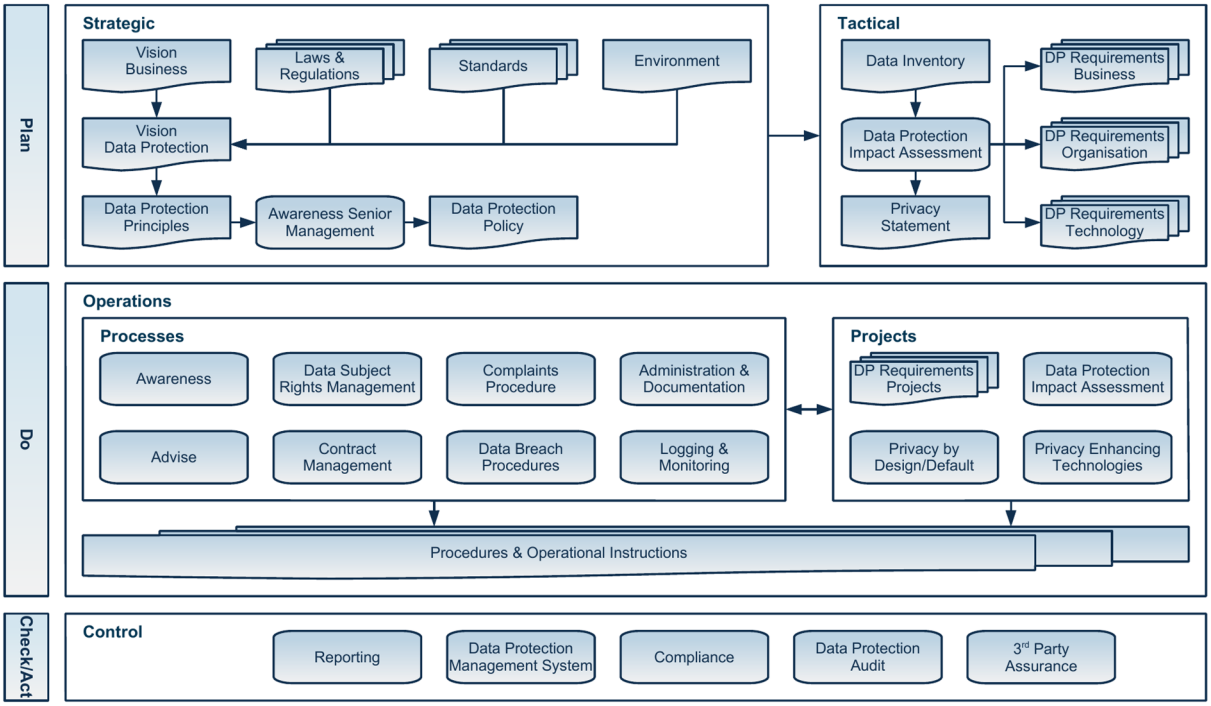
SECO®
INSTITUTE

WHITEPAPER
DPMF



Introduction

In today's digital and data-dependent economy, personal data is a valuable asset for organisations and consumers alike. Organisations in every sector rely on global data flows and connectivity to expand their brands, innovate their products and services, and optimise their processes. Consumers, in turn, view their data as a commodity that should be traded for benefits rather than be given away for free.

The enhanced use and appreciation of personal data pose three main challenges for organisations: to stay ahead of evolving cyber threats, to comply with increasingly stringent privacy and data protection laws, and to meet customers' enhanced privacy expectations. Today, and even more in the interconnected society of tomorrow, organisations' prosperity largely depends on their ability to protect data and demonstrate to consumers and regulators that they are reliable data custodians. This requires the implementation of effective and forward-looking privacy and data protection programs.

The SECO-Institute's Data Protection Management Framework is based on the premise that effective data protection can only be achieved along the principles of privacy by design and continuous improvement. The Framework provides a step-by-step guide to building a strong data protection culture by integrating and anchoring data protection in the organisation's strategic, tactical and operational management and managing data protection in a plan-do-check-act quality improvement cycle.

In the SECO-Institute's Privacy & Data Protection Practitioner course, the Framework is used to guide students through the steps of achieving and demonstrating GDPR-compliance.

Embedding Data Protection into the Organisation's Strategic Management

The creation of a data protection culture starts with making data protection one of the organisation's values, setting out the overarching direction for the organisation's data protection efforts, and building enterprise-wide commitment to data protection. This is achieved through a **Vision on Data Protection** and a **Strategic Data Protection Policy**.

Vision on Data Protection

The Vision on Data Protection is a document that describes what role data protection plays in the organisation, how data protection can contribute to the organisation's success, and what general data protection principles the organisation will follow. Naturally, the content of the Vision depends on the organisation's specific context. To decide what to include in the Vision, we need to analyse four main aspects:

Input for the Vision

1. **The organisation's corporate mission, vision and strategy**

Corporate mission describes why the organisation exists and whose needs it aims to satisfy. Corporate vision delineates the goals the organisation intends to achieve in the future. Corporate strategy defines the concrete objectives, the ways of their achieving and the key performance indicators.

Corporate mission, vision and strategy centre around corporate goals, ambitions and needs, some of which have a close link with data protection. Such links should be identified and described in the Vision on Data Protection. If a customer service agency's corporate vision is to "*assist customers by answering their questions, concerns and inquiries*", the Vision on Data Protection should point out that customers will only trust the agency with their questions, concerns and inquiries if they are convinced they can trust the agency with their personal data. Describing how data protection contributes to corporate goal attainment is crucial for establishing data protection as a core organisational value and obtaining the Board's support for data protection.

2. **The legal and regulatory requirements the organisation must meet**

In addition to data protection and privacy laws, the organisation is subject to other laws and regulations that have important privacy and data protection implications (corporate governance, e-commerce or financial regulations, to name just a few). To channel the organisation's data protection efforts and to demonstrate what a crucial role data protection plays in the organisation's overall legal compliance, all relevant legal and regulatory requirements (and compliance obligations) should be identified and outlined in the Vision on Data Protection.

3. **The quality standards the organisation has implemented or intends to implement in the future**

Quality standards are either imposed on the organisation by a regulatory body (for example, payment security standards are mandatory for entities that work with cardholder data) or implemented by the organisation voluntarily to guarantee the quality of products and services and gain a competitive advantage by enhancing consumer trust. Just as laws and regulations, quality standards also contain

requirements that are highly relevant for the organisation's data protection and should be incorporated into the Vision on Data Protection.

4. **The organisation's environment: the socio-political context in which the organisation exists**

The organisation's socio-political context means the overall political and social expectations that exist towards the organisation. Different organisations face different expectations as to how they should handle personal data. For some companies, a data breach is a minor inconvenience, whereas for others a data breach entails significant reputational damage and customer loss. Social and political expectations should be incorporated into the Vision on Data Protection as they help the organisation to set data protection priorities.

Drafting the Vision

The input gained from analysing the organisation's goals, obligations and needs should be described in in the Vision on Data Protection in a structured and transparent way. Accordingly, the Vision should

- outline what requirements the organisation needs to meet in relation to data protection;
- clarify how data protection can contribute to the organisation's success in terms of corporate goal attainment and legal compliance;
- set out strategic goals for the organisation's data protection ("*We will integrate data protection into the business processes", or "We will adopt a risk-averse approach to legal compliance"*);
- set out a strategy to achieve the strategic goals ("*We will make risk assessments an inherent component of project management",* or "*We will document every activity and decision in relation to personal data"*);
- translate the content and the focus areas to so-called **general data protection principles**. These are simple statements that reflect the organisation's overall attitude to data protection and the use of personal data ("*We will always choose the alternative that represents the lowest risk level").*

General data protection principles provide a solid foundation for the Strategic Data Protection Policy and enable decision-making in new situations that are not addressed in that strategic policy. Furthermore, well-formulated and concise principles can be easily remembered, which makes them an excellent tool to instil awareness and strengthen commitment to the Vision and data protection in general. To strengthen commitment, the Vision should contain achievable goals for senior management as well as employees.

Bringing the Vision to Life

Drafting a Vision document does not automatically make data protection a part of the organisational culture. The document can only fulfil its purpose if it is actively supported by the whole enterprise, from senior management to employees. Senior management must find the right techniques to actively promote the Vision and make it an integral part of employees' day-to-day experience. The most popular tools for this are peer-to-peer recognition, gamification, and the collective celebration of individual success stories. Senior management's attitude to the Vision is a crucial determinant, as organisational culture is largely shaped by the leaders' behaviour.

Strategic Data Protection Policy

While the Vision on Data Protection sets the main direction for the organisation's data protection efforts, the Strategic Data Protection Policy establishes general data protection rules, roles and responsibilities.

The rules set out in the Strategic Data Protection Policy (the strategic policy statements) should follow from the Vision's well-formulated and actively promoted general data protection principles. The stronger the link between the general principles and the Strategic Policy, the more cohesive the policy will become. Likewise, the more actively the Vision's general principles are promoted, the more accepted the policy will be among employees. The power of a policy statement such as "*all employees must follow the organisation's Clear Desk and Clear Screen Policy in their daily activities*", depends largely on employees' awareness and understanding of why personal data and data protection are important to the organisation.

The identification of roles and responsibilities means formalising the organisation's data protection expectations towards the Data Protection Officer (DPO), the Chief Information Security Officer (CISO), the Marketing Director, the HR Officer, line managers, and employees in general. (For example: "*In cooperation with the DPO, all line managers must familiarise employees with the content of the Strategic Data Protection Policy*"). The rules and responsibilities set out in the strategic policy govern the arrangements made at the tactical level (the so-called issue-specific policies).

When drafting the Strategic Policy (or any policy, for that matter), it should be borne in mind that the document is meant for *people*. A policy can only achieve its goal if employees see its relevance for their daily activities, and if the content is unambiguous and easily understood. Tailoring the language to the target audience and establishing clear lines of accountability enhance employees' willingness to adhere to the policy. The policy statements must explicitly describe who is expected to do what (for example: "*All employees are expected to wear their badges in a visible way while they are on the premises*" instead of "*Wearing a badge is mandatory*"). Sanctions for non-compliance must also be described in a transparent manner.

As is the case with the Vision, work should not be considered complete when the Policy is drafted. First of all, the organisation needs to ensure that the Policy reflects reality. This can only be achieved by managing the Policy in its own plan-do-check-act cycle. It is recommended to document all discussions and considerations relating to the policy, and use the information as input for policy review cycles. Drafting the policy should include establishing criteria based on which the policy will be reviewed, and allocating responsibility for the maintenance of the document.

Besides the content, the language and the administration of the Strategic Policy, attention should be paid to its communication and active promotion. All stakeholders who are expected to abide by the policy must be aware of its contents. Including the policy in the introduction program for new employees, creating an e-learning page on the intranet, organising quizzes and prize contests, or encouraging discussion about the latest data protection news in the context of the Policy, are all excellent tools to enhance understanding, awareness and staff engagement.

Embedding Data Protection into the Organisation's Tactical Management

At the tactical level, more specific rules and requirements are developed regarding the organisation's use and protection of personal data. To identify these rules and requirements, the organisation first needs to chart all of its processing activities and assess the data protection risks inherent in each activity.

Data Inventories and Data Flow Diagrams

Data inventories are performed to identify

- the personal data processed by the organisation
- the processes that use (collect, store, disclose, transfer, etc.) personal data
- the systems involved in the processing
- the persons involved in the processing (including employees who have access to the data as well as external recipients)

The easiest way to chart and analyse the information is the creation of data flow diagrams. These are simplified drawings that show how data flows through an information system.

The first step in creating a data flow diagram is to draw up the input side (what data goes into the system from what source) and the output side (what data goes out of the system and how it is used). Having drawn up a general overview of the data flows, a detailed diagram should be made for each process. At this phase, more information can be added to the diagrams (the categories of personal data concerned, the purposes of the processing, the legal grounds, and other relevant information). A crucial addition is the name and contact information of process owners, data owners and those responsible for the identified systems and data flows. Process owners should bear primary responsibility for data protection in their process.

Data Protection Impact Assessments

Having collected the relevant information about each process, the organisation needs to identify the vulnerabilities that might result in threats to the personal data. Subsequently, the organisation needs to determine the likelihood of the threats these vulnerabilities pose, and the severity of the impact each threat may have on the organisation and its data subjects. This is performed through risk assessments and/or Data Protection Impact Assessments (specific types of risk assessment that aim to identify and evaluate the risks the personal data processing entails for data subjects' rights and freedoms).

In certain legal frameworks, risk assessments and Data Protection Impact Assessments (Privacy Impact Assessments) are mandatory. The GDPR, for example, requires data controllers to demonstrate that all their security measures are based on appropriate risk and Data Protection Impact assessments, and that the measures provide sufficient protection to keep the risks at acceptable levels. Risk assessments should be performed even where they are not required by law, since effective security measures can only be determined in relation the sensitivity of the personal data processed, the vulnerabilities of the systems involved, and the likelihood of threats.

Data Protection Impact Assessments should be performed on every process, analysing as many aspects as possible (most importantly, the categories of personal data concerned, the purposes for which the different categories are processed, the legal bases, and the identity of the recipients). It is

crucial to bear in mind that not all threats come from external actors, such as hackers or social engineers. Non-compliance with the applicable laws (insufficient information for data subjects or weak controller-processor agreements) may also pose threats that are likely to have a high impact on the organisation and its data subjects.

Privacy Notice and the Identification of Business, Organisational and Technical Requirements

Detailed data flow diagrams and extensive Data Protection Impact Assessments provide the organisation with a deep insight into its own processing activities. The information obtained from data flow diagrams and risk assessments should lead to the creation or adjustment of the organisation's Privacy Notice (or Privacy Statement), ensuring that the document contains all the information required by law. On the other hand, data flow diagrams and impact assessments enable the organisation to identify specific **business, organisational** and **technical requirements** that need to be met in order to achieve the goals and principles set out in the Vision and to comply with the general rules and responsibilities outlined in the Strategic Data Protection Policy.

The most important **business requirement** is to embed data protection into business processes, procedures and projects, and to integrate the processes, procedures and all data protection activities into a management system (the Data Protection Management System), in order to ensure data protection's continual improvement. In this context, agreements should be made on how data protection will be integrated into processes and procedures, and decisions should be taken as to whether the integration should take place by adjusting already existing business practices or by implementing new practices. For example, the organisation may decide to integrate Data Protection Impact Assessments into an existing Business Continuity or Risk Management process, and integrate data breach procedures into an existing Incident Management process. The operational level of the Framework provides an overview of the data protection processes that need to be addressed in this regard.

Organisational data protection requirements include the establishment of the necessary functions and tasks in relation to data protection. Depending on the organisation's situation, this may include the detailed description of the role of the Data Protection Officer (or other data protection experts), together with the role of process owners, data owners and other relevant actors.

Technical data protection requirements (such as access control, authentication, secure transfer mechanisms, pseudonymisation, anonymisation, or data flow monitoring) are also identified based on the nature of the processing activities, the personal data concerned and the risks involved in the processing.

The identification of **business, organisational and technical requirements** results in the creation of agreements that contain more specific rules than the Vision and the Strategic Policy. Typical documents at the tactical level are:

- **Issue-specific policies**: binding agreements that describe specific data protection rules in a certain area. Examples of such documents include data subject rights management policies, access control policies, clear desk/clear screen policies, mobile device policies, or data breach response policies.
- **Guidelines**: recommendations of a less binding nature.
- **Behavioural codes**: binding agreements that describe the behaviour required from employees.

Embedding Data Protection into the Organisation's Operational Management

At the tactical level, different data protection requirements have been identified. These requirements (and the pertaining agreements) are implemented at the operational level, by integrating data protection processes and activities into the existing business practices, and/or by adopting new practices. The agreements made at operational level are set out in **procedures**, **work instructions** and **technical documentation**.

- **Procedures** are general descriptions of the actions that need to be taken to ensure and facilitate compliance with the organisation's (more abstract) policies.
- **Work instructions** are detailed documents that describe how the actions described in the procedures must be performed.
- **Technical documentation** includes information on the technical aspects, such servers, devices, and log files.

Operational-level agreements may relate to ongoing activities (**processes**), such as project management or reporting, and innovations (**projects**). Naturally, processes and projects and their data protection requirements are closely intertwined.

Processes

In the context of data protection, the most important processes are:

- **Awareness**: Effective data protection requires employees to be aware of data protection risks and handle personal data accordingly. To implement or improve awareness measures, the organisation needs to analyse employees' behaviour towards personal data, chart the behaviours that present a data protection concern, define the desirable behaviours, and determine how employees will be inspired towards behavioural change. It is also essential to decide how progress will be assessed.

- **Data subject rights management**: Data subject rights are an important focus area in legal compliance and consumer relationships. To manage data subject rights in accordance with the applicable legal requirements and consumers' expectations, the organisation needs to have a clear picture of the data subject rights that can be related to the different phases of the data life cycle (for example, under the GDPR, data collection is tied to the data subject's right to be informed, while storage has a close relationship with the data subject's right to erasure). In this context, the organisation needs to decide what solution should be implemented to manage data subject rights (a simple Excel sheet or a more complex tool). Finally, the organisation needs to establish a process to handle data subject requests (e.g. a regularly checked Service Desk mailbox), and clarify what part the DPO plays in managing data subject rights and handling data subject requests.

- **Complaints procedure**: Although the law may not oblige the organisation to set up its own complaints procedure (the GDPR, for instance, only requires controllers to inform data subjects about their right to lodge a complaint with the supervisory authority), it is advisable to set up a complaints procedure. Such a procedure allows the organisation to establish the criteria that determine whether the complaint is truly about personal data processing, and to establish rules for the timely handling of complaints, the creation of the necessary documentation, and the DPO's involvement.

- **Administration and documentation:** The appropriate administration and documentation of data protection activities play a crucial role in demonstrating legal compliance. Under the GDPR, the controller must evidence every step it has taken in relation to data protection. To facilitate legal compliance, the organisation needs to ensure that the administration (oversight and supervision) and the documentation (drafting, formatting, submitting, reviewing, approving, distributing, reposting and tracking documents) of the organisation's data protection operations are regulated by clear and unambiguous agreements.

- **The DPO's advisory role:** In line with the DPO's general responsibilities set out in the Strategic Policy, the organisation needs to create formal rules relating to the exercise of the DPO's advisory role in relation to the business processes. To ensure that the DPO fulfils its function, agreements should be made on the DPO's role in raising awareness, monitoring adherence to the policies, and ensuring that the mandatory documentation (processing registers, impact assessments, etc.) is maintained. Particular attention should be paid to the DPO's cooperation with the Board of Directors, HR, IT, Sales and Marketing, and the legal or compliance department.

- **Contract management:** To ensure legal compliance, controller-processor agreements should be managed in a contract life cycle. In this context, it is essential to identify what functions (DPO, legal department, IT department, compliance department) play a role in each contract life cycle phase.

- **Data breach (notification) procedures:** Such procedures are created to facilitate compliance with the data breach notification obligations imposed on the organisation by law, and to contain reputational damage in the event of a data breach. Data breach procedures should provide unambiguous criteria as to when an incident should be considered a data breach. They should also set out the steps of notifying the parties concerned and documenting the breach.

- **Logging & monitoring:** Good logging and monitoring practices (early detection and remediation) enable the organisation to minimise the consequences of privacy failures, and facilitate the confirmation or exclusion of a data breach.

Projects

As projects usually result in a change, their implementation is likely to entail new data protection risks. Effective data protection requires assessing these risks at the earliest possible point. This means that data protection, especially Data Protection Impact Assessments and privacy-enhancing technologies (anonymisation, pseudonymisation, encryption, access control, and similar technologies), should become an integral part of every project. Security or privacy documents, templates or requirements should be integrated into the organisation's project management methodology.

Control

Control is an essential component of the quality improvement cycle: it is the driver of well-considered decision-making and good governance. The control phase encompasses reports, the integration of all data protection processes and activities into a Data Protection Management System, the performance of audits, and third-party assurance.

Reports

Reports inform stakeholders of the effectiveness of the organisation's operations, and the state of play in corporate goal attainment and legal compliance. Reports are an essential element of continual improvement, as they provide useful insights into possible gaps between "rule" and "practice".

Data protection reports may be aimed at assessing

- the overall maturity of the organisation's data protection program
- the effectiveness of the security measures – to improve resource allocation
- trends – to enable proactive action, such as policy adjustments or the creation of new policies
- Return on Investment (ROI) – to assess whether investments are paying off, e.g. in the case of data protection and privacy trainings

When establishing a data protection reporting mechanisms, particular attention should be paid to the identification of key performance indicators. These are quantifiable measures that can be used to assess the organisation's performance against the strategic and operational goals. Good reports allow the organisation to draw conclusions about what practices are effective, what goals have been achieved, and what areas require enhanced attention. Reports support effective governance by enabling senior management to identify risks and set priorities.

Data Protection Management System (DPMS)

Integrating all data protection processes and activities (including reporting mechanisms) into a Data Protection Management System enables the organisation to establish effective governance and continually improve the organisation's data protection. By creating a DPMS, data protection becomes an integral part of corporate governance.

The DPMS can be integrated into an already existing Information Security Management System (ISMS). The two management systems can be easily related to each other, as they both aim to adopt a systematic and risk-based approach to information/data management, considering three main aspects: people, processes and IT systems. An ISO/IEC 27001-compliant information management system implements controls in the same domains as a DPMS:

- The context of the organisation (goals, requirements, expectations and needs)
- Leadership (awareness, commitment and policy)
- Planning (data protection objectives and risk management)
- Support (documentation/accountability, awareness and resources and competencies)
- Operation (implementation of controls and processes; projects)
- Performance evaluation (monitoring and reporting, management reviews and audits)
- Improvement (use outcomes of the previous steps to establish a continuous improvement cycle)

If the DPMS is integrated into an ISMS, specific data protection policies, procedures and controls should be added to the existing information security safeguards.

Compliance

Compliance refers to the organisation's adherence to mandated boundaries (laws and regulations) and voluntary boundaries (internal policies, procedures, and similar standard-setting documents). Governance, Risk Management and Compliance (GRC) are regarded as the three main pillars that work together to assure that an organisation meets its objectives. While Governance aims to lead the organisation towards goal attainment, Risk Management predicts and manages the risks that can hinder the organisation from achieving its goals, and Compliance facilitates goal attainment by monitoring adherence to the law and the organisation's own rules. Compliance is demonstrated through audits.

Data Protection Audits

Audits are formal inspections aimed at verifying compliance (compliance audits) or evaluating whether efficiency targets are met (internal audits). While compliance audits are performed to assess the organisation's compliance with laws or quality standards, internal audits aim at improving the effectiveness of the organisation's operations or risk management, control, and governance processes. Audits are performed by internal compliance officers, external auditors or government officials. Audits are usually coordinated by the organisation's Compliance department.

Privacy and data protection audits are aimed at investigating whether the organisation processes personal data in line with the applicable privacy laws. Such audits may be required by law, but they may also be performed to assure stakeholders that the organisation meets its contractual obligations.

Audit findings constitute a key input for the "act" phase of the quality improvement cycle.

Third-Party Assurance

As the importance of personal data grows and data protection laws become stricter, organisations become increasingly aware that outsourcing functions or activities to a third party (a service organisation) includes risks. Data protection laws, such as the GDPR, mandate outsourcing organisations (controllers) to assure that their processors process personal data in accordance with the law. Together with ultimate responsibility for the processing, the law also gives data controllers the right to perform audits on their processors' data protection controls (including Data Protection Impact Assessments, risk mitigation plans, and the use of privacy by design measures, such as pseudonymisation and data minimisation). For service organisations, third-party assurance through audit reports is an essential business requirement.

One of the most effective ways a service organisation can provide assurance about its risk management and controls is through a Service Auditor Report. A Service Audit Report describes the organisation's controls, and may include the testing of the controls over a six-month period.