GDPR is coming… Are you ready?

GDPR Awareness Presentation

March 2018

The better the question. The better the answer.
The better the world works.

Building a better working world

Contents

GDPR Definitions

Personal Data:

Any data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual; Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier etc.

Sensitive Personal Data:

Personal data consisting of information as to - (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Profiling:

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements

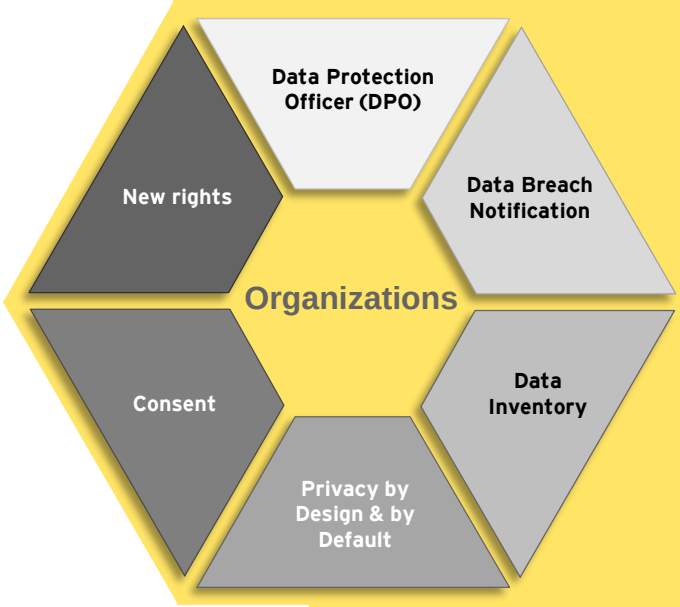
GDPR Overview

- Adopted in the 27th of April 2016
- It comes into force in the 25th of May 2018

- Non compliance could lead to fines of up to 20.000.000€ or 4% of global turnover

- It applies to all foreign companies processing data of EU residents
- Harmonization throughout the EU, makes it easier for non-European companies to comply with these regulations

More stringent and prescriptive data protection compliance challenges



- Introduce the role of a Data Protection Officer (DPO)
- Know your data, including what your data is, where it is held at and how it is managed
- Obtain a clear and precise consent when processing personal data
- Be in the position to erase all data when requested by the subject
- Limit the access to your data as well the processing which takes place
- Perform privacy impact assessments
- Be in the position to report data breach within 72 hours
- Continuously monitor the data privacy risks throughout the organization

GDPR
EU General Data Protection Regulation

What is GDPR?

General Data Protection Regulation (GDPR), is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU)

Key Objectives

1. Give citizens back the control of their personal data
2. Simplify the regulatory environment for international business by unifying the regulation within the EU.

EY

Understanding the market's needs

Still a few organizations are not aware of the new regulation and what this means for their business.

Although many organizations are aware that GDPR is coming, they are struggling to figure out how to approach and tackle with the new requirements.

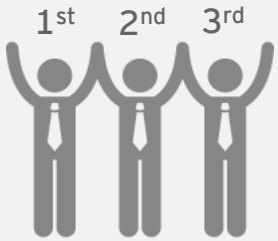
Most common mistake is to assign responsibility to only a "2nd line of defense" function: Information Security or Compliance or Legal Counsel.

The winning approach:
A Holistic View and Mindset

Organizations should assess readiness, create awareness and assign responsibilities throughout the whole enterprise as personal data is processed by almost all employees at some point of their day to day business.

We need to engage all 3 lines of defenses as to minimize the risks of non compliance to the GDPR requirements.

Compliance with the GDPR requirements is an enterprise wide issue!



Lines of Defense

1st Line of Defense: Data protection risks should be identified within business processes and mitigating controls should be operated throughout the business. Awareness over GDPR requirements should be at the same high level.

2nd Line of Defense: Compliance, IT Security and Legal need to provide insight and advice over the organizations operations as to ensure proper design of mitigating measures. Deep knowledge of GDPR requirements is a must.

3rd line of defense: Internal Audit and other independent assurers should include data protection in their audit plans as to increase the level of assurance towards compliance with GDPR requirements.

EY

Our approach

GDPR Readiness Assessment

We have developed a "GDPR readiness" maturity assessment tool through which we will conclude on the current state of your business environment. Our approach follows a holistic view covering all 3 line of defenses as well as all aspects of the business:

People:

The level of current GDPR awareness needs to be assessed. A roadmap covering specific actions as to elevate awareness and competencies will be prepared according to specific needs.

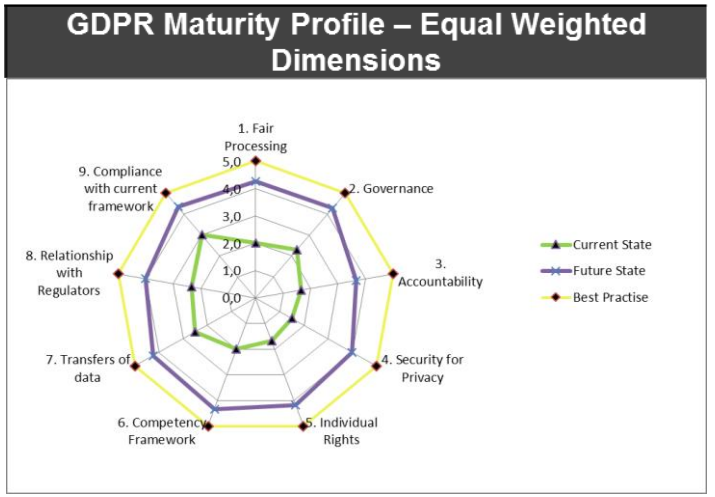
Business Processes:

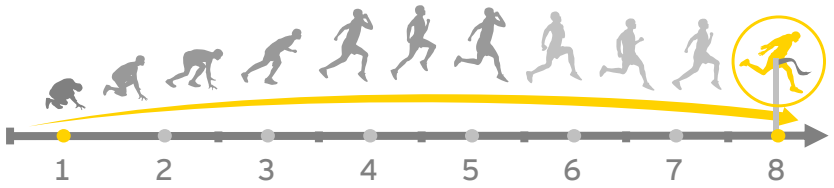
Our assessment covers Business processes, policies and controls as to ensure that GDPR requirements are covered throughout the whole business.

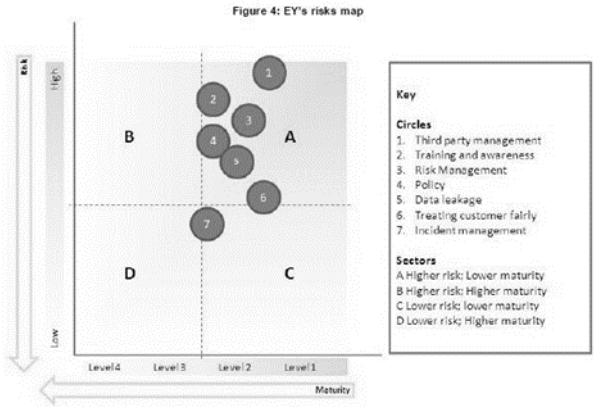
IT Systems:

Our approach covers the IT aspect of the business by assessing proper design of relevant IT policies and controls.

Our approach has been designed by a multidisciplinary team covering all key aspects affected by GDPR. By combining our competencies over **Legal, Compliance, IT** and **Risk,** we are confident that our approach will exceed your expectations and get you ready for the requirements set by the new regulation.







Our approach

GDPR Readiness Assessment

We have utilized our global methodology over "maturity assessments" as to identify current gaps towards compliance with the forthcoming GDPR requirements. We are confident that the below approach will fully meet your objectives and will support your efforts over building a compliant business environment.

A. Understanding of Current practices

- Identify key stakeholders from each function which will eventually form the data protection coordination team.
- Engage in meetings with key stakeholders of each function as to understand day to day business and current practices over processing of personal data throughout the whole entity.
- Identify and review key documents (e.g. Policies, Standard Procedures, contracts etc.) as to identify fundamental gaps.
- Identify and review the organization's key systems and applications as to understand how these are utilized, what sort of data is processed and how these are interfaced.
- Identify third parties with which the organization has established a business relationship.
- Identify and document all points which personal data is being processed.

Work Product: *N/A Preliminary phase/gathering info*

Added Value for you: Through interaction with your people during this phase of the project, we will have the opportunity to practically assess their awareness over Data Privacy issues and understanding of GDPR requirements. At the same time, as we acknowledge the significance and difficulties in changing the way your people do business (culture), we will help you manage and communicate these changes on a constant basis.

B. Assessment of current state

- Meet with project liaison as to define the desired future state for your organization.
- Utilize "maturity assessment tool" as to assess each pillar of the GDPR and define current maturity of your organization.
- Identify gaps resulting from the comparison of current and future state .
- Prepare preliminary report including all gaps identified.
- Agree with key stakeholders and project liaison our understanding of current state and the gaps identified through the assessment.

Work Product: Preliminary report including only gaps (for discussion purposes)

Added Value for you: Our methodology acknowledges that companies may decide to adopt leading practices instead of only complying with the new requirements. Under this context the future state is mutually agreed with you as to identify cases which there is a cost benefit in implementing leading practices.

C. Preparation of roadmap/action plans

- Prepare a recommended action plan for gaps identified under each pillar of the GDPR.
- Quick wins will be presented distinctively as to easily assign for implementation
- For actions which should be viewed as projects, we will prepare "Project briefs" with suggested approach for execution.
- Actions will be prioritized depending on the significance and effort/duration required for implementation.
- Initial planning of implementation as well as communication of next steps will be supported by our team.

Work Product: Final report including current maturity, gaps and roadmap with prioritized actions

Added Value for you: We acknowledge that complicated solutions do not prove expertise and definitely cannot serve as a means of efficient knowledge transfer. In this context we commit to deliver you material which will really serve the purpose and reduce the learning curve of your people.

EY

Our approach
GDPR Readiness Assessment

Overview

Our team of multidisciplinary professionals has decomposed the GDPR requirements under 8 distinct dimensions which are further broken down to specific components, as to allow for a practical and straightforward assessment. In more detail the dimensions and relevant components assessed are presented below:

GDPR Dimensions and components

1. **Fair Processing**
   a) Transparency
   b) Collection & Purpose Limitation
   c) Consent
   d) Quality
2. **Governance**
   a) DPO
   b) Data Privacy Team
   c) 2nd and 3rd Line of Defense
   d) Data Protection & Security Policies
   e) Procedures & Controls
3. **Accountability**
   a) Data Inventory
   b) DPIA
   c) Data Protection by Design & by Default
4. **Security for Privacy**
   a) Data Breach Readiness & Response
   b) Security of Processing
5. **Individual Rights**
   a) Right to Information and Access to personal data
   b) Right to Rectification
   c) Right to Erasure (Right to be Forgotten)
   d) Right to Data Portability
   e) Right to Object and Restrict Processing
6. **Competency Framework**
   a. Awareness
   b. Training
   c. Certification
7. **Transfers of Data**
   a. Cross-border Transfers (BCRs, SCCs)
   b. Third Party Management
   c. Joint Controllers
8. **Relationship with Regulators**
   a. Notifications/Application for Authorization
   b. Co-operation/Consultation with DPA

Our approach
GDPR Readiness Assessment

Maturity Assessment tool

Our tool has been prepared as to allow for a quick and focused assessment. It has been set in the basis of 5 maturity levels. The 1st level of maturity indicates an Inefficient environment in relation to the requirements whereas level 5 indicates an Optimum (leading Practice) level of maturity. Each Dimension and its components (presented in previous section) are assessed in order to conclude on their current level of maturity. Following, gaps between the current level assigned and the desired future state are identified. Following the levels of maturity along with a short description are presented:

1 Insufficient

This level of maturity indicates that the company is operating without taking into consideration key aspects of the requirements. Inefficiencies usually lie at the "design" level.

Effort and resources required as to achieve compliance from this stage usually are high.

2 Developing

This level of maturity indicates that the company has acknowledged and identified their gaps. Efforts towards designing the proper environment have began. Usually requirements are covered by distinct functions (in silos)

Effort and resources required as to achieve compliance are moderate

3 Standard

This level of maturity indicates that the majority of current requirements are met and a basic design of compliant practices is in place. Under this level the exceptions identified are mainly operational or minor alteration to current design are required.

Effort and resources required as to achieve compliance are low

4 Advanced

The level of maturity indicates that the company is operating in a way which demonstrates adherence to the requirements. Proper design is in place and the business practices are efficient.

Minimum effort and resources required as to sustain efficiencies.

5 Optimum

The level of maturity indicates that the company is operating at a level over and above the requirements. Business practices established by the company are considered leading and are consist of an example for others.

Our approach

Data flow mapping & Data Inventory

Below we have utilized our global methodology as to prepare a data inventory template (as requested per article 30 of GDPR) and populate it for two selected high risk areas as well as document the life cycle of data (data flow mapping) for two selected high risk areas. Overall, our approach will also include the design and documentation of a process regarding the updating and monitoring of data flow and data inventory.

A. Understanding of Current practices

- This step will be covered through the GDPR 360 assessment phase.

Work Product: *N/A*

Added Value for you: Our methodology ensures that we will cover all required inquires and document gathering required for data flow mapping and data inventory preparation through the preliminary phase of the GDPR 360 degree assessment. Under this context the added value for you will be the utilization of knowledge gained from the assessment project which translates to lower total costs for your company.

B. Data flow mapping

- Validate understanding of process points over which personal data is being processed.
- Preparation of function map for two high risk data processing activities including distribution points of personal data towards third parties.
- Preparation of flow charts for two high risk data processing activities, presenting the personal data end to end lifecycle (from collection to destruction).
- Design and Documentation of process required for updating and monitoring the data flow.

Work Product: Data flow maps for two high risk data processing activities, updated data classification

Added Value for you: We acknowledge that your goal is to obtain sustainable results as to be in the position to follow appropriate practice after the completion of this project. Under this context we will provide you with the required tools and knowledge as to properly update and monitor your personal data flows .

C. Data Inventory preparation

- Prepare the data inventory template according to the specific requirements of your company.
- Document all required fields as to have a complete data inventory covering all current points of personal data processing per purpose.
- Validate information with key stakeholders responsible for each point of personal data processing.
- Design and documentation of process required for updating and monitoring the data inventory.

Work Product: Data Inventory template populated for two selected high risk areas, process documentation over updating and maintaining a data inventory

Added Value for you: Our goal is to provide you with the required tools and knowledge as to be in the position to maintain the results derived through this project. A comprehensive process along with a comprehensive data inventory file will provide for evidence of proper data management.

Overview of our proposed approach

Data Protection Impact Assessment (DPIA)

Below we have utilized our global methodology over "DPIA" as to understand current data processing activities, identify high risk areas, design and develop a tailored DPIA methodology and template that fully meet your needs as well as perform one DPIA over a selected high risk area. We are confident that the below approach will fully meet your objectives and support your efforts over building a GDPR compliant business environment.

A. Understanding of Current Data Processing Activities

- This step will be covered through the GDPR 360 assessment as well as the Data flow mapping and Data Inventory (as per article 30) validation phases.

Work Product: *N/A*

B. Identify High Risk Areas

- Define thresholds and triggers for the DPIA process (high-risk processing activities)
- Identify high risk areas that will be subject to DPIA.
- Communicate and validate high risk areas with key stakeholders.
- Prioritize high risk area.
- Prepare high risk area reporting.

Work Product: *Detailed high risk area reporting*

C. Prepare DPIA Methodology and Template / Perform one DPIA

- Prepare the tailored DPIA methodology, including the determination of the impact factors (factors as to determine whether the impact of a processing operation on the protection of personal data is high / medium / low).
- Develop a customized DPIA template in accordance to the defined methodology and GDPR requirements.
- Provide and explain the DPIA methodology and the template method of use to key stakeholders.
- Perform one DPIA over a selected high risk area.
- Prepare the DPIA report including the impact level of the processing activities and the privacy controls required as to mitigate identified risks.

Work Product: *Methodology over performing a Data Protection Impact Assessment (DPIA) along with the relevant template, Data Protection Impact Assessment (DPIA) report.*

Questions

EY

Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 152,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

EY refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.