Deloitte.

General Data Protection Regulation

Main changes & challenges

SAS Forum Belux – June 12, 2017

Introduction

Data Protection & Privacy on the corporate agenda

- Technology today is allowing companies to gain important **competitive advantages** through cross-border and inter-departmental **sharing of (personal) data**.

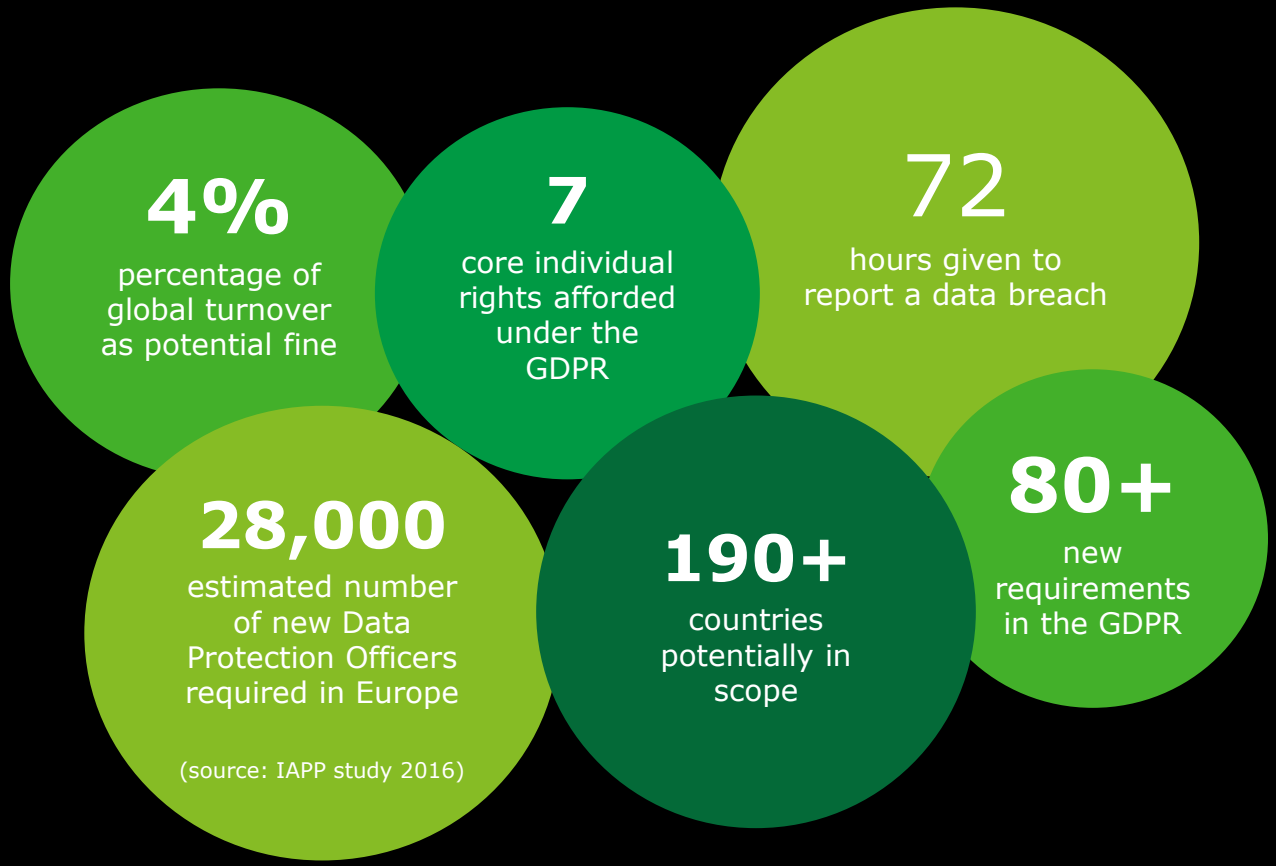
- Privacy requires a fresh and more **holistic approach**.

- **General Data Protection Regulation (GDPR)** has the objective to harmonize the current fragmented legal framework for data privacy across Europe.

- GDPR enters into force by 28th of May 2018

- The GDPR introduces new **challenges** for organizations:

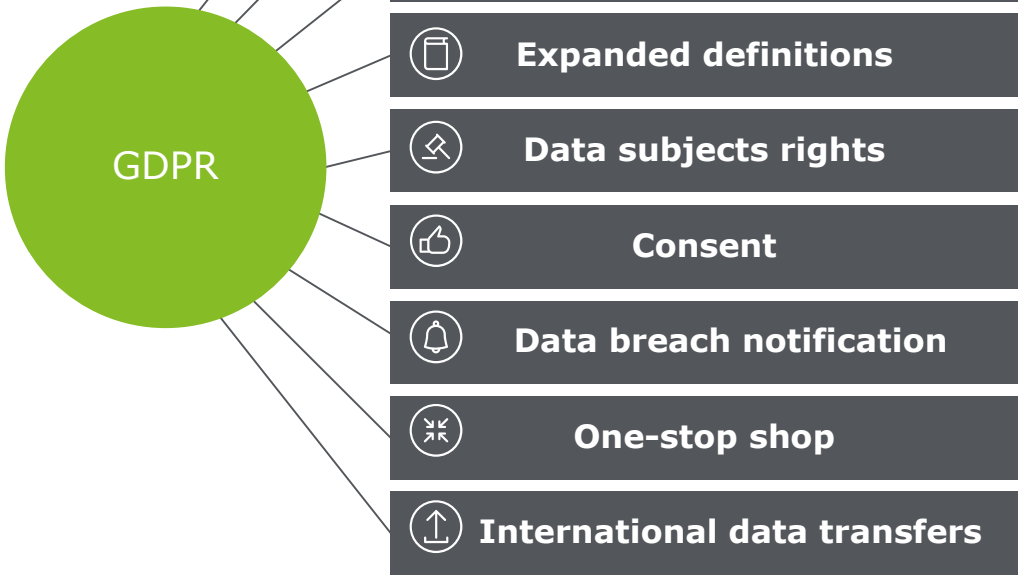
GDPR
Overview of the main changes



General Data Protection Regulation

Scope

What will change against the former 1995 EU Data Protection Directive ?



Applies to players **not established in the EU** but whose activities consist of targeting data subjects in the EU

Data Protection Authorities will be entitled to impose **fines ranging between 2 to 4% of annual turnover**

Explicit obligation to the controller as well as the processor to be able to **demonstrate their compliance to the GDPR**

Personal data now **explicitly includes location data, IP addresses, online and technology identifiers**

Reinforced rights: access, rectification, restriction, erasure, objection to processing; no automated processing and profiling

Spelled out more clearly and focus on ability of individuals to distinguish a consent

A controller has to **report** a personal data breach to the Data Protection Authority **within 72h** after becoming aware of it

Data Protection Authorities (DPA) of main establishment can act as lead DPA, supervising processing activities throughout the EU

Binding Corporate Rules (BCR) explicitly mentioned as recognized data transfer mechanism

GDPR
Both major risks and opportunities

Risks:

- **Financial risk:** Penalties of up to 4% of annual revenues or EUR 20 million, whichever is higher
- **Reputational risk:** Fines and privacy violations can create negative press that erode customer confidence and brand equity
- **Operational risk:** Unless properly designed and implemented, patchwork efforts at GDPR create risks to the efficiency and reliability of operations
- **Extra-territorial risk:** 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.)

GDPR
Requirements: five main areas

1. Data Governance

The tone on the top, policies, roles, responsibilities, and organizational structures support the protection of individuals' privacy

2. Data Subject Rights

Controllers gives individuals ("data subjects") control over what data is processed about them and for what purpose

3. Security of Personal Data

Personal data is processed securely; authorities and where applicable data subjects are notified of high-risk breaches

4. Data Transfers

Legal and procedural controls are in place to ensure the adequate protection of personal data by 3rd parties

5. Data Protection Principles

Business and HR processes are such that the processing of personal data is lawful, purpose-limited, and transparent to the data subject

How does it impact YOUR company in real life…

GDPR affects all organizational layers and lifecycle stages of data management

Information Security and Risk Management

Governance, organisation & policy

Processes

Data

Technology

Define an organizational **strategy** (risk- vs. compliance- based, brand-alignment, etc.), **roles, responsibilities, accountability, training, policies**, and **risk appetite**,

Re-design business and HR processes to comply with **GDPR Data Protection Principles**; enhance existing or build new **control processes** for security, breach notification, privacy by design/default, PIA, audit, etc.

Build **records of processing**; provide clearer, more proactive **control over the data lifecycle** collection, storage / retention, usage, and journeys / lineage

Explore **technological solutions** to better protect, manage and control data usage, e.g. minimizing data collection, preventing data proliferation, using data anonymization, streamlining data subject requests, etc.

SAS Accelerators

Start preparing now

Becoming compliant - Action items

Changes triggering updates

Review the following items to ensure that they still comply with the GDPR requirements:

- Information notice
- Access right procedure (including rectification, erasure and objection)
- Processing based on consent
- Processing based on automated decision making (including profiling)
- Agreements with third parties processing personal data
- Data security

Becoming compliant - Action items

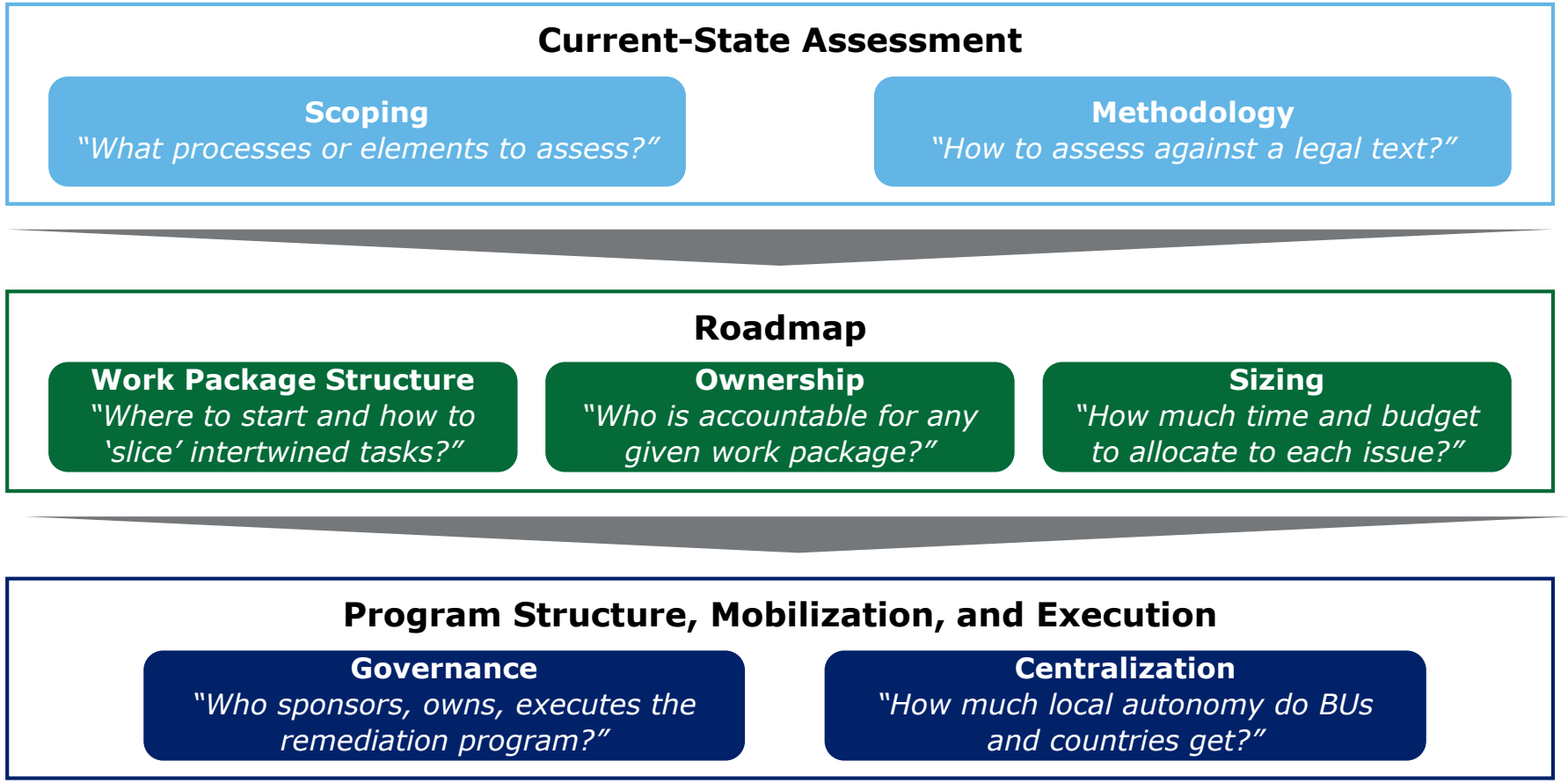
Changes triggering updates

If not yet in place and if applicable to your organization, consider how you can implement the following new operational requirements :

- Implement the right to portability
- Appoint a DPO (internal / external)
- Document each processing of personal data
- Create a PIA methodology
- Create privacy training and awareness
- Create a third party assessment methodology
- Set up a data breach management procedure
- Determine which processes require a prior consultation

Becoming Compliant – Process

A structured approach helps companies mobilize and avoids the risks of over-analysis and getting lost in details



Tackling GDPR: Our pragmatic, holistic approach

Where to start: a layered, risk based approach leveraging on tested project methodology

Project methodology

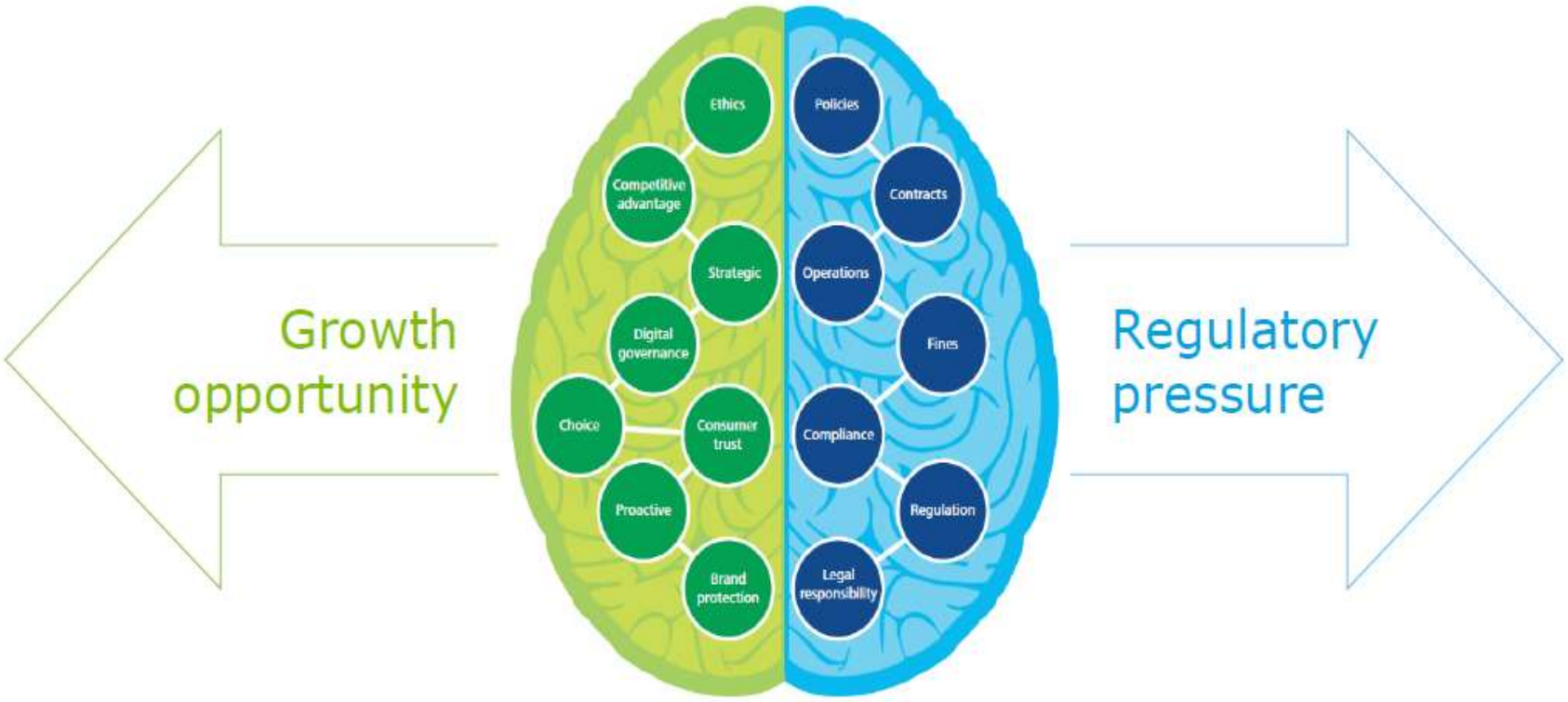
	Inception	Elaboration	Construction	Transition
	Quick scan / Detailed gap			
Main objectives	• The Inception step aims at assessing the current status of the organization for meeting the GDPR requirements • This phase also allows to obtain a roadmap for implementing a sustainable framework for data protection, in respect to the GDPR • It is divided into two sub steps: – Quick scan – Detailed gap analysis	• Develop the project implementation and resource plans • Define detailed functional and non-functional requirements • Define the organizational and technical solutions design for all components • Prepare documentation for GDPR purposes	• Implement the actions of the Work Packages agreed in the previous phases • Develop and configure the enterprise IT assets to implement specified solution • Test the related business processes and supporting IT systems • Implement and test the mitigation measures for reducing privacy risks • Prepare documentation for GDPR purposes	• Prepare for and execute the transition to the new solutions and processes • Validate final user acceptance • Train users and ensure continued awareness • Form or enhance a support organization to manage the environment after transition

Can be performed for the whole organization or at business unit/country level

At the end of the inception, the different work packages will be defined. Each work package could follow a different timeline and project approach (e.g. waterfall, hybrid agile or agile) depending on its scope and priority

Turn your GDPR journey as an opportunity

Beyond regulatory obligation, GDPR is a unique opportunity to reinforce a trustful relationship with your customers and employees



Contact details

Erik Luysterborg
Partner – Enterprise Risk Services
Zaventem (Belgium)

Erik Luysterborg is a partner within Deloitte Belgium (Group Enterprise Risk Services).

He holds the international certificate of the CIPP (Certified International Privacy Professional) and has acted as Chief Privacy Officer for Deloitte worldwide (DTT) for four years.

Christophe Hallard
Partner – Analytics & Information Management
Zaventem (Belgium)

Christophe Hallard is a partner within Deloitte Belgium.

He cumulates more than 20 years of experience in supporting organizations to manage their data (governance, architecture, strategy, analytics) and gain meaningful insights out of their data.

Deloitte.