January 2018

Data Protection Management System for GDPR compliance - using COBIT®

Contents

Executive summary

The General Data Protection Regulation (GDPR) delivers a fundamental change in how controllers and processors handle personal data. Data protection can no longer be an afterthought. The protection of personal data must be designed into the functioning of business operations, with privacy in mind at every step and the default position for privacy being that the strictest settings are applied without any manual input from the end users.

COBIT® is a popular framework used widely around the world to define information and technology processes; determine key activities and the related inputs and outputs; implement key practices; measure, evaluate and monitor performance; identify instances of non-conformance and manage information and technology risks through the selection and implementation of suitable controls.

The GDPR imposes a broad range of technological and organisational obligations with which enterprises must comply. Many controllers and processors are struggling to protect the fundamental rights and freedoms of data subjects as they do not adequately understand who, what, where, when, why and how personal data is being processed.

COBIT®, being a reference model for information and technology processing, can provide controllers and processors with the information required to determine how best to protect the rights of data subjects whose personal data is being processed. Organised around 37 processes and seven enablers of good governance, management and operations, COBIT® can be used as the foundation on which an organisation builds its capability to process personal data lawfully.

To fulfil the requirements of the GDPR, organisations will need to transform their legal obligations into practical organisational and technical measures.

As many organisations do not have people who understand information and technology well enough to determine best practices for processing personal data, the risk of non-compliance with the GDPR will be high.

Organisations should make use of COBIT® to design their data protection processes such as data subject access requests, data protection incident response and breach reporting. They can also use COBIT® to plan, implement, operate and monitor

- information security
- application controls for completeness, accuracy and validity of personal data
- technical and organisational safeguards for the lawful processing of personal data.

Using COBIT® to address the obligations of the GDPR is benefecial as COBIT® is a single, holistic framework that can be easily adapted to an organisation's specific needs. It can scale from being used as a reference for just a few data protection activities, for providing the design for executable data protection processes, to being an integrated, enterprise-wide, governance and management system to develop, implement, operate and monitor all data protection practices in accordance with the GDPR.

Today, enterprises no longer need to spend months learning about COBIT® and working on its implementation. A fully functional implementation of the COBIT® framework is available "out-of-the-box" to support an enterprise in fulfilling its GDPR obligations using recognised best practices for information and technology.

A GDPR compliance programme can be accelerated with the aid of a Data Protection Management System and by using COBIT®. The Data Protection Management System provides the automation, orchestration and document management to control the many data protection activities that are required across an organisation, scaling from small entities to large multi-national organisations. Information from the COBIT® framework can provide assistance with the design, build and delivery of a GDPR compliance framework as well as identify and develop technical and organisational safeguards for processing personal data.

Step-by-step guidance is available in the Data Protection Management System to help controllers work through the GDPR requirements and build a compliance framework that is easily adapted to their particular needs. COBIT® process templates can assist controllers in establishing and operating the data protection processes that will enable data subjects to exercise their rights and freedoms.

A master plan for protecting personal data should be created to identify and organise activities, determine priority and assign tasks to personnel with operational responsibilities across the organisation.

A Data Protection Management System can be used to:

- plan the workload
- assign tasks
- communicate requirements
- provide support
- track progress
- collect evidence of results.

Data protection dashboards are customisable and can provide overviews of:

- programme percentage completed
- current status of compliance with the GDPR
- status of particular technical and organisational measures
- progress within business units
- status of processor compliance.

Templates are available for inventorising the personal data processed, mapping data flows, performing data protection impact assessments and conducting audits of operational environments.

A threat and vulnerability catalogue provides information for risk analsyis and the library of safeguards can assist with identifying suitable technical and organisational measures to protect the rigts of data subjects.

Data Protection Management System using COBIT

Inventorise personal data

Complete data maps

Record and respond to data subject access requests

Keep track of the privacy-related safeguards across the organisation

Map data protection policies to operational practices

Manage processor contracts

Perfom audits using best practice catalogues

Manage consent withdrawal and/or refresh

Process data correction requests

Validate processor compliance

Work with the supervisory authorities.

Peter Hill
Director

GDPR Services
Data Protection Management Systems

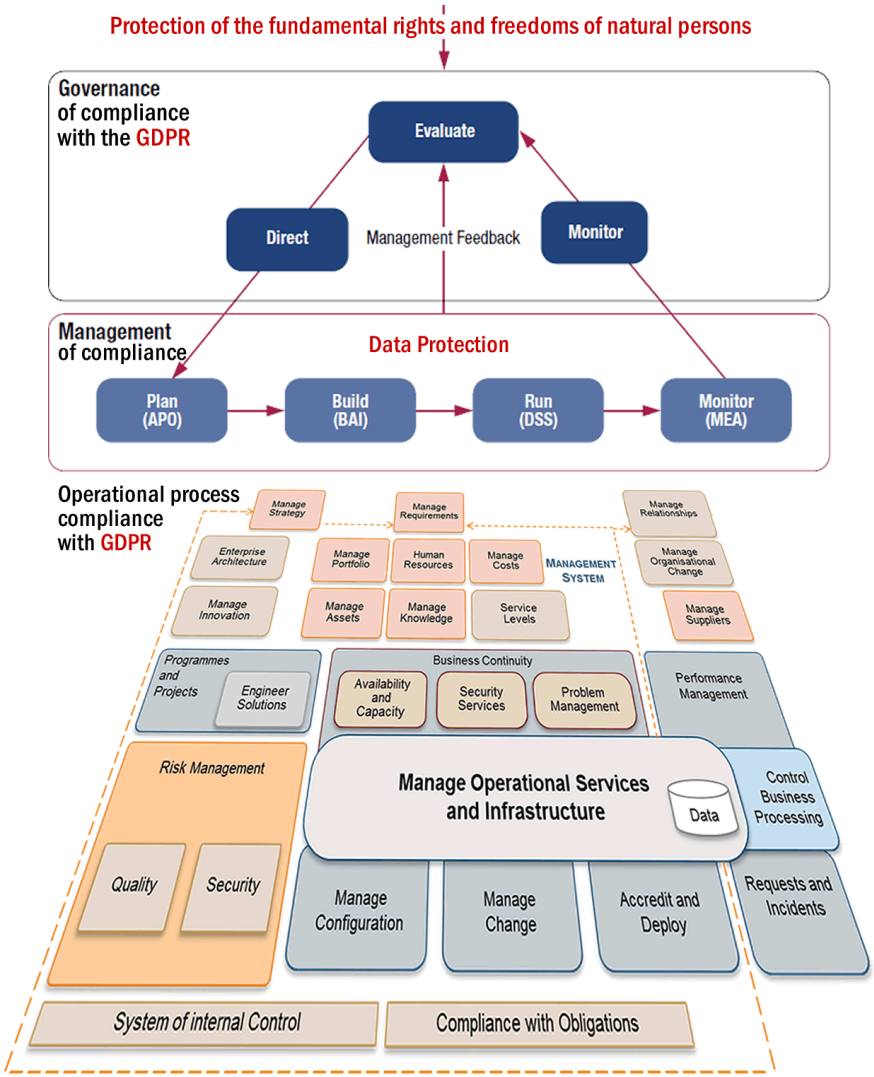
Mobile: +44 (0)3333 031103
Email: info@itgovernance.com

Guus Teley
Director

GDPR Solutions
Data Protection Management Systems

Mobile: +31 (6) 1486 4089
Email: guus@itgovernance.com

Using COBIT to establish a data protection management system for the GDPR



The integrated COBIT® governance, management and process model

COBIT® is a governance, management and process framework published by ISACA. It can be used as the foundation for addressing the requirements of the GDPR. As a governance, management and process model for information and technology, COBIT® can be used to institutionalise the enablers of information and technology governance, management and operations.

People (organisational structure, frameworks, skill and culture), processes, information and technology are all integrated in a governance and management system to address the requirements of the GDPR. The COBIT® process descriptions assist in clarifying governance, management and operational roles, responsibilities and tasks for data protection and to comply with requirements of the GDPR.

COBIT® is a reference model that describes how to establish a governance framework, a management system and a wide range of processes that are relevant to data protection and necessary to protect the rights of data subjects in accordance with the GDPR.

The COBIT® framework recognises that governance is different from management. It defines governance as ensuring that stakeholder needs, conditions and options are evaluated to determine and agree with the objectives to be achieved - for the GDPR this would be data protection. It includes setting a direction through prioritisation and decision-making and monitoring performance and compliance.

Management comprises the activities undertaken in alignment with the direction set by the governing body to achieve the eneterprise's data protection objectives. Typically, management will plan, build, run and monitor a wide range of activities that, for reasons of effectiveness and efficiency, are best organised in processes.

In many respects, the approach to the GDPR is the same as that for any other business objective of the organisation. It starts with identifying the stakeholders and prioritising their needs. For the purpose of the GDPR, an organisation will first establish the enterprise goals for data protection, translate these into business function, process, service, product, project, information system and technology goals, and cascade these goals to the underpinning enablers (described in the GDPR as technical and organisational measures) such as policies, frameworks, skills, organisational structure, culture, processes and services and technologies.

Many data protection tasks are required to comply with the GDPR. Some will have a discrete life-cycle and others will be ongoing. The COBIT® approach is to use a management system to direct and control data protection activities required enterprise-wide. A master plan is created to comply with the GDPR and the activities are assigned to process owners and team members who will then build capability to fulfil the GDPR requirements, run the data protection activities whenever necessary and react when non-comformance with the GDPR is detected. The approach is to start small and, using the management system, continuously improve.

Tools for the Data Protection Officer

Data protection officers (DPO) do not have to be lawyers but they do need:

- expert knowledge of data protection laws and practices
- a good understanding of the organisation's data processing arrangements
- knowledge of information and technology infrastructure, and
- to be prepared to respond to requests from individuals who want to exercise their rights regarding the processing of their personal data.

Centralising data protection can reduce bureaucracy and provide an efficient way to ensure compliance with the GDPR's data protection requirements. This is especially true when it comes to sophisticated data processing activities and cross-border data flows within a large organisation or group of organisations.

Effective GDPR compliance management by the DPO will reduce interventions by the supervisory authorities and can help prevent costly disputes.

To understand how tools can help the DPO, consider the following main responsibilities of the DPO:

- perform his or her tasks having due regard to the risk associated with processing operations
- provide independent supervision of an organisation's compliance with the GDPR
- inform and advise the controller or the processor and the employees who carry out processing of their GDPR obligations
- monitor compliance with the GDPR, the policies of the controller or processor in relation to the protection of personal data, and the related audits
- monitor the responses of the data controller, including the reviews carried out by the controller to assess if processing is performed in accordance with the data protection impact assessment
- act as the contact point for the supervisory authority on issues relating to processing, including when prior consultation is required.

The Data Protection Management System will assist the data protection officer with:

- maintaining an inventory of information assets
- maintaining a register of legal and contractual data processing obligations
- collecting information (data mapping) and documenting the processing of personal data
- maintaining a repository of relevant data processing information
- maintaining catalogues of data protection threats
- performing data protection threat and vulnerability assessments
- assigning and tracking progress with data protection related activities
- detailing preferred data processing practices for specific business units
- maintaining catalogues of data processing safeguards
- identifying safeguards and monitoring effectiveness
- monitoring privacy sensitive business practices
- receiving alerts of vulnerabilities and interferences with data subjects' rights
- recording and processing information requests and handling complaints
- measuring conformance and performance
- tracking responses to instances of non-conformance.

"Tools" and automated processes of the Data Protection Management System that can assist DPOs include:

- case management to handle data subject requests and complaints
- incident management to process breaches and notifications
- inventory and data mapping
- risk assessment for prior consultation
- data protection impact assessments
- technical and organisational measures library
- technical and organisational measures assessment programmes
- data subject access requests
- consent management
- data correction and destruction
- processor contract management
- processor service validation
- verification of processor assertions of compliance.

Components of a Data Protection Management System for the GDPR - using COBIT®

Establish accountability for compliance with the GDPR - demonstrate the status of data protection

The GDPR specifies that controllers are responsible for and must be able to demonstrate that they comply with the principles relating to the processing of personal data.

Controllers are required to:

- implement appropriate technical and organisational measures
- introduce data protection by design and by default where relevant
- ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and
- review and update the measures where necessary.

The Data Protection Management System enables controllers to establish a governance framework and management system by using the COBIT® principles as a guide. Next they can assign data protection responsibilities to personnel across process domains using the COBIT® process templates as a reference for clarifying responsibilitiy and as the basis for determining the most appropriate technical and organisational measures.

A central repository maintains details of the operational process activities, the risks to data subjects from processing personal data in the processes, and details of the controls (technical and organisational measures) selected and implemented. Evidence regarding status of implemented controls and their effectiveness is stored within the management system, protected using role-based access controls, for later use in evaluating and demonstrating compliance.

Record operational processes – identify the use of personal data and map data flows

Recording details about the processing of personal data in the organisation's operational processes is amongst the most time consuming data protection activities required by the GDPR.

Whilst a risk-based approach is needed for most activities, it is first necessary to establish an inventory of information assets and document the data flow of each process before a data protection impact assessment can be completed.

With many business processes (human resources, marketing, etc.) often being similarly structured across organisations, creating customisable generic process templates will save time and increase efficiency.

Frequently there are insufficient resources available to assist with the identification of personal data being processed that are able to determine whether the processing of personal data is necessary and can recognise which technical and organisational measures are best to counter the risks to the data subjects. The COBIT® framework can assist controllers with data mapping as it has extensive guidance on process activities, data flows and internal controls for many processes.

Organisations are required to maintain records of the categories of individuals whose data is being processed, the categories of recipients of the data, geographical whereabouts of the data, the retention periods that apply to the data and the security measures implemented. Using the COBIT® process descriptions will assist controllers with quickly producing the required records.

Records relating to the processing of personal data and progress with completing the documentation can be maintained within the Data Protection Management System.

Perform data protection impact assessments - identify the impact on the rights of data subjects

A data protection impact assessment (DPIA) is a process designed to describe the processing, assess the necessity and proportionality of a process and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing the risk and determining the measures necessary to address the risks).

DPIAs are important tools for accountability, as they help controllers not only to comply with the requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance. In other words, a DPIA is an important process for building and demonstrating compliance.

COBIT® can assist controllers with developing a process to undertake data protection impact assessments as well as recognising the impact that processing personal data has on business processes, services, products, projects, IT processes, IT applications, and IT systems.

Often a single organisation will find that it requires between 20 to 40 data protection impact assessments. In larger organisations and groups of enterprise the number of DPIAs required increases considerably. Sometimes the processes across a group of enterprises will be fairly similar and there could be considerable cost savings from establishing templates for sharable DPIAs .

While a single Data Protection Management System is able to support any number of enterprises and their respective DPIAs, the benefits of a single management system should be evaluated against the impact that this may have on the rights and freedoms of any data subjects whose data may be stored within the system's database (e.g. subject access request database).

Implement technical and organisational measures to protect the rights of data subjects

The GDPR requires controllers to take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure and demonstrate that processing is performed in accordance with the GDPR. The challenge for controllers is to operationalise this legal requirement in a technical manner.

In the Data Protection Management System a common language is used to ensure that the legal requirements are are actually implemented as technically specified. Use is made of data protection objectives to establish a link and to identify data protection requirements that can be assigned to individual processing objectives according to their importance, intended effect, and the expected outcome objective so that implementation takes place in a structured manner.

The data protection requirements are transformed into specific technical and organisational measures via these data protection objectives. Often the data protection objectives are in a state of dual interplay. Strengthening one data protection objective will be to the detriment of its counterpart. Careful evaluation is necessary to achieve the proper balance between data protection objectives.

The Data Protection Management System helps controllers to establish, implement and maintain the many different technical and organisational measures usually required across an enterprise.

Establish processes for breach notification, data subject requests and consent management

Under the rules of the GDPR, controllers have to inform the supervisory authorities of breaches in processing personal data without undue delay, and within 72 hours of becoming aware of the breach. In cases where a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the controller must also notify the data subjects without undue delay.

To be in a position to respond to a breach effectively and notify the supervisory authorities in the manner required, a process is required to log each breach, guide the response, track the resolution of the breach, as well as communicate relevant information to the supervisory authorities in the expected manner.

The GDPR codifies a broad range of procedures and controls that are required to protect the fundamental rights and freedoms of data subjects when processing their personal data.

Where the nature, scope, context or purpose of data processing are likely to result in a high risk to the rights and freedoms of the data subject, the processor has the obligation to perform a data protection impact assessment. When determining whether a high risk results from processing personal data, the process used should be repeatable and then later demonstrable to the supervisory authorities.

A Data Protection Management System with pre-defined processes for compliance with the GDPR will help controllers fulfil their obligations using automated processes to manage the workflow, keep track of the progress and maintain records as evidence.

Measure, evaluate and monitor performance and conformance with the GDPR

Data protection objectives serve to identify the data protection requirements for the operation of business processes in compliance with the GDPR. The technical and functional design of information systems and related organisational structures help institutionalise the data protection requirements and transform objectives into specific technical and organisational measures.

The COBIT® framework can assist controllers with the technical and functional design of information systems and the related organisational arrangements. It assists controllers in developing measures that are effective in monitoring the compliance of the operational processes.

A Data Protection Management System includes processes to measure the effectiveness of the implemented measures and conformance with the GDPR.

Actions and events in business processes that can impact the achievement of the selected data protection objectives of the business processes are identified and measured, evaluated and monitored. Non-conformance is identified and reported to controllers for action.