GDPR – Two Years After

An empirical and analytical impact evaluation

By,
Knud Erik Skouby,
Lene T Sørensen,
Samant Khajuria

20 January 2021

TERMA
ALLIES IN INNOVATION

Introduction

- Two basic principles in the GDPR
  - **Protection of the data of natural persons "Personally identifiable information (PII)"**
    - "Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed"
    - Lawfulness, fairness and Transparency | Purpose limitation | Data minimization |Accuracy | Storage Limitation | Integrity and confidentiality | Accountability.
  - **Function of the internal market**
    - Relates to the free flow of personal data between member states based on uniform binding rules for the protection of private data.
- Looking into the protection of the data
  - The most significant change to data protection impacting companies/ organizations around the globe in internal structure and ways of doing business.
- Discuss the impact of GDPR after two years
  - What has it generally meant for the companies?
  - What are the challenges of implementation for the companies?
  - How has companies coped with the requirements?
  - Which impact has it had on the business model for the content providers?

EU's survey on GDPR "Two Years"

- **Citizens are more empowered and aware of their rights**.
  - **69% of the population** above the age of 16 in the EU have heard about the GDPR and **71% of people** heard about their national data protection authority.
  - **User play more active role** with what is happening with their data in the digital transition.
  - Trust-worthy innovation, notably through a **risk-based approach** and principles such as **data protection by design and default**.
- Businesses, including SME, now have just one set of rules to which to adhere.
  - Benefit from the same opportunities, regardless of whether they are established and where the processing takes place.
- Creates level playing field for the companies not established in the EU but operating here.
  - Privacy compliance has become a competitive quality that customers are increasingly taking into consideration when choosing their services.
- GDPR being applied to new technologies – Risk based model, future EU framework for AI
- GDPR contribution to global data protection standards – emerged as a reference point and acted as catalyst for many countries considering how to modernize their privacy rules.
- GDPR facilitated international data flows – offer a modernized toolbox to facilitate the transfer of personal data from the EU to a 3rd country.

Enforcement Challenges in GDPR

- **GDPR implementation overview** – Incentivize organizations to see their data protection compliance and strategy as a business enabler.
- **Refining data types** – Poorly equipped for situations involving personal data. Uncertainties regarding pseudonymization and anonymization needs to be reduced.
- **Fragmentation** – local laws and authorities; Margin of manoeuvre led to the creation of differing rules.
- **Transparency** – With new obligations, led to an overload of information, some of which is only relevant for experts as opposed to generating more effective protection for the average user.
- **Purpose Limitation** - The GDPR states that purposes must be ‘specified, explicit and legitimate’ but does not provide clear requirements as to how concretely or abstractly a purpose may be described.
- **Same processing, multiple legal bases** – Same processing activities may fall under different legal bases simultaneously.
- EX.,
  - Consent
  - Data subject rights
  - Separate and joint controllers
  - 3rd country transfers

Overview of GDPR impact

Empirical findings

Company Related issues

- GDPR is generally regarded as groundbreaking and successful legislation and the appropriate measure required to aid governments and citizens in regaining control of data security.

- GDPR has directly impacted data privacy and security standards while also indirectly encouraging organizations to develop and improve their cybersecurity measures, limiting the risks of any potential data breach.

- Many organizations have hired or promoted Data Protection Officers to manage any organizational GDPR concerns regarding compliance. However, DPO in the organizational structure of companies – often resulting in lack of influence on strategic decisions.

- Organizations assessed for compliance in one nation state by Data Protection Agencies (DPA) is free to operate throughout all European countries.

- DPAs in the different countries are giving very different levels of support to companies and act apparently very different in pursuing data breaches.

- The GDPR creates a level playing field with companies not established in the EU but operating here. It is globally becoming clear to organizations that compliance with the regulation is mandatory for all handling data related to EU-activities – by 2020 446 cases of GDPR violations was enforced outside of the EU.

User Related Issues

- Some organizations have experienced, data breaches have a devastating impact on the reputation of an organization.
  - Users and customers value their privacy, and their confidence can be irrevocably damaged if a breach of data does occur and their information is made available unknowingly.

- Users are more willing to share their private information if they believe their data is being stored and used in line with GDPR.
  - If an organization can become a trusted holder of information, their odds in creating a long-lasting and loyal relationship with a customer will improve significantly.

- Users and customers are far more likely to accept the mandatory opt-in from organizations and businesses they are interested in.

- The new consent form allows customers to control if and how they are contacted by an organization, empowering them with the full control of who and how they share their data.

The Survey

Four large organizations head quartered in Denmark

Represent large, international companies with many employees and offices abroad.

Purpose

To understand the economic impact and challenges that GDPR has had on the companies/organizations.

The survey asked the participants to describe the actions that was taken to comply with the GDPR.

The Survey

- Questions
  - Please, describe the actions and process it has taken in your company to comply with the GDPR? (If you do not fully comply to the GDPR, please explain the challenges)
  - How has GDPR made an impact on your business?
  - Please, give an estimate on the economic impact it has had on your company (percentage of costs)
  - Have you encountered any unfortunate challenges in the process of compliance with GDPR? Which?
  - Where do you see GDPR is leading?
  - Do you see benefits of GDPR – which?

The Survey

- The following elements were mentioned:

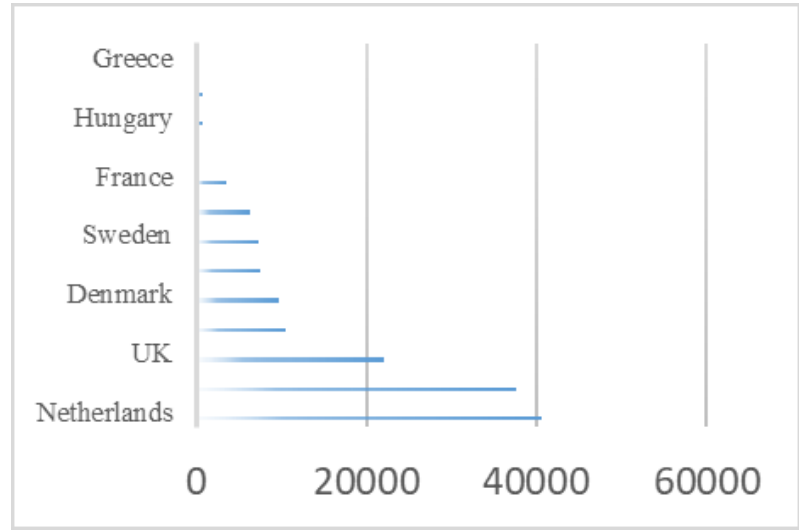
  – Data flows to identify data processing, storage and others.
  – Implemented Vendor Management Program where the GDPR is a key element.
  – Started an IAM program to gain better control and governance regarding access to systems and on and off boarding of employees
  – Design of data programs to ensure compliance.
  – Appointed local responsible in different markets to ensure local embedding and maintenance of compliance
  – Yearly global activity plans to ensure that compliance stays on the radar in the right markets, training, awareness campaigns etc.
  – Control framework to monitor processes and procedures are in place in different markets
  – Establishment of center of excellence
  – Education of employees
  – Establishment of processes and procedures to comply with GDPR and still run the normal business

Drivers

Legal Requirements & Requirements to Organizational structures

Drivers – Legal Requirements

- Fines
  - GDPR fines are organized in two levels and applies to any entity that handles EU citizens data.
    - The upper level of fines can go up to 20 million Euro or 4% of global turnover and lower level can go up to 10 million Euro or 2% of global turnover.
    - The fine regime is uniform and defined at EU. However, this is not the case for the implementation.
  - Total number of notified data breaches in the period May 2018 – January 2020 ranges from 40,647 in the Netherlands to 232 in Greece and Germany 37,636, UK 21,181 breach notifications.
  - Total amount of fines issued for data breaches in the EU until end of Jan 2020 was 114 Million Euro and over 160,000 data breach notifications.
  - UK British airways got a record 200 million penalty (reduced to 20 million Euro)
  - Marriot hotel chain got a 100 million fine (reduced to 20,6 million Euro)



Drivers – Requirements to Organizational structures

Data Protection Officer

Role already existed in some organizations and gave it statutory importance. However, not all the companies are required by law to formally appoint a DPO to oversee GDPR compliance.

Book keeping

To fully appreciate the scope of the GDPR and duties towards compliance, it is important to understand the personal data organizations are collecting and that they already are in possession. The organizations must map the flow of personal information into, out of, and also within the organization.

Gap Assessment

This step is the start as well as an iterative process that lives within organization's lifecycle. This includes a comparison between the current security and privacy controls already embedded in the organization, policies and procedures vs. the control requirements from the regulation.

Policies, Procedures and Modify Processes

This step is where the organizations will update their initial and ongoing policies and procedures by fulfilling requirements from the regulation. In addition to this, to verify if the processes are complying all aspects of the data life cycle and privacy principles, the organizations might need to modify some processes.

Training of employees

Training employees within the organization is very important part of GDPR impact and dissemination. All the policies, procedures and processes fail if they are not handled and followed by skill and privacy-aware employees.

Monitor Compliance

Monitor of compliance often comes with internal accountability and involves many departments like IT, HR, Legal, Marketing, Sales etc. In addition, it also represents a constant overview and follow-up in all the above-mentioned steps.

Conclusion

- Two years after its entry into application, the GDPR has been an overall success, meeting many of the expectations.
  - Even if several areas for future improvement have also been identified.

- Like most stakeholders and data protection authorities, the Commission is also of the view that it would be premature to draw definite conclusions as to the application of the GDPR and to provide for proposals for its revision.

- It is likely that most of the issues identified by Member States and stakeholders will benefit from more experience in the application of the Regulation in the coming years.

- Increasing global convergence around principles that are shared by the GDPR offers new opportunities to facilitate safe data flows, to the benefit of citizens and businesses alike.