigative, corrective, advisory and authorization powers.
They will be entitled to impose administrative fines up to 4% of the groups worldwide annual turnover, or up to 20 millions.

Broader territorial scope

The GDPR will not only apply to processing activities of data controllers and processors established in the EU or using equipment located in the EU, but also to those that are not established in the EU but whose activities target data subjects are in the EU.

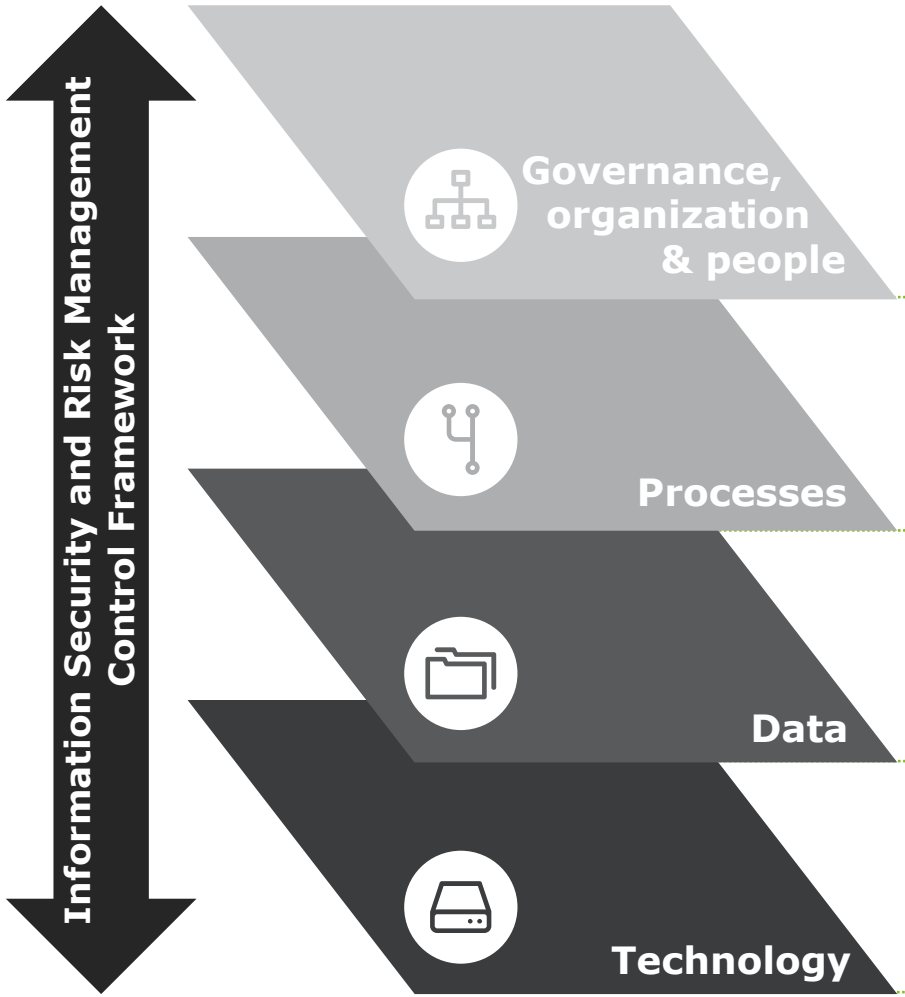
One stop shop

When having activities in more than 1 EU member state, the Data Protection Authority (DPA) of main establishment could act as lead DPA, supervising processing activities throughout the EU.
This will ease the interaction for controllers and processors with lead DPA while other DPAs will still have a say in cross-border operations through consistency and cooperation procedures.

GDPR impacts on organizations and how to address the new challenges

Impacts on the operating model

GPDR will mainly impact four layers of the operating model



Governance, organization & people

- Support from leadership
- Definition of roles and responsibilities
- Identification of communication channels
- Definition and implementation of policies and procedures
- Training awareness, etc.

Processes

- Review the business processes using personal data (current and future)
- Identification of the processes with risks
- Embodying Privacy by Design / by Default in the business processes
- Include the data subjects rights in the processes design, etc.

Data

- Identification of the personal data collected and processed
- Implementation of data management, etc.

Technology

- Identification of the systems supporting data processing
- Assessing the risks and the related mitigation measures
- Ensuring that the functionalities are "Privacy Friendly" and will allow to implement Privacy by Design / by Default, etc.

DOCUMENTATION

What is next ?
How to prepare GDPR compliance

Where to start?

Gap Analysis

	Objectives	Activities	Outputs
Quick Scan	The Quick Scan provides the organization with a **first data protection status** regarding the GDPR. The Quick Scan mainly focuses on identifying the **scope to be considered by the organization** under the GDPR and the h**igh-level gaps** related to the Regulation.	1 Identify the business and administrative processes 2 Define the scope to be considered with regards to the GDPR 3 Identify the risks areas 4 Identify the current high level status against GDPR	**"Cartography" of the personal data processes within the organization** **Risks areas and the high-level status of compliance** **Recommended next steps**
Detailed Gap Assessment	The Detailed Gap Assessment allows to identify **in detail the gaps with the Regulation, the current risks and the mitigation measures for reducing these privacy risks.** The detailed Gap Assessment provides the organization **with a roadmap** for implementing a sustainable framework for data protection, in respect to the GDPR.	1 Assess into details the current risks / existing measures Further measures for reducing risks 2 Analyse into details the gaps with GDPR requirements Further practical measures for meeting the requirements 3 Regroup the measures into Work Packages (priorities, duration, efforts, etc.) Propose a global roadmap	**Risks assessments and recommended mitigation measures** **Current level of compliance and the further measures** **Target Operating Model (work packages)** **Global Roadmap**

Deloitte.

THANK YOU

Deloitte.