MAINTAINING DATA PROTECTION AND PRIVACY BEYOND GDPR IMPLEMENTATION

ISACA®

ABSTRACT

The EU's General Data Protection Regulation (GDPR) becomes applicable and enforceable on 25 May 2018. Any enterprise that processes data on individuals in the EU must institute specific privacy protections for that information or face regulatory penalties for violations. As a result, organizations around the world have been making preparations in order to demonstrate compliance by the deadline. However, business leaders should not view GDPR requirements as a project or one-time event. Properly scoped, GDPR is only part of an enterprise's overall strategy for data protection and privacy, and this strategy is ongoing and ever-evolving as circumstances arise. This white paper examines the issues surrounding GDPR's impact on this strategy, the competencies and responsibilities needed in an organization to support the strategy, the relevant standards to consider, and the key elements to establish in the operational life cycle.

CONTENTS

Maintaining Data Protection and Privacy Beyond GDPR Implementation

Introduction

No matter the size of the organization, if it is processing personal data of natural, living persons in the European Union (EU)/European Economic Area (EEA), the organization needs to be aware of its obligations to the General Data Protection Regulation (GDPR).

Although the GDPR represents a massive challenge for many organizations, it does build upon existing data protection legislation that goes back decades and, in most cases, legislation of which organizations should already be aware. However, from a data protection perspective, specific GDPR requirements must be evaluated together with requirements from other applicable legislation relevant to the operations of the organization.

The focus must therefore be on "data protection/data privacy" rather than "GDPR," and on "program" rather than "project," taking into account the fluidity of legislation.

In addition, while compliance with GDPR may be required, it is not the only potential benefits of this data protection exercise. This situation is an opportunity for organizations to better understand their suppliers and customer base, as well as address any strategic business advantages to be gained from a new focus on privacy.

To aid in the enterprise's efforts, this white paper has broken down the discussion into these sections:

- Developing a Comprehensive Data Protection Strategy
- Implementing and Optimizing the Data Protection Program Under GDPR
- Integrating Relevant Standards into the Data Protection Program
- Establishing an Operational Life Cycle and Continuous Improvement

Developing a Comprehensive Data Protection Strategy

Unfortunately, new legislation is often perceived as a hindrance to organizations, especially in commercial sectors. Framing the GDPR in a positive light and identifying the opportunities that it offers can enable organizations to differentiate themselves in their markets, improve their image and build trust with an array of internal and external stakeholders.

Organizations therefore need to formulate their approach to addressing the GDPR by either updating their existing data protection strategy or crafting one from scratch.

An organization's formal privacy program should be based on the execution of a data protection strategy aligned with the goals and objectives of the organization. The program is an ongoing endeavor, so, in the context of GDPR, 25 May 2018 should be viewed as a milestone rather than a finish date within your larger privacy program. However, authorities do expect specific GDPR compliance for your enterprise to be achieved by that date.

The data protection strategy for an organization should take in a number of factors including (and in no particular order):

- Size and nature of the business
- Business model (business to business [B2B], business to consumer [B2C], consumer to consumer [C2C])
- Market sector
- Categories of data subjects
- The data being processed
- Competitors
- Risk exposure and appetite
- The level of dependency on the processing of personal data
- Jurisdictions
- Other compliance requirements
- Business and data custody strategies
- Reliance on third parties, including contractors, outsourced activities, and the supply chain
- Size of workforce
- Available resources

An effective data protection strategy needs to be crafted with the involvement of a wide group of stakeholders. For example, the legal department may insist on following the letter of the law, which could be at odds with objectives of the chief financial officer (CFO), who may want to fund only "a minimum level of compliance." Colleagues within the business may see opportunities to enhance brand image or differentiate products or services from the competition. A strong emphasis by the chief information officer (CIO)/chief technology officer (CTO) on technology may fail to acknowledge the critical element of addressing the people/cultural change needed—not a wise strategy when so many data breaches are triggered by humans (employees poorly trained or with the wrong mindset could be the organization's biggest risk).

Developing a data protection strategy does not need to be a difficult task. A good starting point is to assemble the key stakeholders in the organization in one or more facilitated workshops and agree on the key strategic elements. Among the issues to consider are the current state of data protection in the organization (the as-is analysis), any key areas that require attention, priorities and targets for May 2018 and beyond, key performance indicators for change or progress, relevant existing projects underway, and any new initiatives needed.

Many inputs to the strategy, especially elements from the as-is analysis, are typically delivered as part of a pre-analysis phase of a data privacy/GDPR project or program. Once the strategic elements are agreed upon and documented, costs are projected and a realistic benefits case is created to secure funding so program mobilization can begin.

Ultimately, the proper strategy depends upon a number of factors. Agreeing on the right approach for the enterprise may result in a data protection strategy that is compliance-based, ethics-based, risk-based or a combination of the three—whatever best meets the needs and expectations of internal and external stakeholders. If the right stakeholders are not involved, or the program is anchored in the wrong place in the organization, the strategy may be needlessly too focused on compliance or may miss business opportunities.

Risk-Based Strategy

Using a risk-based strategy approach could indicate that the enterprise accepts that, on 25 May 2018, there will be gaps, so it is important for the organization to take steps to demonstrate serious GDPR compliance efforts. If the strategy is documented, it should show progress on a plan by closing gaps and addressing risk, with establishment of sufficient policies, procedures, embedded roles and responsibilities to govern data protection beyond May 2018. Doing so would indicate that the risk-based strategy could be perceived as sound.

Even though the GDPR contains many hard requirements, there are other sections that are less defined. The text of the GDPR contains words and phrases such as "appropriate," "cost of implementation," "context," and "adequate," which may be open to interpretation. This ambiguity allows the use of certain risk-based strategies, provided the enterprise can demonstrate good-faith efforts toward compliance.

Ethics-Based Strategy

An ethics-based strategy could be perceived as emphasizing an individual's "right to privacy." In their book *Data Ethics—The New Competitive Advantage*,[1] authors Gry Hasselbalch and Pernille Tranberg detail a number of cases where organizations have taken a strong ethics-based stance.

A good example is the Danish company, LEGO, where the enterprise has placed the protection of children's data at the heart of its online universes. Activities include limits on integrating with social media, strong corporate responsibility regarding use of customer data by suppliers and partners, and no third-party cookies on websites aimed at children under age 13. An ethics-based strategy may require the organization to do more than is required by the GDPR—and, therefore, potentially could cost more—but the benefits to the enterprise may be considered worthwhile.

Compliance-Based Strategy

In simple terms, the compliance-based strategy is ensuring all i's are dotted and t's crossed—it is a legally-driven approach that typically aligns with an existing compliance regime meeting the requirements of other legislation. It is often used by organizations that operate in regulated sectors, such as pharma or financial services.

Also, many organizations providing third-party services, especially when acting as a Processor (in GDPR terms), may need to demonstrate full compliance to their clients, partners, and regulators, etc. These third-party organizations normally have a strong privacy baseline focused on either meeting requirements across multiple jurisdictions and industry sectors, or satisfying the compliance mandates of a niche sector and providing services to clients specifically in that sector.

Triggers to Revisit the Data Protection Strategy

The data protection strategy is one of the key factors in shaping the scope of the enterprise's data privacy program, but there are others. For most organizations, change is inevitable and may require the data protection strategy to be revisited and adjusted periodically. Typical triggers include the following situations.

1 Hasselbalch, G., P. Tranberg; *Data Ethics—The New Competitive Advantage*, PubliShare, 24 October 2016, *http://dataethics.eu/en/book*

MERGERS, ACQUISITIONS AND DIVESTITURES

Restructuring of organizations is a common activity. In fact, according to a recent Deloitte report,[2] the outlook for 2018 is that restructuring activities will continue to accelerate, especially in the technology sector.

When organizations are acquired or merged, a wide range of new compliance requirements often arise, including industry-sector-specific laws and/or jurisdictional regulations and laws. In addition, existing vendor and client agreements become applicable in the new organization.

Mergers and acquisitions typically follow well-defined processes and often a control triggers an evaluation of potential data privacy impacts. In addition, a special focus should be placed on potential inheritance of privacy "debt" during the process. The recent acquisition of Yahoo by Verizon is a good example of how a data breach influences the value of an organization and why it is critical to identify potential "debts" as early as possible in the mergers and acquisitions process.

In the case of divestitures, data processing systems need to be decoupled, and it is critical that no personal data be retained within the organization. A equivalent step is needed in the divestiture process to flag any potential issues.

CHANGE IN BUSINESS STRATEGY

The need for a business to remain competitive or relevant often results in changes to its strategy; responses to competitor behavior, the desire for growth, the need for improvement and efficiency, and the promise of technological evolution are just a few reasons why businesses revisit their strategy. To maintain alignment with strategic business goals and objectives, any changes to the business strategy must trigger an evaluation of possible impacts to the data protection strategy.

CHANGE IN REGULATORY LANDSCAPE

A key part of a privacy program is a mechanism to monitor changes in applicable laws, standards and regulations across all operating environments and jurisdictions. The GDPR is a good example. Although adopted in 2016, the regulation has been under development since around 2012. It is very important to understand the common elements and dependencies among the various compliance requirements—for example, requirements across the data life cycle such as notice, purpose limitation, data minimization, data retention/disposal and individual rights.

CHANGE IN THREAT PICTURE

The threat picture for all organizations processing personal data is ever-changing, and highly significant changes have occurred in recent years. New threats are identified, new vulnerabilities are discovered, and new technologies emerge to address them. The impacts of these changes on an organization's data protection strategy need to be evaluated on a regular basis for the strategy to remain relevant and appropriate.

2 Deloitte, "The state of the deal: M&A trends 2018," *https://www2.deloitte.com/us/en/pag-*

Implementing and Optimizing the Data Protection Program Under GDPR

Once the enterprise has established a data protection strategy that meets the needs of organizational stakeholders, objectives and goals, it is time to establish the proper governance framework to execute the formal data protection program.

The organization will need specific competencies, responsibilities and structures to support the program and maintain its compliance with applicable laws and regulations. Certain roles and reporting arrangements must be created. In addition, GDPR implementation brings its own set of new requirements. Among them is the creation of a new role in the privacy organization—the data protection officer (DPO).

Ultimately, personal data belongs to the individual, and GDPR requires enterprise establishment of a governance framework that serves that mission.

Establishing Program Governance and GDPR Compliance

When developing the specific competencies, responsibilities and structures needed in the organization, leadership will need to consider where to anchor data protection activities within the enterprise as well as the makeup of the teams that ensure compliance and protection.

A key requirement of the GDPR is for organizations to demonstrate "accountability." Part of this involves delegating responsibility to different parts of the organization and assigning data protection responsibilities to those primarily dealing with the processing of personal data. Responsibilities are normally articulated to individuals through policies and procedures and reinforced with education, training and, in some cases, coaching or mentoring.

It is essential that organizations identify the most appropriate place to anchor data protection activities. According to the "IAPP-EY Annual Privacy Governance Report of 2017,"[3] slightly less than half of organizations surveyed place data privacy in their legal departments. This figure has changed very little over the past three years; regulatory compliance departments and information security teams place second and third, respectively. The report also shows that there is a slight upward trend in anchoring data privacy in the corporate ethics function. This may reflect how privacy is being aligned with corporate strategy in those organizations that have identified corporate social responsibility (CSR) as a differentiator in their market.

Where your organization anchors its activities will likely have a pronounced effect on the strategy (or mix of strategies) selected and implemented—risk-based, ethics-based, or compliance-based.

Core Data Protection Team

It is also important to recognize the specific competencies needed in staffing a data privacy program. The size of the program organization may vary according to:

- The size of the organization (headcount and operations)
- The nature of the business
- The volume of personal data processed
- Whether sensitive categories of personal data are processed
- The organization's risk exposure and risk appetite

For large organizations, a core data protection team or data protection office may be created, consisting of roles such as data protection program manager and

3 International Association of Privacy Professionals and EY, "IAPP-EY Annual Privacy Governance Report of 2017," *https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf*

data protection analyst. For smaller organizations, responsibilities may be embedded in existing roles dispersed across various functional areas, including information security, legal, compliance, information risk and information governance.

The program manager's role is to establish and oversee the overall data protection program and manage the program staff, as well as embed data protection awareness and specific data protection responsibilities across the organization. Typically, the role includes the following responsibilities:

- Defining a data protection strategy aligned with the strategic objectives of the organization
- Developing and implementing an overall data protection program framework
- Managing the program team
- Establishing and maintaining an overview of all data protection laws and regulations applicable to the organization
- Establishing and maintaining data inventories and maps covering the personal data processing life cycle
- Defining and implementing data assessment models appropriate to the organization
- Defining and implementing a framework for managing data protection and privacy risk
- Defining and implementing appropriate data protection policies and procedures to ensure compliance with applicable data protection laws and regulations, as well as internal organizational policies
- Ensuring third-party risk is adequately managed
- Establishing and maintaining a data protection awareness and training program
- Ensuring appropriate policies and controls (i.e., architectural or technical processes) are in place to protect personal data and the privacy rights of data subjects
- Monitoring compliance and tracking and reporting the performance of the program

Data protection analysts support the program manager by fulfilling the following responsibilities across the organization:

- Monitoring applicable data protection legislation
- Conducting data assessments
- Conducting gap analysis
- Conducting data protection risk analysis
- Maintaining data protection policies and procedures
- Monitoring program performance metrics
- Monitoring data-protection-related incidents
- Planning for and responding to data breaches

The privacy team will be typically supported by others across the enterprise who possess competences in:

- Data protection law
- Employment law
- Information security
- Information governance
- Records management
- Information risk management
- Process management
- Master data management
- Various IT competencies

Data Protection Officer

Even though the DPO is grouped with "governance activities" and "team structures" in this white paper, this GDPR-mandated role essentially provides independent oversight of data protection activities. While installing a formal DPO role is not mandatory for every enterprise, fulfilling the responsibilities that would be covered by the DPO role is mandatory for all enterprises seeking compliance.

The GDPR sets clear requirements to organizations about the appointment of a DPO. The flowchart in **figure 1**, produced by *DPO Network Europe*,[4] can be used to determine whether a DPO is required to be named in the enterprise.

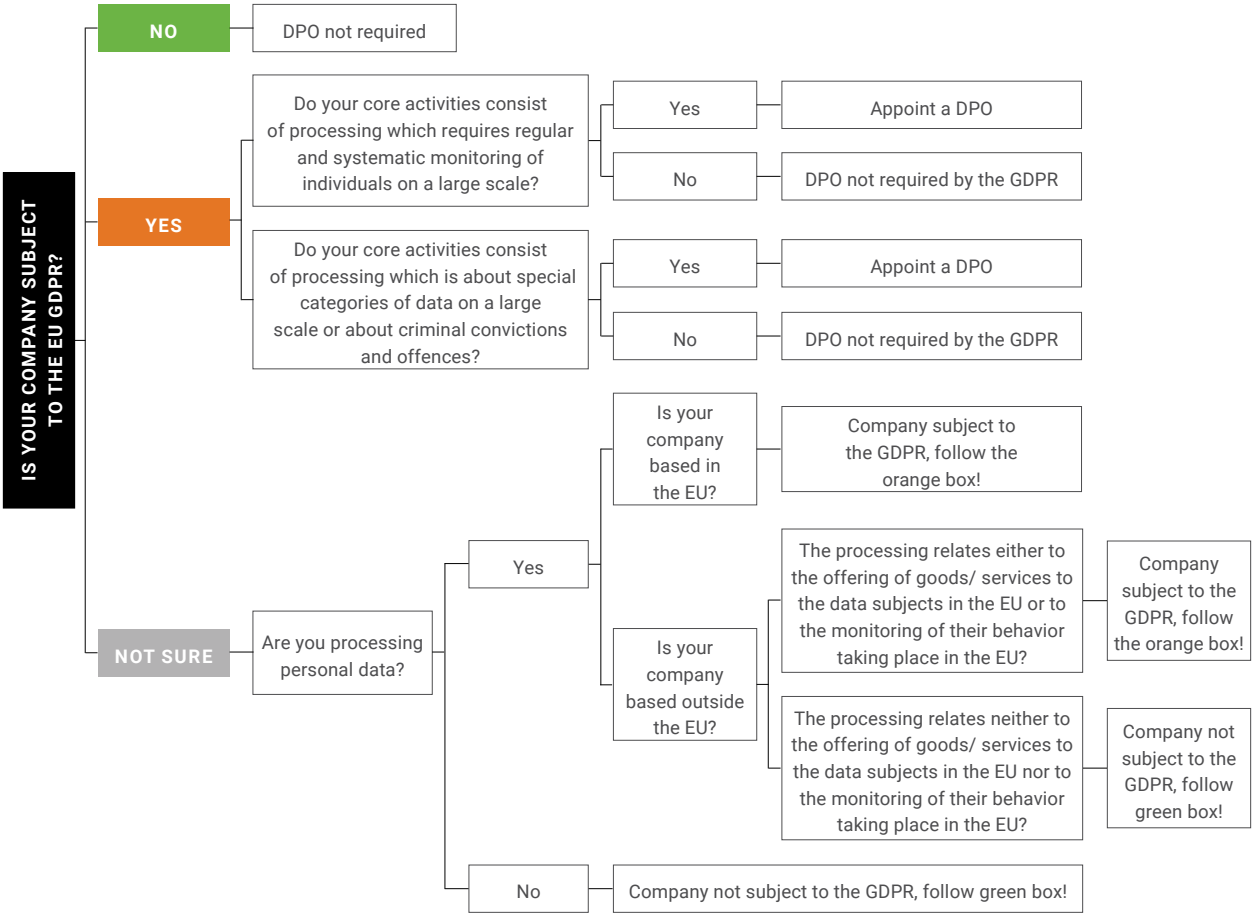


FIGURE 1: Requirement for a DPO

Source: DPO Network Europe.

4 DPO Network Europe, "Should your company appoint a data protection officer (DPO) under the GDPR?" *https://www.dponetwork.eu/uploads/3/1/7/3/31732293/gdpr_dpo_decisiontree.pdf*

KEY RESPONSIBILITIES AND SKILLS OF THE DPO ROLE

This position and its duties, as set forth in the GDPR requirements, will require a person with a unique skill set. Among the responsibilities for this role:

- Ensuring the organization and its employees are informed of key compliance requirements
- Ensuring employees working with the processing of personal data are trained according to their job role
- Conducting audits to ensure GDPR compliance
- Proactively addressing data protection issues
- Acting as the focal point between the organization and data protection supervisory authorities
- Monitoring performance and providing advice to the organization on all matters of data protection
- Ensuring records of processing activities are maintained by the organization
- Communicating with data subjects on how their data are being processed, their rights as a data subject, and the measures the organization has in place to protect their personal data during processing

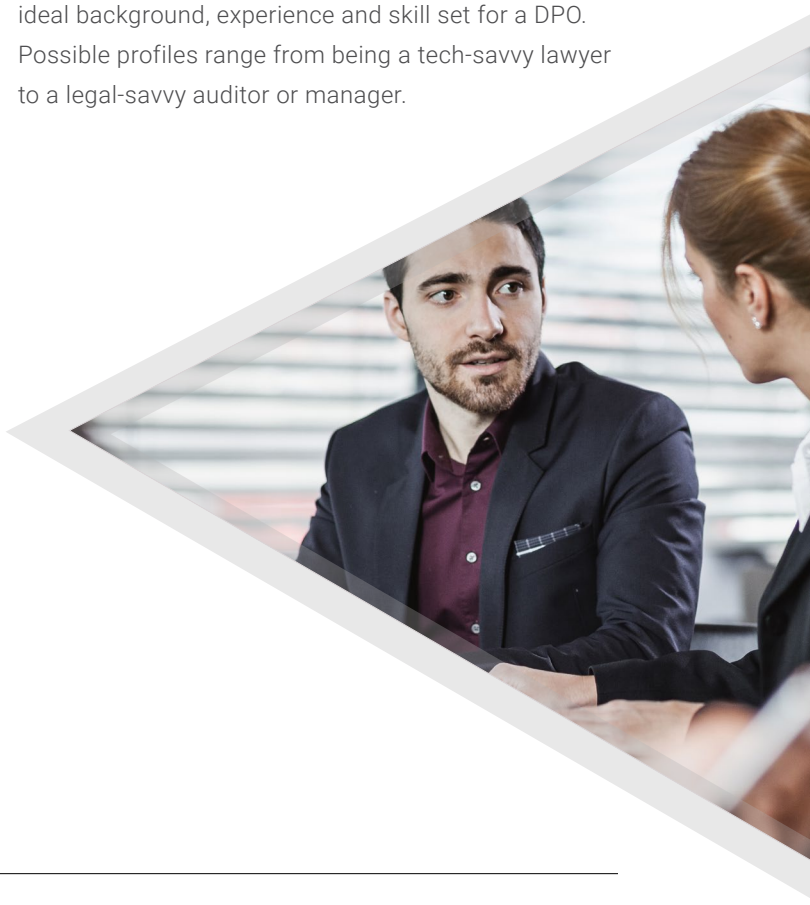
The GDPR also states the DPO should possess specific qualities, including:

- Integrity and high professional ethics
- Expertise in relevant national and European data protection laws, practices and relevant case law, including an in-depth understanding of the GDPR
- Understanding of the processing operations carried out by the organization
- Understanding of information technologies and data security
- Knowledge of the business sector and the organization
- Ability to promote a data protection culture within the organization

The GDPR is clear concerning some requirements associated with the role. However, if these requirements are not understood correctly, unnecessary constraints could be placed on an organization:

- The DPO shall act independently but may fulfill other tasks and duties as long as they do not result in a conflict of interest.
- The DPO shall be bound by secrecy or confidentiality concerning the performance of his/her tasks, in accordance with Union or Member State law.
- The DPO must be autonomous; he/she shall not be instructed by the organization on how to complete the role's tasks.
- A DPO is protected under the GDPR from unfair dismissal or termination for reasons relating to their performance of the DPO role.

There is much debate about what constitutes the ideal background, experience and skill set for a DPO. Possible profiles range from being a tech-savvy lawyer to a legal-savvy auditor or manager.



FULFILLING THE DPO ROLE

Organizations that require a DPO or voluntarily have decided to appoint one have the option of fulfilling the role internally, externally or through a combination of the two. A market has emerged for third-party businesses offering external independent DPO services.

For large or internationally dispersed organizations, the workload will undoubtedly be too demanding for one person, so organizations may look to establish a central DPO at the headquarters level and delegate responsibilities to cover specific functional areas or markets across the organization.

In addition, some enterprises may struggle to find an individual possessing all of the broad range of competencies required for a DPO, as outlined in the GDPR. In these cases, the competencies could be split across multiple individuals and, again, may be fulfilled by internal or external resources or a combination of the two.

Many organizations have already appointed (multiple) DPOs across their markets or operations. For larger enterprises, this will help ensure that a DPO is accessible. However, appointing multiple DPOs triggers ramifications that should be carefully considered. For those organizations that have established a "network" of multiple DPOs, the DPO requirements under GDPR apply to all named DPOs (which can lead to constraints on the enterprise, as previously noted). To avoid these constraints, organizations may prefer to appoint staff to perform "DPO-like" tasks but give a title that avoids any risk of confusion (e.g., data privacy director or data protection manager).

Organizations that voluntarily name a DPO will be required to comply with the GDPR requirements for the DPO role as if the appointment had been mandatory—again, leading to potential constraints that must be considered.

Currently, there are too many organizations with little or no focus on data protection. Now, these enterprises face the daunting task of complying with complex legislation, often struggling with where to begin. They possess scarce data protection resources, and if it is mandatory for them to appoint a DPO, they must overcome the additional challenge of how to establish the role.

Without a suitable candidate internally, organizations may need to take a pragmatic approach and hire external expertise to mentor an internal candidate who possesses good business and organizational knowledge supplemented by sound communication and project management skills and rooted in technical competencies from information security, audit and/or risk management.

Data Protection Board

A formal interface needs to be created to establish and maintain alignment between the data protection program and the rest of the organization. In many organizations, this is achieved by forming a committee consisting of key data protection stakeholders from across the organization.

Ideally, the stakeholders will be senior figures with a mandate to make strategic decisions within the data protection board as well as sufficient clout to ensure strategies and plans are implemented within their own functional areas.

In larger organizations, the overall data protection board may be supplemented by a network of supporting board structures. This may be beneficial for global organizations with regions or autonomous business areas.

The purpose of the data protection board is to help the enterprise view data protection as a value-adding

activity rather than an obstacle to business. The board should meet on a regular basis to review program status, monitor the progress of initiatives, review risk exposure, and help remove any blockages where the program cannot move forward due to business issues and vice versa.

Change Management

For many organizations, the GDPR presents an organizational change challenge: Existing culture and mindsets are impacted, new roles are established, and responsibilities are strengthened. Where the needed organizational change is perceived as high, it is recommended to add an organizational change manager to the program to increase the likelihood that the enterprise is ready to absorb and enact the planned changes. A change manager will typically work with a structured approach such as the Prosci® ADKAR® Model,[5] an acronym for:

- **Awareness** of the business reasons for change. Awareness is the goal/outcome of early communications related to an organizational change.
- **Desire** to engage and participate in the change. Desire is the goal/outcome of sponsorship and resistance management.
- **Knowledge** about how to change. Knowledge is the goal/outcome of training and coaching.
- **Ability** to realize or implement the change at the required performance level. Ability is the goal/outcome of additional coaching, practice and time.
- **Reinforcement** to ensure change endures. Reinforcement is the goal/outcome of adoption measurement, corrective action and recognition of successful change.

When an organization undertakes an initiative such as establishing a data protection program, change happens only when the affected employees can say with confidence, "I have the **awareness**, **desire**, **knowledge**, **ability** and **reinforcement** to make this change happen."

ADKAR is an effective tool for:

- Planning change management activities
- Diagnosing gaps
- Developing corrective actions
- Supporting managers and supervisors

Integrating Relevant Standards into the Data Protection Program

If the organization is already able to demonstrate compliance with existing data protection legislation, then it is highly likely that complying with GDPR will be a much easier task than it will be for organizations with less mature privacy functions. It is also highly likely that a foundational control framework supported or inspired by industry standards is already in place.

For other organizations, the challenge and effort will be considerably greater. However, there are several relevant industry standards that organizations should consider to avoid reinventing the wheel for its data protection program.

When implementing controls from multiple standards, organizations need to be aware of some negative impacts that may occur, including:

- Controls may not work together in a cohesive manner (i.e., a control from one standard may work in opposition to a control from another standard).
- Controls may overlap or circumstances may arise where controls may be duplicated, resulting in wasted cost and/or effort.

5 Prosci, "What is the ADKAR model," *https://www.prosci.com/adkar/adkar-model* (Prosci and ADKAR are registered trademarks of Prosci, Inc. Used with permission.)

- Vast amounts of documentation may be required for each standard.
- Terminology may differ across standards, resulting in confusion for users.
- Silos of controls may be quickly established without dependencies or synergies identified.

It is, therefore, essential that integration of standards be carefully planned and opportunities and risk identified to avoid some of these pitfalls.

ISO/IEC 27000 Series—Information Security Management Systems

The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series is a set of information security standards that provide best-practice recommendations for information security management.

ISO/IEC 27001 and ISO/IEC 27002, in particular, are of interest from a GDPR perspective. ISO/IEC 27001 specifies an information security management system (ISMS) and ISO/IEC 27002 provides a catalog of information security controls that can be managed through the ISMS. Together, these two standards will help organizations comply with GDPR Article 32, "Security of processing." Mapping of selected ISO/IEC 27000 controls to the GDPR has been done by the Confederation of Danish Industry (specifically, the Danish ICT and Electronics Federation)[6] and ISO27001security.com.[7]

ISO/IEC AWI 27552 is a new standard under development that is particularly relevant to data privacy. It will be an enhancement to ISO/IEC 27001 for privacy management.

BS 10012—Personal Information Management System

This British Standard is a specification for a personal information management system (PIMS) and it supports many organizations in their implementation of appropriate information governance. The overall goals are to ensure good governance around data protection and its anchoring at the board level. This standard has been recently updated (April 2017) and the overall changes reflect alignment with ISO standard structure and GDPR. The new standard has a section for updated terms and definitions and separate sections concerning planning the PIMS and implementing/operating the PIMS.

ISO 29100—Information Technology—Security Techniques—Privacy Framework

Although the current version (2011) is not aligned with the GDPR, this ISO standard still provides a valuable, if not inspirational, framework for data privacy. The terminology may confuse some (among other things, "personally identifiable information [PII]" instead of "personal data," and yes there is a difference!). Since the scope of the standard covers only automated processing (not manual processing), it may make BS 10012 a worthwhile alternative.

6 The Danish ICT and Electronics Federation (DI Digital), "General Data Protection Regulation—Implementation in Danish companies," *http://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Persondataforordningen_engelsk.pdf*

7 ISO 27001 Security, "Mapping between GDPR (the EU General Data Protection Regulation) and ISO27K," November 2016, *http://iso27001security.com/ISO27k_GDPR_mapping_release_1.docx*

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53—Security and Privacy Controls for Information Systems and Organizations

Although not specifically aligned with European data protection legislation, this publication is a control standard that provides a comprehensive catalog of more than 300 controls that are flexible and customizable. Unlike earlier versions of the publication, the latest draft (revision 5)[8] makes the structure of the controls more outcome-based. It also identifies those controls that are both security and privacy controls, as well as those controls that are directly relevant to a data privacy program.

ISO 15489—Records Management

This standard covers records management, which, from a GDPR Article 30 perspective, is highly relevant. Article 30 requires organizations to maintain records of processing activities. Although GDPR does not specify exactly how this should be accomplished, evidence is required to demonstrate compliance, so it is advisable to follow best practices. Following ISO 15489 ensures both paper and electronic records are maintained, easily available and documented in the correct manner across their life cycle, from creation to disposal.

ISO 8000—Master Data Management

ISO 8000 is a series of "parts" that set out requirements for master data quality and the portability of enterprise master data. To reduce risk, organizations will benefit from creating and maintaining one single master reference source for all personal data, resulting in fewer errors and duplicate entries. This will also enable fulfilment of data subject rights. Under GDPR, in specific circumstances, data subjects have a number of rights including:

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object

ISO 22301—Societal Security—Business Continuity Management Systems—Requirements

ISO 22301 is a standard covering business continuity management. It was developed to help organizations deal with disruptive incidents to minimize major operational impacts and reduce any resulting losses. After implementation, organizations will be prepared to prevent and detect threats, while also being ready to act effectively and efficiently before, during and after a negative event. In GDPR terms, this standard is particularly relevant to data breach scenarios. Alternatively, organizations can also build upon existing crisis management procedures that may be in place.

PAS 99—Integrated Management Systems

PAS is the acronym for Publicly Available Specification, but it is not actually a formal standard despite following a similar naming convention. PAS 99[9] has been developed and published by the British Standards Institution to help organizations integrate two or more management system frameworks into a single framework. Potential benefits include:

8 National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," Draft SP 800-53, August 2017, *https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf*

9 BSI, "PAS 99 Integrated Management Systems," *https://www.bsigroup.com/en-GB/pas-99-integrated-management/*

- A single set of documentation for policies, processes and procedures
- Greater efficiency by removing duplicative efforts
- Greater ease in continual improvement efforts of management systems
- Less auditing effort
- Less confusion for users (different standards, different terms, etc.,) and more coherent training and awareness programs

Other Sources

There is a broad range of other sources of inspiration for data protection, including various blogs and articles from some of the reputable data privacy law firms. In addition, supervisory authorities—for example, the UK's Information Commissioner's Office (ICO),[10] France's Commission Nationale de l'Informatique et des Libertes (CNIL),[11] Ireland's Data Protection Commissioner (DPC)[12] and Norway's Datatilsynet[13]—also offer comprehensive websites with extensive resources, including tools, templates, guidance, white papers and investigation reports valuable to any data privacy program.

Establishing an Operational Life Cycle and Continuous Improvement

A life cycle model is integral to ensuring a continued focus on data privacy and a protection program that is ever-evolving to meet changing needs. The model will help to create a culture that prioritizes data protection throughout the organization, embedding it in daily operations. In addition, when new laws and regulations or business circumstances require changes to the data protection program, having an operation life cycle in place makes the task less daunting.

The key modules of a typical operation life cycle are briefly described in **figure 2**. Certainly, this model is not the only one; other established life cycle models can be used as well (e.g., plan-do-check-act).

10 *https://ico.org.uk*

11 *https: //www.cnil.fr*

12 *https://www.dataprotection.ie*

13 *https://www.datatilsynet.no*

EVALUATE

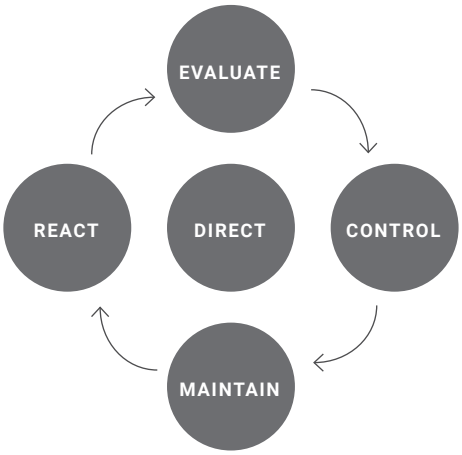
The process of evaluating can include several distinct activities, including:

- Analysis of the organizational impact of applicable laws and regulations
- Assessment of how the organization lives up to (external) laws, regulations, and client obligations, and (internal) policies and procedures
- Risk assessment of the operational data processing system
- Risk assessment of third-party vendors
- Privacy impact assessments/data protection impact assessments of new initiatives, processes, products and services
- Gap analysis
- Creation of a risk register, including a risk acceptance database
- Development of a privacy risk model
- Use of a three-tiered organizational model (business activities/processes, business applications, IT infrastructure)
- Mapping and analysis of data flow
- Creation of a data map/inventory
- Development of a registry of processing activities
- Assessment of program performance

REACT

Every well-designed data management program must anticipate and prepare for instances of control failure. Elements to be considered in preparation and response include:

- Incident planning
- Incident handling
- Data breach
  - Response team
  - Planning
  - Training and awareness
  - Wargaming/ rehearsal
  - -Detection
  - -Response
  - -Investigation
  - -Recovery
  - -Lessons learned
- Data subject requests
- Complaints
- Communication with supervisory authorities
- Client requests



CONTROL

Control can be analyzed from various standpoints, such as:

- Legal controls across the data management life cycle
  - Collection/creation
  - Storage/retention
  - Usage/disclosure
  - Disposal
- Data protection by design/default
- Risk treatment
  - Technical controls
  - Policy and procedural controls
  - Organizational controls
  - Risk transfer

MAINTAIN

Maintenance activities ensure a well-functioning data management life cycle and consist of the following components, among others:

- Audit and assurance
  - Attestation
  - Audit program
  - Third-party vendors
  - Internal policies and procedures
- Database of applicable laws and regulation
- Monitoring of changes to applicable laws and regulations
- Monitoring of privacy and security trends, and industry standards and bodies
- Training and awareness
- Organizational alignment/stakeholder management
- Reporting
- Revise privacy and security controls in line with new findings over time

DIRECT

The GDPR clearly shows the need for strong, specific and well-structured guidance for the privacy program, include entities and components such as:

- Data protection board
- Direction, approvals and decisions
- Data protection strategy
- Program management
- Program roles and responsibilities
- Risk register
- Remediation plans

FIGURE 2: Example Operations Life cycle Model

Source: DPO Network Europe.

Conclusion

The GDPR represents the biggest revamp of data protection legislation in the past two decades and has ramifications for organizations globally. Eduardo Ustaran, an internationally recognized expert in privacy and data protection law, recently stated in an article: "…very few (if anyone) will be truly and fully compliant with the GDPR when the time comes."[14] Even so, authorities will expect your enterprise is making the effort and will expect proof of that effort.

For organizations used to addressing compliance challenges and who are already able to demonstrate compliance to existing data protection legislation, the GDPR may only represent an expansion of their existing regime.

For those organizations that previously may have accepted the risk of non-compliance either intentionally (due to lack of enforcement or low penalties), or accepted the risk in ignorance or denial, a new and potentially time-consuming effort must be undertaken to formally improve data protection within the organization. Becoming operationally compliant requires investment and focus from all parts of the enterprise.

14 *https://iapp.org/news/a/privacy-in-2018-expect-the-unexpected/*

Acknowledgments

ISACA would like to recognize:

Lead Developer

Tim Clements
CGEIT, CRISC, FBCS CITP,
FIP, CIPP/E, CIPM, CIPT
Privacy Program Management,
Mitigate, Denmark

Expert Reviewer

Sue Milton
CISA, CGEIT
GEIT Business Advisor, UK

ISACA Board of Directors

Theresa Grafenstine
CISA, CRISC, CGEIT, CGAP, CGMA,
CIA, CISSP, CPA,
Deloitte-Arlington, VA, USA, Chair

Robert Clyde
CISM,
Clyde Consulting LLC, USA, Vice-Chair

Brennan Baybeck
CISA, CRISC, CISM, CISSP,
Oracle Corporation, USA, Director

Zubin Chagpar
CISA, CISM, PMP,
Amazon Web Services, UK, Director

Peter Christiaans
CISA, CRISC, CISM, PMP,
Deloitte Consulting LLP, USA, Director

Hironori Goto
CISA, CRISC, CISM, CGEIT, ABCP,
Five-I, LLC, Japan, Director

Mike Hughes
CISA, CRISC, CGEIT,
Haines Watts, UK, Director

Leonard Ong
CISA, CRISC, CISM, CGEIT, CPP, CFE,
PMP, CIPM, CIPT, CISSP ISSMP-ISSAP,
CSSLP, CITBCM, GCIA, GCIH,
GSNA, GCFA,
Merck & Co., Inc., Singapore, Director

R.V. Raghu
CISA, CRISC,
Versatilist Consulting India Pvt. Ltd.,
India, Director

Jo Stewart-Rattray
CISA, CRISC, CISM, CGEIT, FACS CP,
BRM Holdich, Australia, Director

Ted Wolff
CISA,
Vanguard, Inc., USA, Director

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5
Certified Assessor, CIA, CRMA,
EGIT | Enterprise Governance of IT
(Pty) Ltd, South Africa, Director

Christos K. Dimitriadis, Ph.D.
CISA, CRISC, CISM,
Intralot, S.A., Greece, Past Chair

Robert E Stroud
CRISC, CGEIT,
Forrester Research, Inc., USA, Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA,
Queensland Government, Australia,
Past Chair

Matt Loeb
CGEIT, FASAE, CAE, ISACA,
USA, Director

About ISACA

ISACA® (isaca.org) helps professionals around the globe realize the positive potential of technology in an evolving digital world. By offering industry-leading knowledge, standards, credentialing and education, ISACA enables professionals to apply technology in ways that instill confidence, address threats, drive innovation and create positive momentum for their organizations. Established in 1969, ISACA is a global association serving more than 500,000 engaged professionals in 188 countries. ISACA is the creator of the COBIT® framework, which helps organizations effectively govern and manage their information and technology. Through its Cybersecurity Nexus™ (CSX), ISACA helps organizations develop skilled cyber workforces and enables individuals to grow and advance their cyber careers.

ISACA®

3701 Algonquin Road, Suite 1010
Rolling Meadows, Il 60008 USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Web: www.isaca.org

Provide Feedback:
www.isaca.org/Data-Protection-Beyond-GDPR

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
www.twitter.com/ISACANews

Join ISACA on LinkedIn:
www.linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ