GDPR Audit – Test your environment… sustain your design

Alexandros Hassapis
EY Director – Forensic & Integrity Services

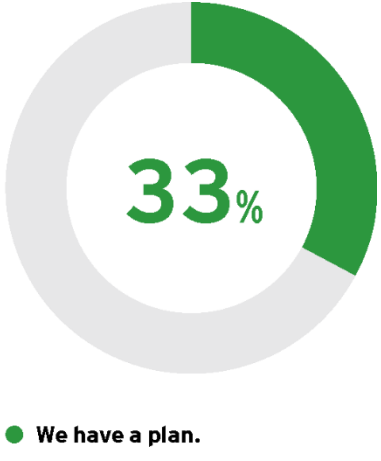
The better the question. The better the answer.
The better the world works.

Building a better working world

Contents

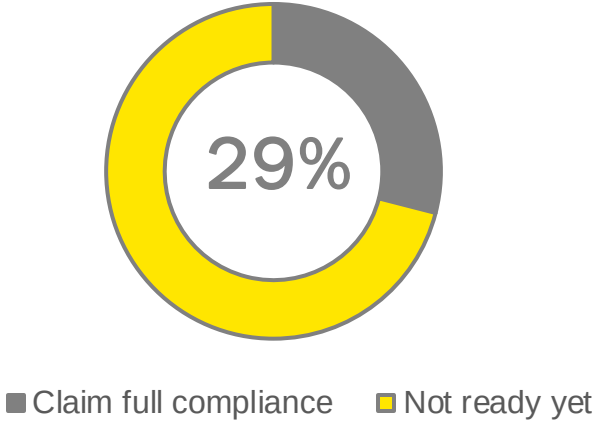
GDPR – Current status
Statistics

Survey conducted by EY in cooperation with IAPP in 2017 revealed that only 33% of organization had a plan as to how to tackle with GDPR challenges.



Survey conducted by ISACA during April 2018 revealed 29% of companies surveyed claim to be fully compliant after the 25th of May

"Source, ISACA, GDPR Readiness Survey, May 2018"



Although some claim full compliance… whether companies are indeed operating in compliance is yet questionable

GDPR – Current status
Is claiming compliance enough?

Claim: We have designed access controls under which users are granted role based access rights to our systems and applications

Fact: Although the company has established access controls for its systems and applications, the rights have not been granted by considering the level of personal data processing. The most common example is Customer Relationship Systems (CRM) for which full access (right to read data, right to alter data, right to save data, right to access full data set etc) is granted to almost any employee who is client facing.

Access controls should be re-designed as to limit the users' access only to the personal data needed for his/her duties and restrict unnecessary processing

GDPR – Current status
Is claiming compliance enough?

Claim: We have reviewed all our personal data processing activities and have ensured that there is a proper legal basis for processing

Fact: The company considered that they are in compliance because they asked for the consent of all data subjects for all processing taking place. It turned out that from a total of about 50 processing activities, consent was the legal basis for only 6 processing activities.

The company should have identified the cases which there is a legitimate basis other than consent and request for consent only for the cases required

GDPR – Current status
Is claiming compliance enough?

Claim: We have assigned a DPO in our company

Fact: Most of the companies claiming the assignment of a DPO have selected an employee who does not meet the requirements regarding the absence of any conflict of interest. Such examples are the assignment of the Internal Auditor, the company's legal counsel, the IT Security officer while still having the responsibility of their prior position.

The company should assign the role of the DPO to someone who can execute his/her duties independently. In more detail he/she should not be someone who determines the purposes and means of the processing of personal data.

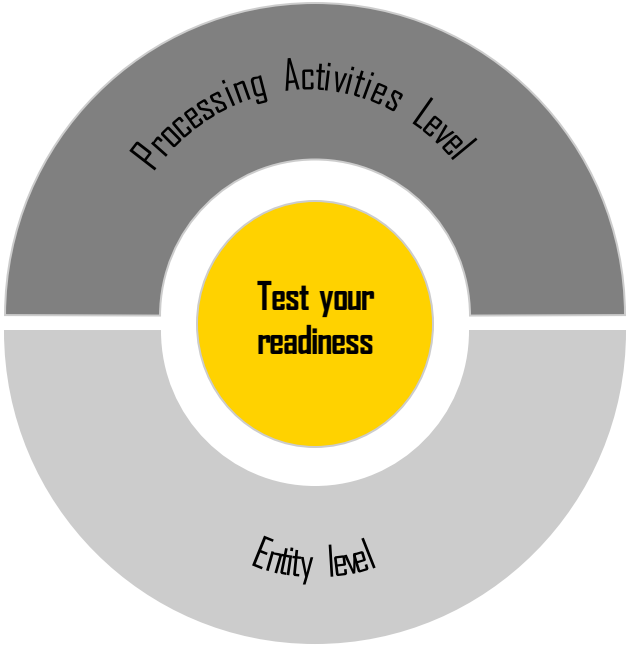
GDPR – Current status
Is claiming compliance enough?

Claim: We have taken all measures as to ensure safe storage and distribution of data

Fact: Although the company had designed key IT controls (Network controls, Access controls etc.), files containing personal and sensitive personal data were stored and distributed without the application of key controls which are designed to safeguard the data within the file (password protection of file, encryption of data within the file etc.). Moreover the company had not classified the personal and/or sensitive personal data processed as to impose specific controls according to their classification.

Data should be classified within the company and controls safeguarding the data while stored and distributed should be applied according to their classification.

GDPR – Audit
Overview



Phase 1: Prepare

1. Identify Risks
2. Document Control Objectives
3. Identify Controls

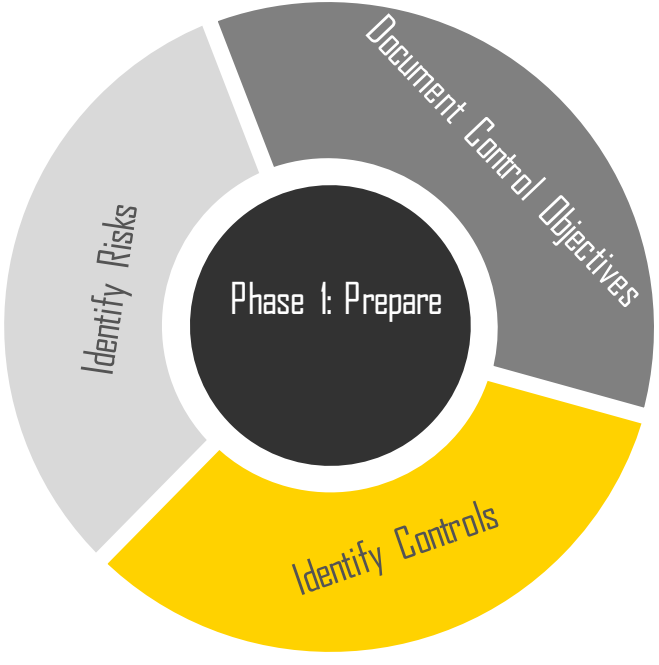
Phase 2: Audit

4. Test the Design of Controls
5. Test Operating Effectiveness of Controls
6. Identify Exceptions

Phase 3: Report and Monitor

7. Report on overall compliance
8. Monitor Exception Action Plan
9. Apply Compliance Program

GDPR – Audit
Phase 1: Prepare



1. Identify risks

- Identify risks at an entity level
- Identify the risks which are applicable for each point of personal data processing, based on EY GDPR normative risk model:

  Risk categories: i) Collection risks, ii) Recording risks, iii) Storage risks, iv) Archiving risks, v) Usage risks, vi) Transfer risks and vii) Disposal risks

2. Document control objectives

- Document what the purpose of the entity level and process level controls should be in order to mitigate the risks identified

3. Identify Controls

- Design and document the control descriptions which could mitigate the entity level and process level risks.

A Risk and Control Matrix (RCM) should be prepared for each personal data processing activity included in the data inventory

GDPR – Audit
Phase 2: Audit

4. Test the Design of Controls

- Challenge the design of existing controls as to assess the adequacy of risk mitigation
- Test to be commenced by walking through one sample of the control

5. Test the Operating Effectiveness of Controls

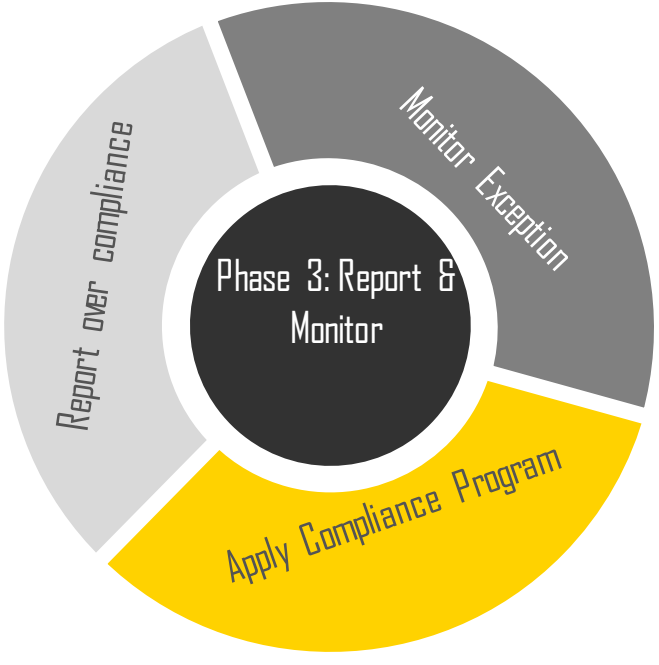
- Decide on sample for testing
- Prepare audit program
- Execute testing of controls

6. Identify Exceptions

- Identify and verify exceptions with control owners
- Agree action plans with control owners

For cases in which controls do not exist, new controls should be designed by the processing activity owner after consulting the DPO

GDPR – Audit
Phase 3: Report and Monitor



7. Report on overall compliance

- Conclusions over control effectiveness along with exceptions identified and relevant are reported to executive management
- Data inventory is updated as to depict the efficiency of particular measures

8. Monitor Exception Action Plan

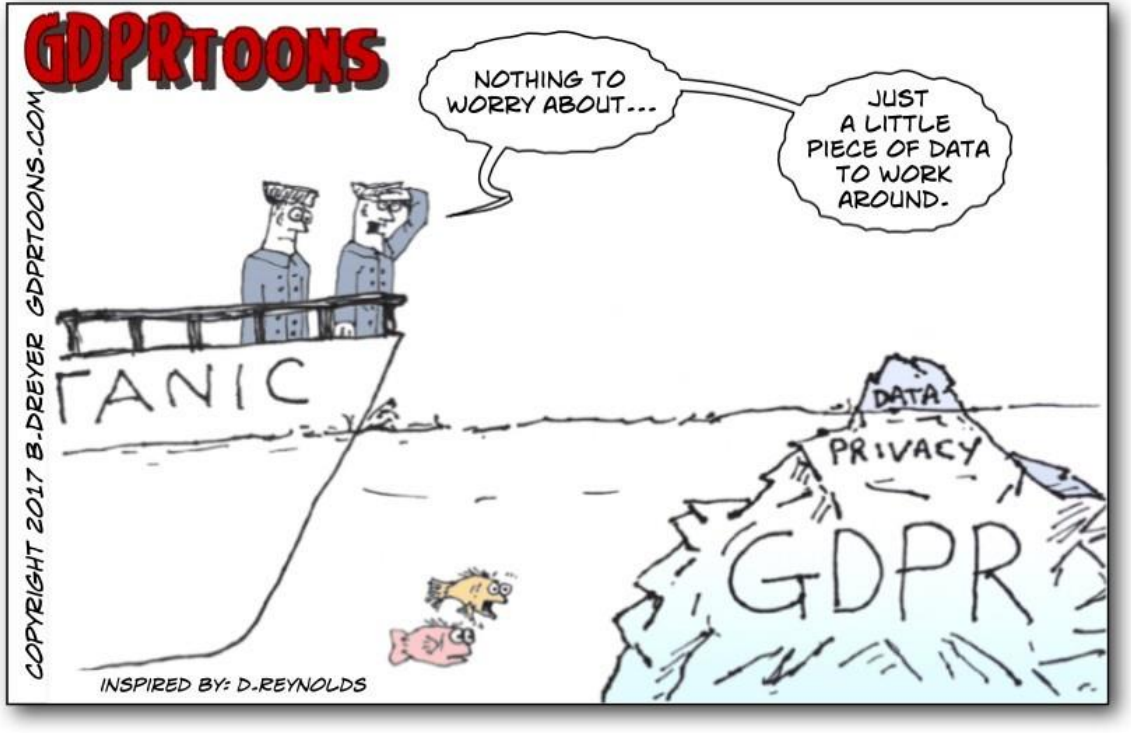
- Follow up with control owners as to ensure proper and timely completion of agreed actions
- Report on any given delays concerning the completion of actions as for executive management to assume the risk or impose authority

9. Apply Compliance Program

- Validate Risk & Control Matrix and perform the GDPR audit on a periodic basis (at least yearly)

By connecting your RCMs with your data inventory you can easily provide evidence of efficiency over organizational measures which have been designed to mitigate GDPR related risks

GDPR – Audit
Conclusion



GDPR – Audit
Questions?

THANK YOU

EY

Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the 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 ey.com.