

GDPR is coming... Are you ready?

GDPR Presentation

May 2018



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



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.

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.

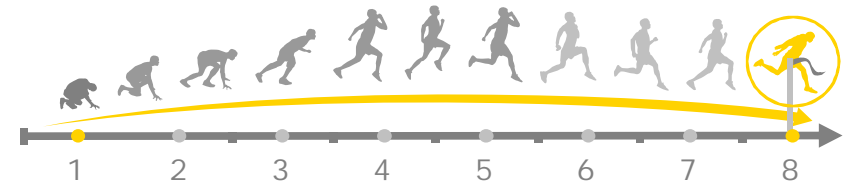
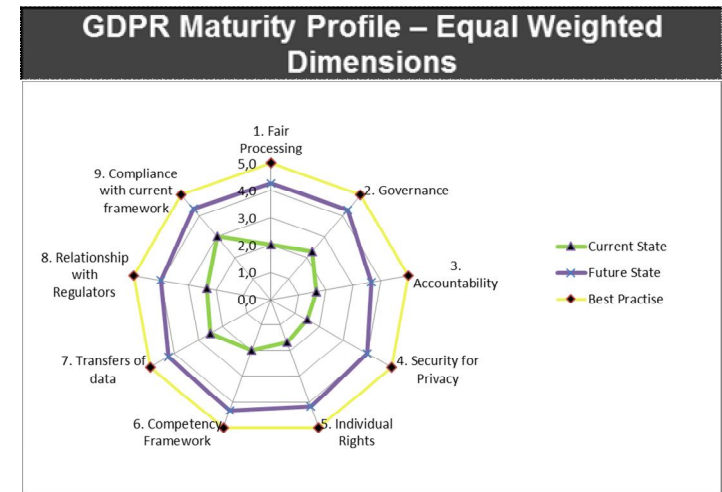
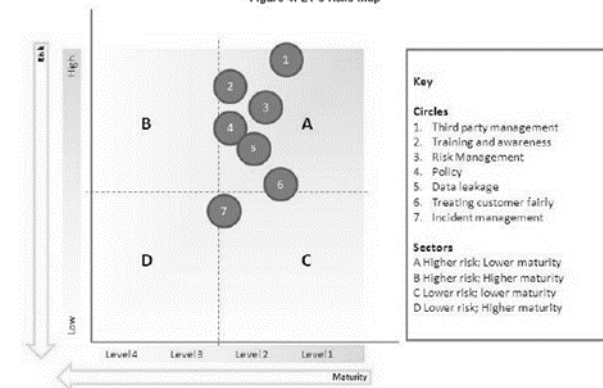


Figure 4: EY's risks map



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.

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.

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: *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.

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.

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.

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

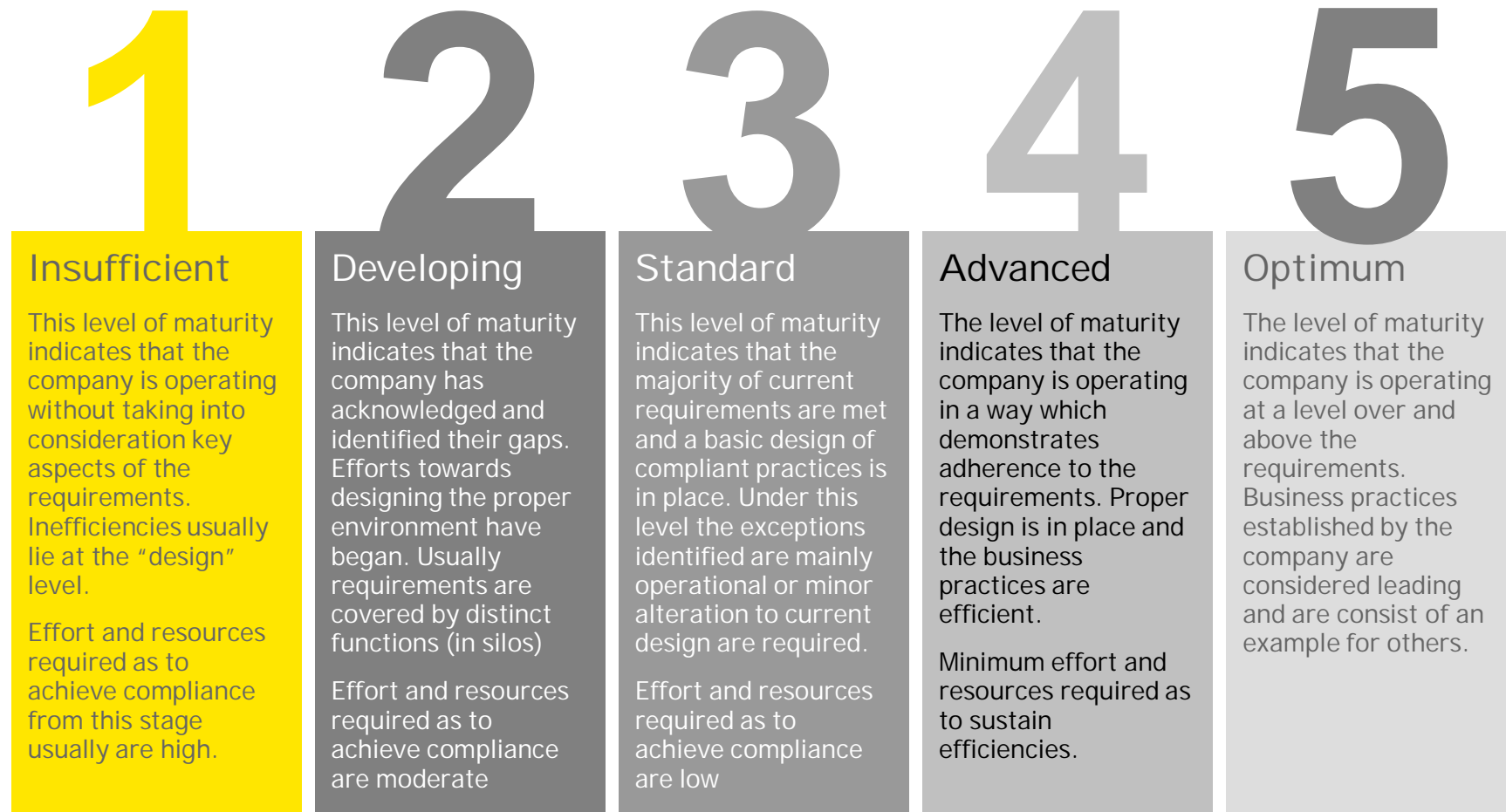
1. Fair Processing
 - a) Transparency
 - b) Collection & Purpose Limitation
 - c) Consent
 - d) Quality
2. Governance
 - a) DPO
 - b) Data Privacy Team
 - c) 2nd and 3rd Line of Defense
 - d) Data Protection & Security Policies
 - e) Procedures & Controls
3. Accountability
 - a) Data Inventory
 - b) 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:



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.

© 2016 EY. All rights reserved.
Confidential and proprietary.
Subject to contract.