IBM Security

General Data Protection Regulation

THE NEW EU REGULATION AND ITS IMPACT

Christian Nern
Head of IBM Security Software DACH

07.11.2017

IBM

General Data Protection Regulation – GDPR

1. **What is it all about?**

2. **Where are we now with GDPR?**

3. **How businesses can prepare**

General Data Protection Regulation – GDPR

The European Union (EU) calls GDPR the "**most important change in data privacy regulation in 20 years.**" Passed in April 2016, the EU law will become enforceable on May 25, 2018.

Ovum Research found that **54% of executives** at large enterprises said GDPR compliance is their **top data privacy and security priority**. Only 7% said complying with GDPR mandates wasn't a top concern.

In Ovum Research , **52% of the IT decision-makers** surveyed said they believe GDPR will result in **business fines** for their companies.

GDPR – What is it all about?

New rules for obtaining consent and allowing people to withdraw consent for data collection

- Data breach notification **within 72 hours of awareness**
- The right for consumers:
  - to have their **data erased**
  - to see **any data companies have about them**
  - to **move their data** from one provider to another
- The requirement for companies:
  - to **appoint a Data Protection Officer**
  - to **build privacy into their systems** and **limit employee access** to personal data
- Although GDPR is an EU regulation, it **applies to organizations all around the world**
- Those companies that aren't in compliance **by May 25, 2018**, will face penalties up to **$20 million €** or “2**% of the total worldwide annual turnover** of the preceding financial year, whichever is higher.“

Where are we now with GDPR?

- ***Data protection with technical equipment and privacy-friendly default settings (Art. 25, 35)***
  - Risk identification, access documentation
  - Access of the right person at the right time to right data
  - Which personal data is processed and why?
  - How is the data processed?
  - Which risk are related?
  - How can risks be reduced?

- ***Security of processing (Art. 32):***
  - Data security: encryption and pseudonymity
  - Confidentiality, integrity, resilience
  - Availability and restoration
  - Regular review, assessment, and evaluation

- ***Information obligation for data breaches (Art. 33, 34):***
  - Which data is affected?
  - What are the consequences?
  - Notification of regulatory authority and affected persons – within 72 hours
  - What was the reason and how can it be prevented?

GDPR – How businesses can prepare

10 Steps Enterprises Need to Take to Comply with GDPR*

1. Start Discussions Now:

- If your organization hasn't begun preparing for GDPR, you absolutely need to get started today
- Raise awareness about the law among key stakeholders (e.g. IT Leaders)

2. Determine If GDPR Applies to You

- GDPR regulations are so sweeping that they apply to nearly every company with international activity
- Generally applies to:
  - Data controllers: organizations that collect data
  - Data processors: (third-party organizations and cloud computing providers that process data for other organizations)

3. Perform a Thorough Review

- Undertake thorough review of the data you currently have that might be covered by the law
- Conduct a privacy risk assessment (e.g. classify information and data in broad categories)

* Source: https://www.informationweek.com/strategic-cio/10-steps-enterprises-need-to-take-to-comply-with-gdpr/d/d-id/1330098?

GDPR – How businesses can prepare

10 Steps Enterprises Need to Take to Comply with GDPR

4. Allocate a Budget

- Include costs for new personnel, outside consultants and attorneys, as well as any new technology or services
- PwC report:
  - 77% of companies said that their total data privacy budgets would be **$1 million or more**
  - 9% expected to spend **more than $10 million**

5. Hire a Data Protection Officer (DPO)

- The law states that you must have a DPO if:
  - Enterprise is "public body" or
  - Core activities involve "regular and systematic monitoring of data subjects on a large scale."

6. Develop a Strategy for GDPR Compliance

- Gap assessment: determine where the organization is already in compliance with the law and where additional measures need to be put into place
- DPO should work closely with IT and members of management

GDPR – How businesses can prepare

10 Steps Enterprises Need to Take to Comply with GDPR

7. Put Appropriate Technology, Policies and Procedures in Place

- Experts caution that organizations should do more than the bare minimum to achieve compliance

8. Train Your Employees

- Employees need to understand the basic requirements of the law, as well as how company policies and procedures change

9. Establish a Track Record of Compliance

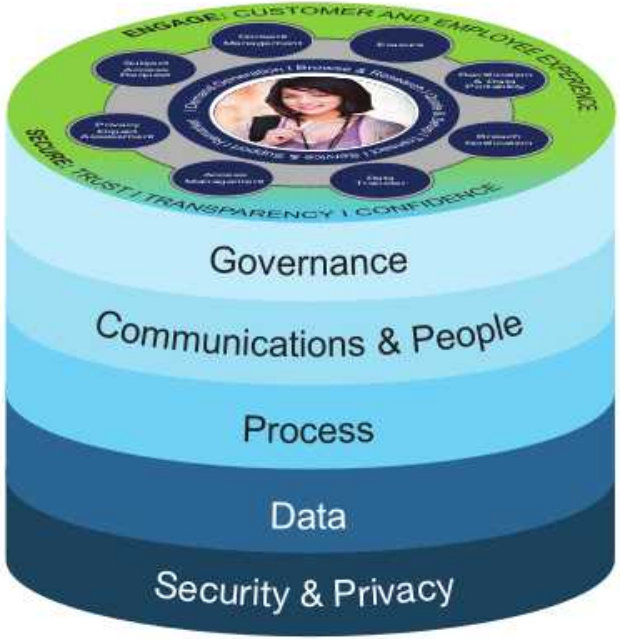
- Organizations shouldn't wait until the deadline but they should make the necessary changes as soon as possible to gain experience with the new practices and technologies before risking fines

10. Monitor Guidance from EU Countries

- Regulators from the EU and the individual EU countries have issued additional guidance to help companies
- Companies need to make sure that they are staying abreast of developments
- They will need to continue monitoring legal and regulatory modifications that may occur after GDPR takes effect

GDPR Layer Model

...IBM's five layer model for GDPR



Governance

GDPR governance, covering amongst others legal assessment, third party management and risk and compliance; DPO role

Communications & People

People and Communications, covering employee awareness and training, and internal and external communication

Process

Processes, covering the GDPR readiness of HR, CRM and other business processes

Data

Data, covering personal data life cycle management and citizen interaction

Security & Privacy

Security, covering cyber security technologies to protect critical personal data and capabilities that enable timely breach notification