GDPR and Corporate Governance

The Role of Internal Audit and Risk Management One Year After Implementation

ECIIA FERMA

November 2019

Content Map

Forewords

ECIIA and FERMA

04

02

Executive Summary

08

03

Key Findings and Recommendations

10

04

Summary of Results

16

05

GDPR and Internal Audit:
Independent assurance over key risks relating to the GDPR

29

06

GDPR and Risk Management:
Integration of the assessment of data privacy risks

33

07

Appendix

37

Forewords

ECIIA Foreword

The EU General Data Protection Regulation (GDPR) Directive was implemented one year ago. Together with cybersecurity, data privacy has been rated as a top priority risk of the modern era, in the recent "Risk in focus for 2020: hot topics for internal auditors", published in September 2019 by the ECIIA[1].

ECIIA and FERMA have collaborated on a governance model to align cyber risk and business strategy in 2018. In 2019 we have decided to work together again on a survey of practitioners in order to collect experience about the GDPR implementation and define key recommendations.

It is more important than ever to incorporate GDPR requirements in the business strategy to leverage on it as a differentiation factor towards competitors.

As governance and risk specialists, the internal audit and risk management functions are well placed to provide insight about GDPR through assurance to boards and senior management, as well as to other stakeholders. They can assist the understanding of the various risks of non-compliance, which go beyond the potentially significant fines. We have also identified key recommendations for the internal auditors, based on best practices collected.

The importance of a strong corporate governance remains a key aspect to comply with the regulation.

As the Three Lines of Defence model is already adopted and used by relevant regulators in Europe (as the ones overseeing banking and also insurances industries), we could imagine the European Commission also leveraging on the Three Lines of Defence model, namely for its incorporation into upcoming GDPR related directives and regulations.

Therefore, I would like to thank all members of the ECIIA -FERMA Group for their very valuable input.

Thierry Thouvenot
President
European Confederation of Institutes of Internal Auditing (ECIIA)

1 www.eciia.eu

FERMA Foreword

The GDPR is now one of the most famous pieces of EU legislation adopted over the last decade, one of the few to be known even by the general public. This transformative law required an unprecedented effort from every business dealing with EU citizens' data to adapt their products, services and processes to the new regulation.

GDPR has shown the ability of the European Union to set norms with a global reach, imposing obligations on non-EU organisations and perceived now as a model for other countries when it comes to data privacy laws.

Since almost every organisation is affected, FERMA and ECIIA share a common interest in the new roles of the risk management and internal audit functions regarding the GDPR and personal data related risks.

It is important for the risk and insurance community to understand the integration of the GDPR in the enterprise risk management (ERM) process and its impact on corporate governance, notably the relationship of the Data Protection Officer (DPO) with the risk management function. This document will serve as a baseline to guide our efforts as a European federation and promote a professional practice of risk management for privacy risks.

Beyond avoiding non-compliance and fines, building a high level of maturity for the management of privacy risks and a full compliance with GDPR is likely to become a market differentiator for most stakeholders: boards, shareholders and the civil society...

At the same time, concerns also arise about the possibility that organisations may refrain from innovating because of GDPR, notably in digital sectors with high growth potential like AI.
Our ambition is to provide European policymakers with unique insight on the implementation of the GDPR by companies. We hope these new elements will contribute to the future review of the GDPR, expected in May 2020.

Jo Willaert
President
Federation of European Risk Management Associations (FERMA)

02

Executive Summary

This paper focuses on the impacts of the GDPR on corporate governance practices in the year following its implementation. Most specifically, it looks at the roles played by internal audit departments and risk management functions.

Using surveys and targeted interviews, we have gathered input from internal auditors and risk managers from various industries throughout Europe to meet the following objectives:

- Promote good governance alongside the GDPR.
- Assess the current situation and identify issues and recommendations for the GDPR.
- Collect best practices regarding good governance for GDPR implementation, including the roles of internal audit and risk management.

Prior to the effective implementation of GDPR in May 2018, most European organisations invested significant efforts to comply with the regulation. As a result, substantial progress has been made in integrating GDPR compliance into existing corporate governance frameworks, as well as adapting corporate governance to address GDPR challenges.

Across Europe and beyond, compliance with the GDPR, or more accurately, compliance failures, has gained significant attention. Organisations need to respond to stakeholders' concerns about personal data, and boards need independent opinion.

The next review of the GDPR should recognise the relevance of a corporate governance framework, such as the Three Lines of Defence model, to embed the management of privacy risks in the organisation. It should also preserve the organisation's ability to innovate.

Data protection risks will decrease if the implementation of the GDPR is integrated in all business processes.

The first part of this report gives the key findings from the research and recommendations for stakeholders: European authorities, organisation governance bodies[1] and practitioners, including internal auditors, risk managers and DPOs.

The second part of the report explains the major findings used to support the recommendations. Detailed elements are available in the appendices.

1 Board and any Governing Body concerned

03

Key Findings and Recommendations

Substantial progress has been made in integrating GDPR compliance into existing corporate governance frameworks, as well as adapting corporate governance to address GDPR challenges. While acknowledging the progress in regard to these different topics, we can still make several recommendations to: European authorities, corporate governance bodies, practitioners (Internal Auditors, Risk Managers) and DPOs.

The findings in this paper are based on analysis of two anonymous web-based surveys and interviews of selected GDPR stakeholders between 31 May and 14 July 2019 across Europe.

Corporate Governance		
Key Findings	Key Recommendations per target	
▪ One year after the implementation of GDPR, the DPO is embedded into the corporate governance of organisations, when DPO is required ▪ Interaction between the DPO risk management and internal audit functions, respectively, is already significant (86% of respondents in contact after only one year). ▪ The DPO is considered to be part of the second line of defence. DPOs are assigned internally 89% of the time and 53% are assigned to an existing function, most often in the compliance or legal department. ▪ Most boards of directors and senior management generally expect full compliance from the organisation with some boards viewing the GDPR as "just another regulation" with which they must comply.	For the European authorities	▪ The GDPR regulation could leverage on a corporate governance framework, such as the Three Lines of Defence model, to naturally place the management of privacy risks in the organisation. (e.g. See 2018 Cyber Risk Governance report)
	For corporate governance bodies	▪ The roles and responsibilities of the DPO in relation to other roles in the organisation should be clearly outlined within a corporate governance framework. ▪ When not already in place, organisations should consider formally adopting the Three Lines of Defence model.
	For practitioners	▪ Working with DPOs, the internal audit and risk management functions should establish formal coordination points which, when integrated into a corporate governance framework, can confirm to both internal and external stakeholders whether compliance expectations are met.

Relations with the regulator		
Key Findings	Key Recommendations per target	
▪ Organisations are worried that insufficient information from national data authorities about the interpretation of technical and financial aspects of the GDPR could lead to unequal treatment of organisations, cross Europe, thereby creating a competitive disadvantage.	For the European authorities	▪ Efforts by the European Data Protection Board to harmonise both the understanding of the technical requirements (e.g. definitions and vocabulary around GDPR) and related enforcement actions (e.g. process and related fines) across the European national data protection authorities should continue. Furthermore, the European Commission should support cooperation between industry bodies and national data authorities to clarify the technical and financial aspects of the GDPR in its 2020 review.

Key challenges for companies		
Key Findings	Key Recommendations per target	
▪ Data breaches and their resulting reputation impacts are among the greatest GDPR risks. ▪ The main challenges posed by the GDPR implementation are: -the uncertainty or complexity of the GDPR's impact on existing systems and processes -the difficulty of incorporating innovation in business processes while addressing data privacy concerns -the resources required to maintain compliance and a culture of data protection.	For the European authorities	▪ The next review of the GDPR should preserve the organisation's ability to innovate.
	For corporate governance bodies	▪ Organisations should systematically involve the DPO in new business processes dealing with privacy matters.
	For practitioners	▪ Awareness of the day-to-day focus on data protection and the GDPR should be strengthened through stronger communication.

Internal Audit Practices		
Key Findings	Key Recommendations per target	
▪ According to internal auditors and risk managers, more than 70% of organisations' boards showed interest in receiving independent assurance from internal audit regarding the GDPR. ▪ About 68% of internal audit departments have already integrated the GDPR into their work and are responding to board or senior management requests for assurance using existing risk-based audit planning techniques. ▪ Roughly 47% of internal audit departments rate the GDPR reputation risk as high. GDPR compliance and operational inherent risks are also rated high by 43% and 41% of the respondents. ▪ Among the GDPR aspects covered by internal audit, governance is the first element (56% of audit plans), design is second (44%) implementation aspects are third (42%).	For corporate governance bodies	▪ Organisations are expected to respond to stakeholders 'concerns over personal data and boards have interest in receiving independent assurance regarding GDPR. ▪ Data protection risk should decrease if the implementation is integrated in all business processes.
	For practitioners	▪ Reviews on Data Privacy are now common part of Internal Audit activities: they should use standard methods to define the audit program for data privacy in each assignment, when required. It should at least cover governance, design and implementation aspects. ▪ Therefore, internal auditors should be duly trained to assess GDPR specific processes and impacts.

Risk Management Practices		
Key Findings	Key Recommendations per target	
▪ 91% of risk managers have implemented measures for preventing and dealing with data security breaches. These measures include embedding privacy risk assessments in new services and products, or setting up business continuity/crisis management plans. ▪ Of the 5 GDPR risk consequences for businesses, respondents consider 4 as high: reputational (47%), compliance (42%), operational (41%) and strategical (31%). The financial aspects are considered as a "medium risk" in 49% of cases. ▪ Of the risk managers' responses, 76% have already included data privacy in their global risk maps and 74% have performed an evaluation of the threats arising from the GDPR implementation.	For corporate governance bodies	▪ Risk managers play a relevant role to ensure a high level of preparation in the management of data privacy risks, including prevention and business continuity and crisis management plans for data breaches. ▪ Most organisations are considering GDPR risks from a holistic view (compliance, operational and reputational negative impacts) to purchase appropriate insurance.
	For practitioners	▪ Data privacy is embedded in most of the existing risk maps. ▪ Most risk managers include understanding of how privacy risks can affect all aspects of the business into their risk assessment so they can propose credible and documented mitigation measures to the senior management of the organisation.

Cooperation between internal audit and risk management on the GDPR		
Key Findings	Key Recommendations per target	
▪ 63% of professionals indicated that there is a good or a strong cooperation between internal audit and risk management, in relation to the GDPR. ▪ Only 11% stated that the cooperation was failing, compared to the 88% of the total sample who stated that there was some existing cooperation, one year after the entry into force of the regulation.	For practitioners	▪ Both professions should interact with the DPO, in line with the Three Lines of Defence model, to deliver a consistent assessment and reporting of data privacy risks that are not repetitive and add real value.

04

Summary of Results

1. GDPR and corporate governance

The Data Protection Officer (DPO)

- DPO is in place

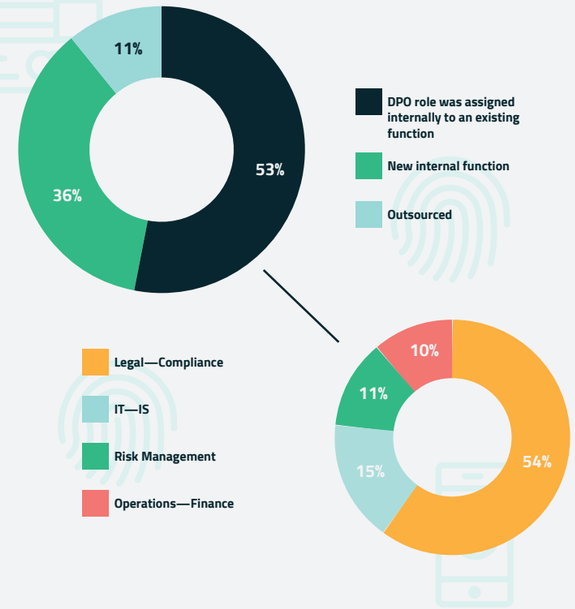
A large majority (82%) of the survey respondents and interviewees declared that their organisations have a DPO in place. This single aspect of compliance with the regulation, assignment of a DPO, could indicate organisations' response could be an indication of the prevalence of processing of personal data in today's business environment.

Of the internal auditor survey respondents, nearly half of the DPOs (49%) were assigned at the European Union (EU) level. Interviewees confirmed that there was an EU or even global DPO assignment, often in addition to country or legal entity DPOs in organisations dealing across Europe.

> "We have a data protection management system used for European DPO level reporting overview (monitoring is done locally).

- DPO is assigned to internal existing function

Question: If your organisation has a DPO, is it internally sourced or outsourced?



Of respondents that do have a DPO, 89% of those DPOs are internal to the organisation, with the majority having been assigned to existing internal functions. When assigned to an existing internal function, the role of DPO is usually (more than 50%) placed under a legal or compliance function.

> Because we have a huge number of employees, we need to take care of their data. Therefore, the DPO position was created in the HR department.

> "The DPO is an external body in our company. This allows us to promote independence and precision.

> In some cases several organisations can appoint a single DPO between them.

Based on the interviews, the DPO often has a legal background (previously or currently in the legal or compliance department). Interviewees also indicated that DPOs ideally have experience and thorough knowledge of the organisation, its systems and its stakeholders. This combination of experience aids the DPO in assessing, advising and reporting to management on data privacy risks. Experienced risk management and compliance professionals often have these same skills, thus the reason for sometimes linking the DPO with their departments.

Reasons for outsourcing remain unclear. Factors that drive externalisation of the DPO role could be the absence of an individual with the right experience or profile, a perceived higher level of independence, or the apparent lack of a need for a full-time DPO, based on the amount of personal data processed.

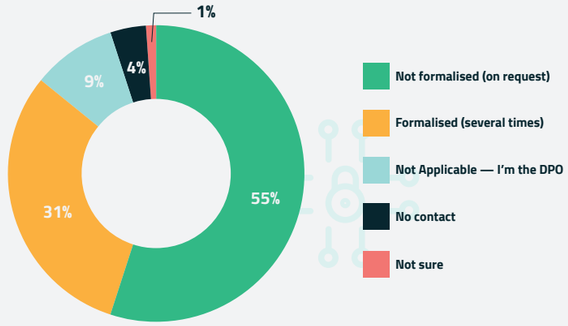
Interviewees often mentioned that even when the role is not outsourced, the internal DPO is supported (with budget assigned) by external legal expertise on GDPR.

The majority of organisations have assigned DPOs internally, often to existing functions, and to individuals with perceived expertise in data privacy topics. Those internal DPOs are most often placed in legal or compliance departments. Two factors that appear to drive the decision to assign a DPO internally: the amount of personal data processed and the expertise available internally to manage GDPR requirements.

2. Interaction and cooperation among practitioners

- Internal auditors and risk managers are in contact with the DPO

Question: What is your level of interaction with the DPO?



Of the responses from the survey respondents, 86% are in contact with the DPO. This shows that there is already significant interaction between this new function and the risk management and internal audit functions, respectively, after only one year.

> By often meeting with the DPO and the IT Manager, I try to make sure companies are aware of GDPR risks. This allows us to be proactive regarding future risks.

The 9% of survey respondents who indicated that they are the DPO were risk managers. In addition, a few interviewees served as joint risk managers/DPOs or joint internal auditors/DPOs.

Regarding a joint risk manager/DPO role, as mentioned in Topic 1 above, there are similarities that can be made between the experience and skill sets of professional risk managers and those required of DPOs as described in the GDPR. Common requirements are: performing a thorough risk assessment, reporting to top management and maintaining confidentiality.

According to the survey and interview results, joint internal auditor/DPO roles are less common. This is logical considering the internal auditor's requirements for independence and objectivity.

> We need to improve the collaboration with the communication department because they have the competence to assess reputational consequences that could hit us, which is not our core competence as Risk Managers.

▪ The Three Lines of Defence Model is applicable to GDPR requirements

Nearly one-third of survey respondents have formalised interactions with the DPO, indicating that many organisations have quickly integrated the DPO within their governance processes. As described by interviewees, that formalisation of roles and interactions often follows the Three Lines of Defence model[1].

The DPO is considered part of the second line of defence. The DPO's primary role is to provide guidance across the organisation (e.g. set standards and tools, establish reporting requirements, advise on Data Protection Impact Assessments (DPIAs), manage implementation projects). The DPO might also undertake internal reviews or oversee external reviews of the level of compliance throughout the organisation, being the contact for the Supervisory Authorities. The surveys' results show that the DPO reports at least annually on its activities and consolidates reporting to the board of directors and other supervisory or management bodies. The DPO is part of the enhanced focus on accountability.

1 The Three Lines of Defence Model: https://www.eciia.eu/what-is-internal-auditing/

With respect to risk management, this second line of defence integrates data privacy risks into the organisation's ERM. When possible, data privacy risks are quantified in line with the organisation's existing risk scoring and mapped along with other risks that the organisation faces.

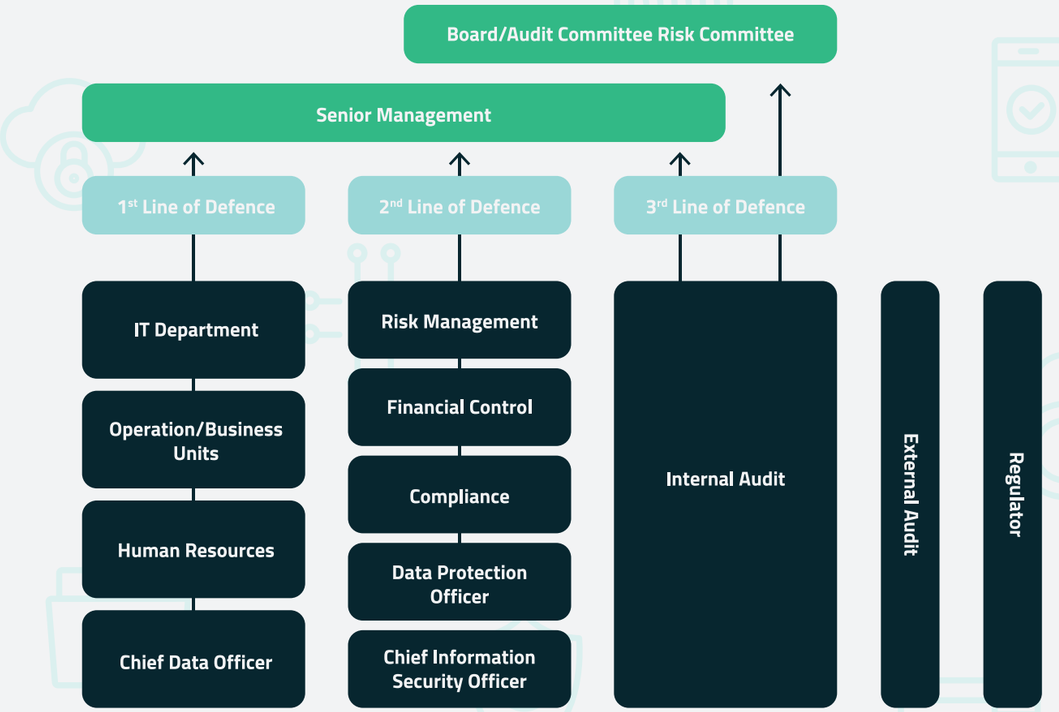
Interviewees overwhelmingly indicated that the business units or local entities who directly handle (process or control) personal data are responsible for ensuring compliance with the GDPR. As the GDPR requires the processor and/or the controller to take responsibility for compliance, this responsibility sets up the business units or local entities as are the first line of defence against data privacy risks.

> "We have a privacy committee created by first line's representatives, strictly related to privacy matters."

Internal audit is the third line of defence and provides independent assurance to the board of directors and management. This independent assurance can include audit of the first lines of defence activities, as well as audits of control processes established by the second line of defence. It can also include advisory assistance, for example during implementation of the initial GDPR compliance efforts.

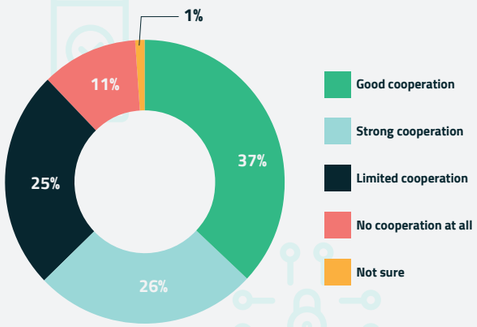
Interviewees stated that there are regularly scheduled meetings with the DPO to allow sharing of risk assessment results and of outcomes from detailed reviews or audits. Furthermore, interviewees often cited discussions among the functions as to how GDPR compliance can best be assessed and by whom.

> "We address the main risks of all the processes of the company. The risk manager engages with the first line and the DPO to make a risk assessment independently. We are also used to inform the internal audit department regarding the assessment. This allows them to build up a risk-based internal audit plan for the whole company."



▪ There is a good cooperation on GDPR between Internal Audit and Risk Management

Question: How strong is the cooperation between Internal Audit and Risk Management regarding GDPR?



Of the survey respondents, 63% indicated that there is a good or a strong cooperation between internal audit and risk management, in relation to GDPR. Only 11% stated the cooperation was failing, while that 88% of the total panel confirmed there is at least some cooperation, one year after the GDPR entered into force.

Such a result is not surprising, considering that both functions are involved in the oversight of risk, and this situation reflects the good governance practices embraced by the Three Lines of Defence model. Although each function focuses on its unique role in the organisation, they often cooperate on risk topics. The addition of data privacy risks to these topics is a logical next step.

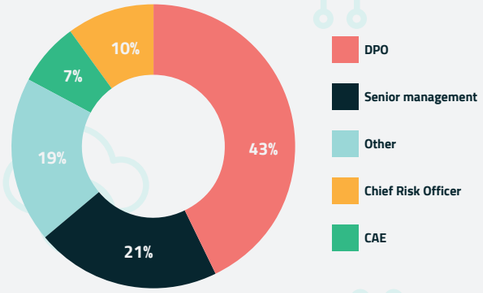
According to feedback from interviewees, cooperation between the functions most often takes the role of regular meetings, specifically to share risk assessment results. Some attempts are made at aligning risk assessment techniques and terminology.

Thanks to their expertise on risks and their broad coverage of the organisation, both risk management and internal audit functions are logical contact points for the DPO on privacy risks. They are also logical partners in supporting each function's unique role. As a result, many organisations have established formal exchanges to promote cooperation between the DPO, risk management and internal audit functions, often defining the roles based on the Three Lines of Defence model.

3. Reporting to the Board about data privacy matters, including the GDPR

▪ Different actors have a role in the reporting process to the Board, but the DPO remains the cornerstone

Question: Who is primarily expected to report to the Board (and/or Audit/Risk Committee) about GDPR compliance and performance in your organisation?



Survey and interview results both indicate that the DPO is primarily responsible for reporting to organisations' boards and senior management about data privacy matters. Furthermore, interviewees noted that there were at least annual updates on GDPR implementation, ongoing compliance, new data privacy risk assessments, training or other key obligations under the GDPR. This demonstrates alignment of practices with the regulation which requires the DPO to directly report to the highest management level of the data controller or the processor.

Of the responses from survey respondents, 17% indicated that risk management and internal audit are reporting on data privacy. The involvement of risk managers and internal auditors shows an integration of the GDPR and data privacy issues into their usual reporting process, just one year after the GDPR implementation. These findings were supported by interviewees who confirmed that for risk managers, reporting on risks for operational activities is among the core responsibilities of a risk manager in charge of ERM. For internal auditors, audit findings regarding GDPR compliance or implementation were integrated into standard audit reports and regular audit reporting to the audit committee, interviewees stated.

21% of survey respondents indicated senior management is primarily responsible for reporting to the board on data privacy. As this group generally reports to the board on all matters, the visibility of

data privacy could be higher or lower will depend on senior management focus and priorities.

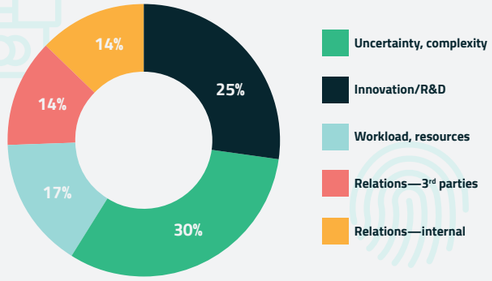
Regarding other functions shown in the chart, the legal and compliance functions are the most cited (nearly 60%) as reporting on data privacy matters. Interviewees confirmed that the compliance function gives regular (usually twice-annually or quarterly) reports to boards and senior management, and that the GDPR is integrated into those reports. This result is in line with Topic 1 above, which describes how the role of the DPO often sits within the legal or compliance function.

> "A big concern for the Board is that the organisation might be responsible for infrastructure it can not control."

For data privacy matters, reporting to boards is primarily done by the DPO. In addition, internal audit and risk management have integrated data privacy matters into their regular reporting processes.

4. Significant challenges posed by the GDPR

Question: What significant challenges has GDPR posed for your organisation?



Both survey respondents and interviewees were asked to cite challenges in implementing the GDPR. Although results can be grouped, these groups vary widely and include challenges incurred (now passed) during implementation, as well as current ones. Here are the top challenges mentioned by the respondents:

- Number 1 challenge: Uncertainty and complexity

Roughly 30% of survey respondents cited challenges regarding the uncertainty or the complexity of the GDPR. These comments include concerns about the scope of application of the GDPR for existing business and systems. For example, in highlighting the proliferation and nearly constant change of information technology, nearly all interviewees stated that keeping up with or ahead of technology was difficult. In addition, respondents and interviewees mentioned the extent of data in legacy systems (outdated computer systems or software that are difficult to maintain) and the technical difficulty in "forgetting[1]" personal information throughout all systems and businesses.

Despite the European Data Protection Board's existing work to harmonise approaches by national data protection authorities[2], the comments about uncertainty also include concerns about how those national authorities will interpret and enforce key aspects of the GDPR. International organisations especially face possible differences in treatment among countries. These may involve , both in applying technical aspects (e.g. how rules are applied for documentation, level of detail to be achieved, frequency and content of reporting) and financial aspects (e.g. fines, appreciation for good-faith efforts). Further, results from the surveys and interviews show that organisations are worried that this insufficient information from national data authorities could lead to unequal treatment of organisations, thereby creating unintentional competitive disadvantage.

> "It is important to have a good relationship with the regulator to clarify what is the level they deem as a high-impact event."

- Number 2 challenge: Innovation and R&D

Both interviewees and survey respondents (25%) expressed concern over how the GDPR might negatively affect innovation, especially with the use of technology, in their organisations. Most comments in this area reflected concern about how the GDPR could hinder the organisation's ability to fully adopt technology and data in new business models and products. Examples included the Internet of Things (IoT) and facial recognition were mentioned.

1 "Forgetting" personal information refers to requirements of the GDPR for the processor or controller to erase a data subject's personal data without undue delay.

2 See the European Commission's Communication from the Commission to the European Parliament and the Council :Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock, published 24 July 2019

> The fast development of technology and trade-off between the need for the company to be always digitalised and online, and the increase of data breaches risks restrains from new business developments.

While acknowledging Data Protection Impact Assessments (DPIAs) are a necessary part of the GDPR, several comments concerned the time required to do them, which resulted in delays to new projects and business. Respondents and interviewees also mentioned an irrational "fear" being adopted in some organisations, resulting in overreactions and shutdown or slowdown of business. The UK is an exception, the ICO has created a "sandbox" to share challenges and receive input from the Regulator.

On the positive side, some interviewees acknowledged that the GDPR did improve some aspects of their organisations. Organisations now have a better inventory of all their data and the roles and responsibilities concerning that data are clearer. This is in line with the opportunities for sound data management described in the *European Commission's Communication to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock*, published 24 July 2019.

▪ Number 3 challenge: Workload and allocated resources

Surprisingly, workload and resources were not cited as the biggest challenges. This could indicate that there had been a high level of budget anticipation; however, interviewees explained that efforts were made to incorporate GDPR compliance into existing processes and systems whenever possible. For example, in some organisations, data breach management was incorporated into existing incident response or incident management processes and systems. These bids to streamline processes do not negate the previously mentioned concerns about the complexity of legacy systems and the sometimes significant efforts necessary to adapt them.

Both survey respondents and interviewees explained that budgets were allocated for implementation, but obtaining budgets for ongoing compliance is more difficult. The need to build compliance is, therefore, greater.

▪ Number 4 challenge: Internal relations

Regarding internal relations, 14% of survey respondents indicated that internal training and maintaining awareness were challenges for the organisation. Several interviewees said this can be a challenge for compliance in general, not just the GDPR.

> Training is very important: I believe everyone in the company should know about the data protection regulation and how they can avoid any risk.

▪ Number 5 challenge: Relations with third parties

Relations with third parties were also cited as a challenge by 14% of survey respondents. Third parties are identified as a potential back door in terms of data protection breaches . Contracts with suppliers were repeatedly highlighted as having required significant time and effort to be updated. This included implementing new contracts where they did not previously exist or reviewing and revising all existing contracts. Though highlighting significant progress, several interviewees indicated this is an ongoing effort that sometimes delay day-to-day work when sharing of data is critical or time-sensitive (e.g. in the healthcare industry).

▪ Transversal and long-term challenge: Relation with third parties

In addition, to challenges cited in the survey, the outcome of interviews indicates that changes in culture and behaviour are also a challenge that is not easy to achieve.

In its *Communication to the European Parliament and the Council: Data protection rules as trust enabler in the EU and beyond-taking stock*, published 24 July 2019, the European Commission stated that "the success of GDPR should not be measured by the number of fines imposed, but by changes in the culture and behaviour of all actors involved."

> If you lose your data, reputation risk is more significant than financial loss.

All interviewees expressed significant progress on this front. However, they also indicated a tendency by both business managers and the board or senior management to revert to the DPO when compliance was not achieved as expected. This indicates a need to strengthen awareness of the DPO's role in the governance model.

Organisations face a range of challenges at varying levels of significance, depending on their approach to implementing GDPR compliance, their previous level of focus on data privacy risks and the amount of personal data they process or control.

Although organisations can address some of these challenges, others are driven by parties external to an organisation and a common approach to dealing with them has not yet emerged.

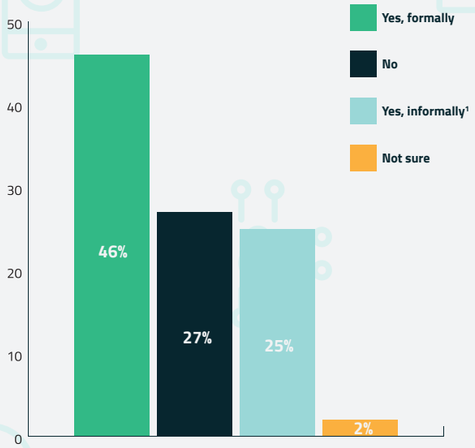
05

GDPR and Internal Audit:

Independent assurance over key risks relating to the GDPR

▪ The internal auditor is an independent assurance provider on GDPR matters

Question: Has your organisation's Board (and/or Executive Management) showed interest in receiving independent assurance from Internal Audit regarding the GDPR?



The broad majority (71%) of chief audit executives confirmed that their board of directors and senior management generally expect full compliance from the organisation as well as independent assurance from internal audit on all regulatory topics, including the GDPR.

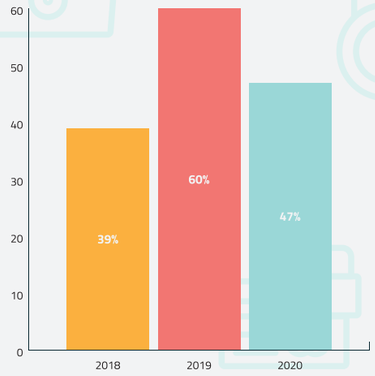
Although 27% of survey respondents said the board has not shown interest in independent assurance, this may reflect recurring survey comments and interviews that some organisations view the GDPR as "just another regulation" with which they must comply. This is especially true in countries where data protection was already highly regulated and this is also true in industries that do not regularly handle consumer data.

> "We trained all auditors, plus extra training for IT auditors, on what to consider for GDPR. Every audit has a checklist to see if GDPR work is needed."

▪ GDPR is fully integrated in annual audit plans

Question: Is GDPR part of your past, actual or upcoming audit plan?

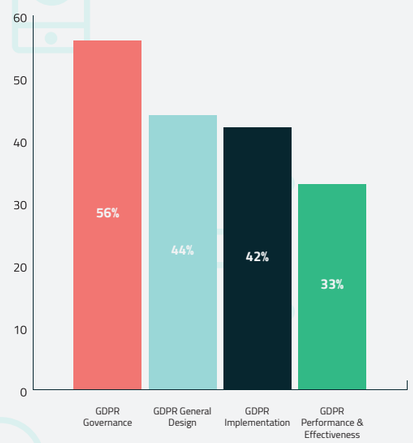
When asked whether the audit plan includes GDPR coverage, both survey respondents and interviews indicated that there had been extensive audit work in either 2018, 2019 or both.



1 Informally means that the assurance GDPR is part of an audit on another topic

Additionally, the GDPR is generally expected to remain in the audit plan in 2020, though the audit hours are likely to be reduced when compared to 2019.

Question: What elements of GDPR do you plan to (or actually) audit?

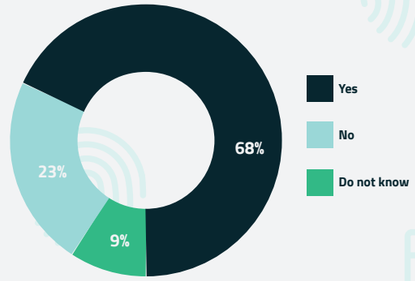


In 2019, the GDPR governance framework remains the key aspect to be audited. Interviewees reported that initial audit coverage focused especially on implementation and set-up of the data privacy governance framework.

One year after entry in force, second bests are still General Design and Implementation.

For the future, the GDPR is expected to be integrated into internal audit's usual risk assessment and planning efforts. Coverage of all aspects, but especially performance and effectiveness (aspects that now represent only a third of the current audit plans), will be determined according to the relative risk and priority that the GDPR takes throughout the organisation.

Question: Do you foresee that the GDPR related engagements will become recurring audits in your audit plan?



While particular audits of the DPO and compliance function (second lines of defence) might be scheduled (68% of the respondents foresee a recurrent auditing process), data privacy is expected to be a topic among others in nearly all business and process audits. Audit coverage will be determined during individual audit planning based on the data privacy risks for each audit unit.

> We put all of the risks in the same scale. GDPR is no different.

Several interviewees explained that they have implemented standard methods for determining coverage of data privacy risks on each audit of a first line of defence business unit. Examples include such as contracts with third parties, existence of personal data in processing, and methods of handling personal data. Answers to these questions determined whether data privacy will be in the scope of the audit. One interviewee highlighted a set of standard work programmes that could be added on to an audit of a business unit when coverage of data privacy risks was necessary.

Many internal audit departments have already integrated the GDPR into their work and are responding to board or senior management requests for assurance using existing risk-based audit planning techniques.

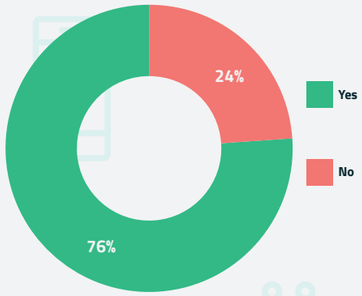
Finally, several interviewees mentioned their advisory work on the GDPR. This ranged from defined roles as observers of the GDPR implementation projects to flexible cooperation with DPOs through information sharing. This cooperation is further described in Topic 2 above, which describes the interaction between the DPO and Internal Audit.

06

GDPR and Risk Management: Integration of the assessment of data privacy risks

▪ GDPR is fully integrated in the global risk mapping process

Is data protection integrated in your global risk mapping?



The majority of risk manager respondents (76%) have already included data privacy in their global risk maps. This reflects risk managers' inclusion of evolving and significant risks in their ERM process. In fact, FERMA's European Risk Manager Report 2018 shows that data fraud/theft (which includes, but is not limited to, personal data) is in the Top 10 risks faced by organisations.

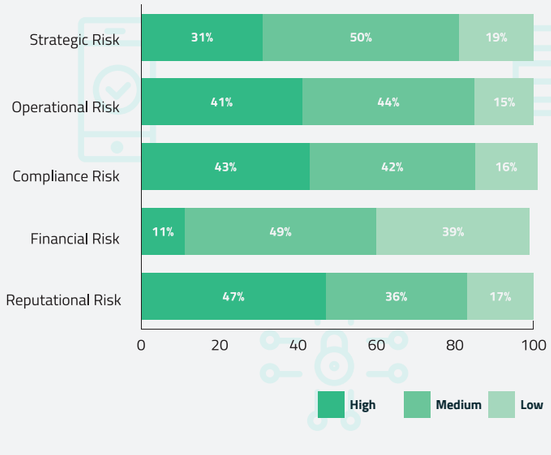
> We are working with a stress test to know the impact for us in terms of reputation and before any financial trigger. This is based on a notoriety score made by an independent company.

Interviewees explained that, although the DPO might be considered a process owner in the ERM risk matrix, data privacy is usually assessed as part of general compliance risk. In addition, related technical risks are assessed as part of IT/cyber and employee risks as part of human resources. Two interviewees described how the risk management function assessed the implementation project for GDPR compliance separately from ongoing compliance maintenance. This allowed risk management to analyse the return on the implementation project as is done for other strategic investments and big projects.

> By reviewing each contract, regarding the process of the data, we are also reviewing our business in a way.

▪ The varied nature of the GDPR implied risks

How do you rate various risks of the GDPR in your organisation?



Of the survey respondents, 47% have assessed the inherent GDPR reputational risk as high, followed by .

This is followed by the compliance risk and operational risk. These findings correspond with feedback from interviewees. They viewed the biggest risks related to data breach (or data loss), again in line with FERMA's European Risk Manager Report 2018, and the corresponding reputation risk that could occur when or if that data breach becomes public knowledge. Again, this is in line with FERMA's European Risk Manager Report 2018.

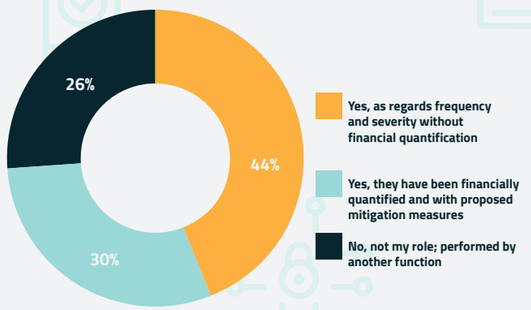
Data breach and reputation risk appear to be less relevant for organisations that do not regularly deal directly with end consumers.

Although recently imposed large fines of high amounts have garnered significant media attention, only 11% of survey respondents believe that the related financial risk is high.

> As we see it as a compliant and reputational risk, we don't really see it as an economic risk. But long term we are looking at it from the reputational side.

- The risk manager is broadly implicated in the threat analysis related to GDPR implementation

Question: Did you perform an evaluation of the threats arising from the GDPR implementation?



The majority of risk managers have incorporated data privacy risks into their existing risk assessments and risk maps.

74% of risk manager respondents assess the threats associated with GDPR implementation, although the process for doing so varies. Already 30% of risk managers are quantifying the financial impact of data protection incidents, using stress test scenarios, an index or a scale. Of the remaining respondents, 44% are performing qualitative assessments of frequency and severity as part of their standard risk management practices. Interviewees explained that, for exposures such as business continuity or reputation damage, these qualitative assessments are estimated or subjective, but based on written guidance.

When risk managers do not evaluate threats from the GDPR (26% of survey respondents), the other parties assessing those threats are most often legal and compliance (29%), the DPO (16%) or business operations (12%).

07

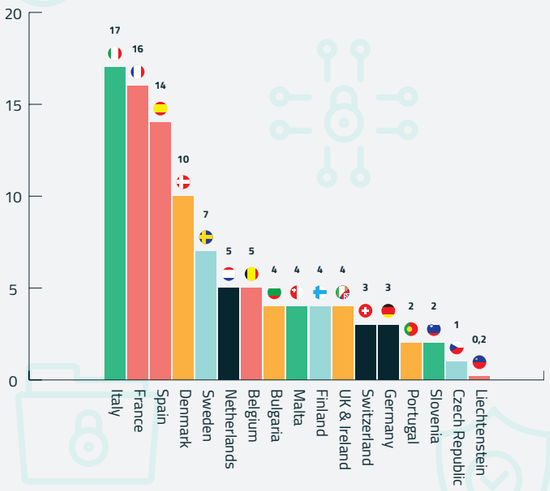
Appendix

Methodology

The findings in this paper are based on analysis from two anonymous web-based surveys and interviews of selected GDPR stakeholders.

One survey consisted of 19 questions distributed through the ECIIA's national institutes to heads of internal audit in five countries: Germany, Italy, France, Spain and the UK. This survey was completed by 124 respondents. A second survey consisted of 10 questions distributed through FERMA's 22 member associations to risk managers throughout Europe. This survey was completed by 205 respondents. All survey responses were received between 31 May and 14 July 2019.

Percentage of participation per country



Each of the two surveys contained five common questions relating to the GDPR impact on corporate governance and one open common question relating to challenges faced in implementation or going forward. The remaining questions in each survey were tailored to the roles of the respondents (Internal Audit or Risk Management).

Respondents were not required to answer all questions, so the response rates can vary among questions. In addition, some questions allowed multiple choices so the responses do not always add to 100%.

In addition, 23 interviews were conducted to provide insight to and elaborate on survey responses. Interviewees included heads of internal audit, risk managers and data protection officers. Interviewees were selected by ECIIA or FERMA national associations. The selection did not statistically represent the survey respondents; however, interviewees did represent varying countries (Italy, Germany, Spain, France and the UK) and diverse industries (telecom, transport, defence, health care, energy, ...).

About Our Organisations

The European Confederation of Institutes of Internal Auditing (ECIIA) is the voice of internal audit in Europe. Our role is to enhance corporate governance through the promotion of the professional practice of internal auditing. Our members comprise 34 national institutes of internal auditing from countries that fall within the wider European region, representing 48.000 individual members.

The ECIIA mission is to further the development of good corporate governance and internal audit at the European level, through knowledge sharing, developing key relationships, and impacting the regulatory environment, by dealing with the European Union, its Parliament and the European Authorities.

The Federation of European Risk Management Associations (FERMA) speaks for the risk management profession in Europe. FERMA brings together 21 risk management associations in 20 European countries. They represent nearly 5,000 professional risk managers active in a wide range of business sectors. FERMA acts on their behalf at European level and promotes the risk management profession.

FERMA provides a risk management perspective on European issues and strengthens the profession through a European risk management certification (RIMAP). As a member of the International Federation of Risk and Insurance Management Associations, FERMA supports the global risk management community and promotes communication on risk with events and publications.

Acknowledgements

The ECIIA and FERMA would like to thank all the people involved in this project for their insight and participation in developing this paper.

ECIIA
Avenue des Arts 41
1040 Brussels
Bruxelles, Belgium
www.eciia.eu

Contacts
Email: info@eciia.eu
Twitter: @EciiaInfo

FERMA
Avenue de Tervuren 273
Tervurenlaan B12
1150 Brussels
Bruxelles, Belgium
www.ferma.eu

Contacts
Email: enquiries@ferma.eu
Twitter: @FERMARISK

Design: pedromiguelxarepe.com