GDPR – Why do you need a CISO?

Table of Contents

1. Introduction

The General Data Protection Regulation[1] ("**GDPR**") introduces new European data protection rules that will directly apply in all EU Member States. GDPR will replace the current European Data Protection Directive 95/46/EC, which left the Member States with a considerable margin for implementation of the Directive's general principles when transposing them into national law. In view of the new enforcement powers of national data protection authorities and of the potentially drastic sanctions, compliance with the new GDPR is essential.

Despite significant attempts to create an adequate level of awareness, many organizations are still wondering how to tackle GDPR.

The way the regulation is written leaves doors open, although the Article 29 Data Protection Working Party ("**WP29**") recently released guidelines on DPOs[2].

DPO is not a new concept. Some countries (e.g. Germany) have already implemented a similar type of function to address Data Privacy. Likewise, large organizations, or those processing sensitive information, also have a Privacy Office as a Governing function. However, most do not have a DPO.

In contrast, the importance of the Chief Information Security Officer ("**CISO**") has increased over the past few years with the move to digital and rise of organized cyber threats. The CISO is in charge of security of information security, which includes private data.

This document aims to provide guidance to organizations looking for a structured approach to addressing a GDPR programme. It also emphasizes the importance of the CISO as a key player for successful implementation.

2. Description of the various GDPR dimensions

GDPR is a complex regulation involving various parties of an organization. To provide more clarity, it can be split into four main dimensions: Legal Compliance, Data Governance, Information Security and Technology. Each one acts on a different level of a company and each dimension must be tightly connected and integrated.

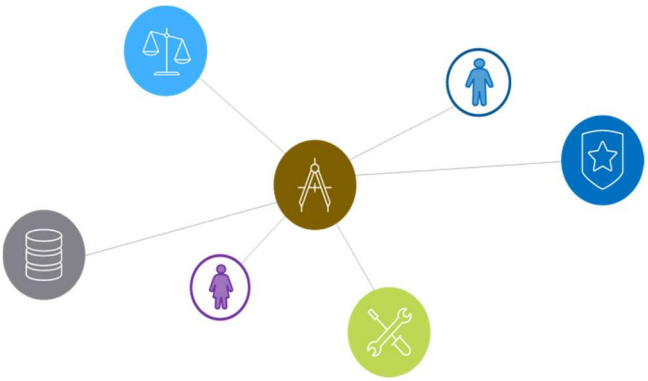
It is essential that all of the pieces of the puzzle are properly integrated and align with exactly the same objective: compliance with GDPR and hence protection of European citizens' rights.

[1] **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *O.J.*, 4 May 2016.**

[2] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), 13 December 2016 (as most recently revised and adopted on 5 April 2017), Brussels, latest version available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

The **integration function** must:

- **Implement** GDPR-compliant policies, process and procedures
- **Ensure** IT solutions will support business objectives
- **Ensure** businesses apply Privacy by Design and Privacy by default principles
- **Raise** awareness across the various parts of the business
- **Coordinate** data privacy activities

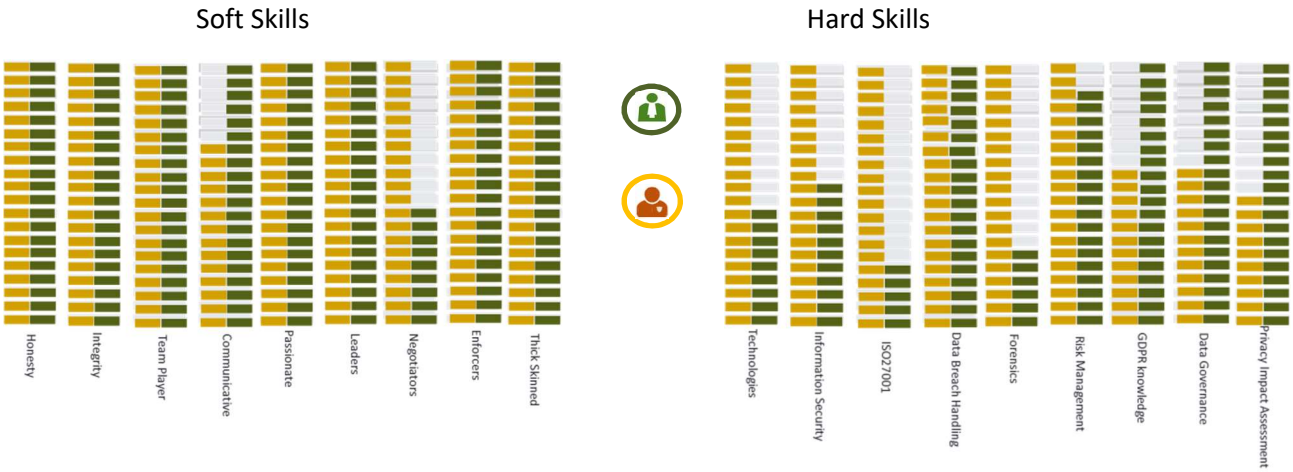


3. The responsibilities of a CISO vs. a DPO

A clear description of roles and responsibilities must be established to ensure proper governance of data privacy-related activities. Organizations must consider:

- Reporting lines
- Mission charter
- Key performance indicators
- Skills

Skills of a DPO vs. CISO



Understanding the Interfaces

Let's look at the various interfaces between the building blocks, as this will also intuitively help in clarifying the areas in which the CISO plays a major role.

Through this framework, organizations will be able to identify which key stakeholder within their organization is active in one or more of these dimensions. They will also establish a clear mission charter for each group, identify interfaces and interaction and define a clear end-to-end programme for implementing and maintaining GDPR compliance.

4. Identifying Risks and Opportunities

The major risks that organization may face during implementation of GDPR are:

- Poor Governance and a lack of clarity regarding roles and responsibilities, leading to potential poor implementation
- Waste of effort and energy, leading to significant operational cost increases

However, when properly organized, organizations will increase the CISO's return on investment, because they will be able to leverage Information Security Management processes to address many of the GDPR challenges. Examples are:

- Risk Assessment
- Security Breach and Crisis Management
- Communication and Awareness
- Control Framework

5. Conclusions

Do I need a CISO?

A CISO is the best ally for organizations seeking to initiate a data privacy programme. DPOs are still being "trained" today and while many claim to be a DPO, they are a few and not very experienced.

The CISO will define GDPR requirements in the security strategy. He/she will manage information risk management, security incidents and crisis management, which are also GDPR requirements.

He/she can advise the DPO on technical solutions and facilitate the relationship with IT and vendors, with whom he/she has an existing, strong and well-established relationship.

Can the CISO be a DPO?

The need for a (mandatory) DPO must first be established according to GDPR and it is recommended not to mix the DPO role with the CISO role.

Organizations where a DPO is not mandatory need to evaluate the usefulness and value of formally appointing a DPO. Remember, it may also provide a competitive advantage as well. This could be achieved through outsourcing this function to organizations that can deliver the DPO function "as a Service".

There might be opportunities, especially when appointing a DPO is not mandatory, where the CISO function could absorb the task of a DPO. Even so, the following needs to be validated:

- **New skills**: remember, the bar is not set at the same level for each position;
- **Workload and resource allocations**: the DPO's responsibility cannot be assigned to the CISO without incurring overheads. Organizations should not take that decision to detriment of cyber security; and
- **Conflict of interest and segregation of duties**: the GDPR and WP29 make it very clear that the DPO must act independently. Depending on the type of organization and who the DPO reports to, this needs to be assessed. WP29 states clearly that senior management positions may result in a conflict of interests. Accordingly, the assessment should determine which functions within the organization would be deemed incompatible with the function of DPO; the function of CISO could easily be on that list. In that regard, if the CISO absorbs the tasks of the DPO, the function must be organized in such a way that no one (especially not the DPA) can confuse the CISO with a (mandatory) DPO, as defined by the GDPR. In other words, the CISO should not do exactly what a DPO would do under GDPR and he/she should not be referred to as a DPO.

However, in the current business context, with the move to digital and the adoption of cloud services, running a business without a CISO function or a DPO function may not be viable in the long term. All CEOs should ask themselves about the need for one and allocate a budget accordingly.

The board will always need to be aware of the Security and Privacy KPIs.

I have no CISO and no DPO, where to invest first?

Organizations should evaluate the scenarios below and assess which one will provide the right balance for meeting compliance obligations while managing the organization's risk appetite:

1. CISO and DPO in-house
2. CISO in-house, acting as DPO
3. CISO in-house, with DPO as a service
4. DPO in-house, with CISO as a service
5. CISO or DPO only
6. None of the above (unlikely)

Where to start?

Approach has developed a pragmatic framework to helping organizations develop a realistic GDPR compliance programme. Thanks to its unique capabilities and proven experience in GRC (Governance, Risk and Compliance), Approach provides organizations with expertise that will generate an immediate return on investment and confidence in reaching and maintaining an adequate level of compliance.

Approach works with partners and lawyers, who enable us to deliver an end-to-end solution that addresses all dimensions of GDPR.

6. About Approach Belgium

Approach has been operating in the Cyber Security industry for the past 16 years. The company's unique spectrum of expertise allows it cover the full value chain of cyber security, from strategic decision-making down to in-depth technical implementation.

Approach's vision is to deliver solutions across the whole lifecycle of information security and risk management, from assessing and advising to implementation, control and management, as well as training and coaching.

Approach's unique value proposition enables it to empower customers in their digital transformation programmes, in areas of compliance such as GDPR, as well as on innovative projects such as smart cities, mobile apps and IoT.

You can find us on , , or on our website: www.approach.be

7. About the authors

Laurent Deheyer
Information Security Risk Professional
Cyber Security Consulting Director at Approach Belgium Laurent.deheyer@approach.be

Marc Degembes
Senior Information Security Consultant at Approach Belgium

Michael Raison
Senior Information Security Consultant & Auditor at Approach Belgium