General Data Protection Regulation (GDPR):
Securing Data, Leading with both Legal and Technical Expertise

Executive Summary

As an independent nonprofit association serving more than 20,000 information and cyber security, audit, risk and technology governance professionals throughout the European Union (EU), and more than 140,000 members around the world, ISACA commends EU member states’ efforts to create the General Data Protection Regulation and welcomes and fully supports the protection it will provide the personal data of its citizens. ISACA believes that the GDPR will also serve as a model for international organisations, supporting the privacy of the individual as a fundamental right.¹ ISACA is supportive of GDPR’s privacy by design, appropriate security measures and the important role of the Data Protection Officer (DPO). At ISACA, we see this regulation as an opportunity to strengthen privacy protections for citizens of the EU and to ensure that those protections travel with the individual, regardless of where they go in the world.

Technologies are advancing at record paces; security can often find itself struggling to keep up with the challenges that advancement brings with it. The list of companies impacted grows day by day. They have suffered serious and expensive data breaches within the past few months. One study estimates that, on average, data breaches cost more than of $3 M Euro, and often include major and immeasurable effects to reputation.²

To effectively address these impacts, organisations need to consider the combination of organisation, people, processes and technology to achieve GDPR compliance. This means embracing a cross-functional team to implement and to bring all the necessary knowledge from key members across an organisation to the table – the c-suite, the CIO, CISO, DPO, legal and compliance professionals, security team members and any other relevant professionals within an organisation’s leadership ranks. They need to be on the team to prepare and to maintain the effort.

As GDPR replaces each EU Members State’s existing Data Protection legislation, it is important that organisations remember that GDPR will be a part of doing business, long after its enactment date in May 2018. Because of the potential heavy fines associated with cases of non-compliance, which can seriously affect both business profitability and reputation, it is more important than ever to work together.

² 2017 Ponemon Cost of Data Breach Study
If organisations approach GDPR compliance in the right way, there are real business benefits. Why wouldn’t an organisation want to ensure information is:

- Obtained fairly and lawfully
- Recorded accurately and reliably
- Verified as the one version of the truth
- Is held securely and confidentially
- Used effectively and ethically and
- Shared appropriately and legally?

Achievement of these objectives will provide business value and as a by-product, go a long way to achieving GDPR compliance.

A key element of GDPR compliance, is the need to fully identify an organisation’s information assets and information risks. As information and technology experts, ISACA is particularly focused on the importance of effectively implementing the GDPR’s privacy by design concept. This concept requires organisations to build privacy directly into technology, systems and practices at the design phase, thereby ensuring the existence of privacy from the outset. ISACA is also focused on the vital connection to cyber security and the need to keep information safe. Appropriate security measures will have to be taken and all staff trained. Additionally, DPOs will be vital to the success of the entire regulation. ISACA staunchly supports the work of DPOs and, supports certifications or similar credentialing efforts as part of the DPO training process. ISACA would welcome the opportunity to share our decades of experience in this area.

Introduction

GDPR updates the Data Protection Act 1998 (DPA), which focused on the population and considered the individual. GDPR focuses on the rights of the individual and considers the population. GDPR focuses on privacy as a human right.

The following information is taken from various sections within the GDPR. GDPR builds on the eight principles defined in the DPA and introduces some new concepts. As used within the provisions of the GDPR, the terms controller and processor are also critical and must be carefully understood. The responsibilities of Data Controllers have been well understood for many years, as part of the DPA, and are those professionals who, either alone or jointly or in common with other persons, determine the

---

References in IAPP Certification Textbooks f14-15, 128, US21, M88-90, 121-122
purposes for which and the way any personal data are to be processed. GDPR defines Data Processes as an entity that process personal data on behalf of a controller where a written contract is in place, which imposes a number of mandatory terms on the Data Processor, as set out in the GDPR.

Organisations need to understand these definitions, where their data is located, particularly if a Cloud service is being used, such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) and that there is much at stake with GDPR including:

- Global in scope – any company doing business in the EU is impacted
- Company reputation impacted if not managed correctly
- Data breaches must be reported within 72 hours of becoming aware

According to a new ISACA survey of senior executives and boards of directors, fewer than one-third are satisfied with their organisation's progress to prepare for GDPR. A concerning 35% are not aware of their organisation’s progress.\(^4\) There are a scant few months remaining until the May enactment of GDPR; having two of every three organisations dissatisfied with their progress on preparations for GDPR is unacceptable. It is critical, throughout the public, private and NGO sectors, that GDPR progress increases in both pace and scope, and ISACA stands ready to assist in those efforts.

**Privacy by Design, Risk Management and Appropriate Security**

Even the best DPO, though, will struggle without the complete engagement from the organisation and strong data protection as well as cyber security defences built into the organisation at a foundational level. Privacy by design facilitates a critical element of GDPR, and calls for "**the controller to ensure only the necessary data is being handled at all.**"\(^5\)

The GDPR requires that organisations implement data protection and cyber security protections, by design, into their offerings, and that such security measures also consider the ongoing advancement of technology. These are elements that cannot be “added on” midway through production; they must be included in the core elements of that offering, be it a product or service. This emphasis on data protection and cyber security by design, that acknowledges the likelihood of technological progress, is a concept that ISACA supports strongly, for the positive benefits of its inclusion will be felt throughout all levels of the enterprise, as well as by consumers. Likewise, ISACA very strongly supports the inclusion of appropriate technology governance measures and procedures that aid the inclusion of

---


data protection and cyber security by design.

Implementing an effective enterprise risk assessment program, in which information is treated as an organisational asset and where responsibility and accountability are exercised at correct levels, requires a risk management structure implemented at the enterprise level. It also requires that all facets of an organisation are assessed against the maturity of their risk management programs. It also must include an ongoing endeavour of follow-up. It is critical to work with the organisation’s identified team, leveraging everyone’s expertise to build the most sound and secure systems possible.

This risk assessment also requires understanding your cyber security status. Organisations must understand where it currently stands before it can move forward with designing the future. Without a complete picture, the future will not work out as planned.

ISACA’s COBIT® 5 for Risk® can be a resource in these efforts, as can similar frameworks that have already been widely adopted throughout the EU. Implementation guidance and a means to measure capabilities is needed. ISACA would welcome the opportunity to assist in bringing together a group of industry leaders that are already experts in the Enterprise Risk Management (ERM) approach to create the implementation guidance that could be adopted throughout the EU.

Fundamentally, data protection and cyber security are enterprise-wide challenges and Enterprise Risk Management priorities. Information—especially personal information—must be treated as a valued asset. Governance roles, responsibilities and accountabilities should be clearly understood and defined in a manner that permeates all levels of the enterprise. Appropriate policies, procedures and processes must be in place across the enterprise to ensure a successful cyber security program.

Data Protection Officers and Value to the Organisation and State

The ideal DPO will have both legal and technical knowledge. He or she must have a sound understanding of information security as well and data privacy. A DPOs with appropriate professional expertise, organisations will be in a better position to effectively work with stakeholders to implement security controls that meet data privacy requirements. A fundamental understanding of Information Technology (IT), along with an understanding of IT Governance is crucial for a DPO. In addition, knowledge of the workings of networks, servers, and other IT infrastructure will make it easier for DPOs to speak to IT when they are trying to ensure that data protection requirements have been implemented.7

It is not enough, however, to merely appoint a DPO and have them directly report to the leadership of

7 Scott Rosenmeirer – ISACA GDPR Working Group Member
an enterprise. Rather, the enterprise, for its part, must make sure that support is available to ensure that their DPO is able to pursue and maintain ongoing excellence in their role. Article 38(2) of the GDPR states: “The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to…maintain his or her expert knowledge.”

The role of DPO, as noted in this provision, is evolving. Committing to a DPO career will likely mean an equivalent commitment to continual professional education. ISACA believes careers in data protection and cyber security should involve a continual reinvigoration of knowledge, skills and abilities, and is best achieved through ongoing professional education efforts. Also, it is important to note not every organisation must appoint a DPO. Public institutions which process data, companies that systematically process personal data on a large scale and organisations that process data relating to specific data categories (such as health data) require a DPO.

In terms of filling the void, organisations can consider looking within to find the solution in some cases. Can they develop current data protection professionals, perhaps from the ranks of the organisation’s current risk and information governance professionals? In a large corporation, data privacy professionals might be considered for the role of Chief Data Officer; for small and media enterprises, managed services might be a more feasible option.

Regarding certifications, some have suggested some sort of professional certification for DPOs; a third-party accreditation that measures knowledge of and adherence to applicable data protection regulatory and statutory requirements. As the role of the DPO becomes more formalised throughout the EU and the world, this is a concept worthy of investigation, and ISACA stands ready to discuss growing our existing certifications to include a DPO component.

Discussion Points

The GDPR is an excellent step forward in the ongoing evolution of data protection, cybersecurity and information governance. The following are a few areas in which ISACA believes that focus should be given in order to ensure effective implementation.

- **The GDPR’s expansion of the DPO role within the business world is commendable.** However, there are many unfilled DPO roles within the business world. Expanding the DPO role to a broader group of practitioners with varied backgrounds to fill the void could prove beneficial, and would certainly be a step forward in ensuring fewer challenges in the enforcement and support of GDPR in the years ahead.

---

8 [https://gdpr-info.eu/art-38-gdpr/](https://gdpr-info.eu/art-38-gdpr/)
9 Mike Hughes – ISACA GDPR Working Group Member
10 Lachaud, E.; “Should the DPO Be Certified?,” International Data Privacy Law 2014; 4 (3): 189-202
• **Increase focus on cyber-readiness requirements.** With the increased threat of breaches, it is critical that organisations are ready to ward off attacks and know exactly where their vulnerabilities are. Therefore, they will need a continuous process to identify potential threats and vulnerabilities and ensure their risk is understood and effectively managed to reduce the chance of a successful attack. Organisations then need to proactively prepare for the aftermath of a successful attack; this includes: pre-planning, professional development and training efforts can no longer be treated as ‘optional’ business costs; strong security efforts will require an emphasis on such educational efforts as a core element of any successful, well-protected organisation.

• **Data protection and cyber security are enterprise-wide challenges and priorities, and deserve to be treated as such; this is a goal ISACA believes firmly supports the spirit and goals of the GDPR.** Applying proven frameworks, at the enterprise level, to risk management and assessment efforts can only serve to benefit both the enterprise and the communities served. This is something that ISACA believes is strongly in keeping with the goals of the GDPR. ISACA suggests the further exploration of the possibility of utilising an ERM approach for data protection and cyber security capabilities within organisations, and stands ready to assist in those endeavours.

• **ISACA would welcome the opportunity to discuss credentials for the DPO role,** which would be recognised by the EU as a valued credential for DPOs.

• **The SME Challenge** many small to medium size organisations are not fully engaged with the need to comply with GDPR. They believe that GDPR is only relevant to large corporate and government bodies. They fail to understand that all organisations have personal information to enable them to run their business, but also, quite often they are an important part of a large corporates, supply chain. ISACA has been working on providing guidance for SME’s for implementing appropriate and proportionate governance and cyber security management controls.

The design of the GDPR has been a thorough and comprehensive process, and that is commendable. The challenge now is its effective implementation, which is both compliant with the regulation and also pragmatic, appropriate and proportionate for the organisation. ISACA looks forward to the continued implementation efforts for the GDPR, and stands ready to assist in any way through our EU community of information and cyber security, audit, risk and technology governance professionals.
About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today’s world is powered by technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organisations. ISACA leverages the expertise of its more than 140,000 members in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 215 chapters and offices in both the United States and China.

ISACA Headquarters: 3701 Algonquin Road, Suite 1010, Rolling Meadows, Illinois, 60008 USA
Web:  www.isaca.org

Contact:
Tara Wisniewski - twisniewski@isaca.org
Jen Gremmels - jgremmels@isaca.org