DPO-Connect

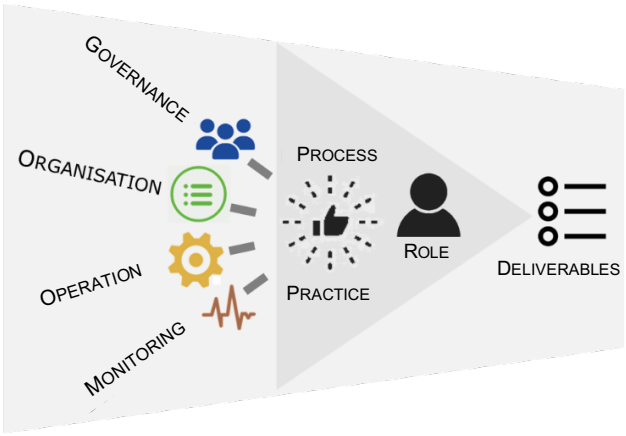
Strengthening the communication and interactions among DPO's and the Belgian DPA through a digital platform

How to develop a GDPR compliance programme?

Florence de Villenfagne and Patrick Soenen

Co-funded by the European Commission

This report was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020). The content of this report represents the views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.



How to develop a GDPR compliance programme

Deliverable D3.2

written by DPO-pro in the framework of the European DPO-Connect project[1]

3 June 2022

Authors: Florence de Villenfagne and Patrick Soenen

Co-funded by the European Commission

DPO-Connect is a project co-funded by the European Commission (DG JUST) under the European Union's Citizens, Equality, Rights and Values programme (2014-2020).

DPO-Connect partners: The Belgian Data Protection Authority (DPA), the Professional Union of DPOs of Belgium (DPO-pro) and the Vrije Universiteit Brussel (VUB)

[1] The content of this deliverable reflects only the opinion of its authors and is in no way an official position of the European Commission, DPO-pro or the other partners of the DPO-Connect project. The European Commission and the authors accept no responsibility for any use that may be made of the information contained therein.

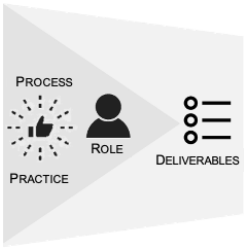
Preamble

When a lawyer and an auditor specialising in data protection write a study together on an GDPR compliance programme, the result is creative and inevitably different from what is usually written about GDPR compliance by lawyers or security specialists.

The idea of this deliverable is to have a fresh, practical view, to see things from an internal responsibilities point of view and thus be able to practically help organisations to structure their GDPR compliance. The General Data Protection Regulation is too general a piece of legislation for organisations to easily implement. As organisations structure their activities in processes by specifying the roles and responsibilities of the various stakeholders, this publication has sought to transpose the requirements of the Regulation into processes, accompanied by responsibility matrices, specifying the deliverables generated as a result.

Who is responsible for the actions? Who has to take action? Who is going to provide help and advice and who absolutely needs to be informed for the GDPR to finally be implemented effectively and sustainably? And what deliverables should come out of the exercise? These are the questions we have tried to answer.

The process reference framework has been borrowed from the work done by the GDPR working group of the IFACI (French Institute for Audit and Internal Control)[2], with their kind permission.



The practices, responsibility matrices and deliverables were developed as part of this publication.

We found a great deal of literature that explains the GDPR, presents the principles and explains the obligations. We have not yet found a presentation that focuses on the usual roles and responsibilities within organisations.

Our work can obviously be improved and we do not guarantee the exhaustiveness of the result. In line with the Plan-Do-Check-Act methodology that we hold dear, we would be delighted to have your constructive feedback to help us complete this study. In the meantime, we hope that our work will be useful to you.

The authors

Florence de Villenfagne *Patrick Soenen*

[2] Cf. *Controlling and Auditing GDPR Risks*, **IFACI GDPR Working Group**, 2021, available to IFACI members only. The working group was composed of Qadir Abdul, Valérie Bonnel, Pascale Chabrillat-Trahin, Maud Choquenet, Gilles Le Beux and Marjorie Mengeaud and facilitated by Patrick Soenen.

Table of contents

1. Purpose and scope

The purpose of the publication is to propose all the general actions to be carried out by an organisation to comply with GDPR in terms of the roles and responsibilities of the organisation's stakeholders and the deliverables to be achieved.

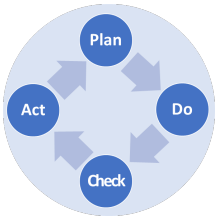
The General Data Protection Regulation3 (hereafter "GDPR" or "Regulation") determines the requirements for the protection of personal data. The European Data Protection Board (EDPB) guidelines provide guidance on understanding the requirements, but do not explain how to practically implement these requirements.

This publication proposes a set of processes that are structured into four areas: Governance, Organisation, Operational Management, Monitoring. (Best) practices[4] are proposed for each process to be implemented within the organisation. Each practice will need to be broken down into a number of tasks required to implement them. These tasks are not included in this study. They will have to be defined according to the importance of the processing of personal data, the sector of activity, the size and internal structure of the organisation, etc.

The publication does not take into account the specificities arising from national legislation or variations according to specific sectors of activity, such as healthcare, which involve the processing of a large number of specific categories of data.

GDPR compliance is a recent development in organisations and this implementation must be integrated into and linked to the governance and control structures and mechanisms in place. Its impact on data governance, risk management and information security is significant and continuous alignment with regulatory requirements is a must.

In addition to the implementation of compliance, its sustainability must be established. In accordance with the Deming Cycle, continuous improvement is based on four steps:



- Plan, which consists of defining the work to be done;
- Do, which involves implementing the activities;
- Check, which consists of ensuring that the activities are carried out as planned;
- Act, which involves adjusting the deployment of activities.

2. Target audience

This guide is intended primarily for Data Protection Officers (DPOs) or equivalent, but also for any person involved with the implementation of the GDPR.

3. Roles and responsibilities

By process, and for each practice - an action contributing to the achievement of the process objective - there is a proposed responsibility matrix using the RASCI model and with the following definitions:

- ***R - Responsible***: the role that performs the work to accomplish the activity. One or more roles can perform the work.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[4] In this document, by '*practices*' we mean the actions necessary to achieve the objective of the process.

- ***A - Accountable***: the role that validates activity, provides accountability and takes responsibility. Each practice has a single person who is accountable, separate from those who perform the activity.
- ***C - Consulted***: the role(s) that is/are consulted and provide(s) information.
- ***I - Informed***: the role(s) that is/are kept informed of the results of the activities.
- **S - *overSight***: The role(s) that verifies/verify the completion of activities and/or compliance with regulations.

Practices specific to these structures are proposed for organisations with extensive governance and control structures. However, organisations that do not have specific functions will need to determine which role will take on the responsibilities.

The following roles are included in the responsibility matrices:

Role	Description
INTERNAL STAKEHOLDERS	
Controller (DC)	The natural or legal person, public authority, department or other body that determines the purposes and means of the processing[5].
Governing body	Often referred to as the Board of Directors, the Governing Body pursues sustainable value creation by the company, by setting the company's strategy, putting in place effective, responsible and ethical leadership and monitoring the company's performance. It approves the internal control and risk management framework proposed by executive management and reviews its implementation.[6]
Executive management[7]	• Is in charge of the operational management • Implements internal checks based on the framework approved by the governing body • Submits financial statements and prepares for regulatory disclosure • Provides the board of directors with the information necessary for it to carry out its responsibilities • Is accountable to the governing body
Audit Committee	This committee assists the board of directors in ensuring the accuracy and fairness of the accounts and the adequacy and effectiveness of the organisation's internal control and risk management systems. It monitors the internal and external audits. The Audit or "Audit and Risk" Committee[8] is established by the Board of Directors.

[5] See definition in Article 4 (7) of the GDPR

[6] See *The Belgian Code on Corporate Governance*, Principle 2 Board - Strategy - Supervision, **Corporate Governance Commission**, 2020, (https://www.corporategovernancecommittee.be/assets/pagedoc/2003973319-1651062453_1651062453-2020-belgian-code-on-corporate-governance.pdf - accessed 3 June 2022)

[7] **Cf. *The Belgian Code on Corporate Governance*, Principle 2 Executive Management, Corporate Governance Commission, 2020, *op.cit.***

[8] Cf. *The Belgian Code on Corporate Governance*, Principle 4 Audit Committee. **Corporate Governance Commission**, 2020, *op.cit.*

Role	Description
Data Protection Officer (DPO) or Privacy Officer (PO)	The DPO is responsible for informing and advising the Controller who has appointed them on their obligations under the GDPR. They also have a role in monitoring compliance with the regulations. While the DPO is a role defined by the GDPR, the Privacy Officer is an unofficial role not defined by the Regulation. It the Controller has an obligation to appoint a DPO under the GDPR, it can only appoint them as "DPO" and the DPO will have the functions and duties set out in the GDPR. If the Controller does not have this obligation, they may still choose to appoint a person in charge of verifying and advising on compliance with the GDPR. They may call them "PO" or otherwise. The PO may therefore perform similar functions to the DPO or only part of them. This is at the discretion of the Controller. If the Controller is not obliged to appoint a DPO, but appoints one anyway, giving them the name of "DPO", this DPO will have to meet all the criteria provided for the DPO by the GDPR (Articles 37 et seq. of the GDPR).
GDPR Contact	Employee who may be designated in a department to relay information from the DPO to employees, advise them, ensure compliance with GDPR requirements on a day-to-day basis, apply the action plan and feed back requests or incidents to the DPO. Some call it something else ("Data Steward" or "Privacy Contact Point", etc.). We have decided to call it "GDPR Contact".
Chief Information Security Officer (CISO)	Person responsible for the implementation and supervision of the information security policy. The name Security Advisor is also used.
Department processing Personal Data (PD)	Any department that processes personal data as part of its operational activities.
Legal department	Department responsible for the legal issues that arise in an organisation. Some organisations appoint the DPO within the legal department.
Information Technology Department (IT)	The Information Technology department is responsible for managing the organisation's information systems. It is responsible for defining the architecture of the information system and designing, installing, deploying and operating it. In this context, it is often involved in the design of personal data processing solutions. These functions are incompatible with that of the DPO.
***Project Management Office* (PMO)**	The organisational structure that centralises all or part of the management and support of the organisation's projects, programmes, and project portfolios.
Human Resources Department (HR)	Human Resources Departments are divided into two main activities, on the one hand the administrative side of human resources management, which covers payroll, legal aspects, employment contracts, etc., and on the other hand human resources development, which includes career management, skills and performance management, recruitment and training.

Role	Description
Internal Control (IC)	In organisations where it exists, Internal Control is responsible for the introduction and management of an internal control system[9] that includes all the resources, behaviours, procedures and actions that contribute to the control of activities, the effectiveness of operations and the efficient use of resources. Internal control must take appropriate account of the significant operational, financial and compliance risks.
Compliance Officer	The Compliance Manager manages and oversees compliance with laws and regulations within the organisation. They provide an inventory of the applicable legal and regulatory requirements. They must ensure that the business and support staff are aware of these requirements so they can comply effectively. They report to the management, the regulator and the authorities. They answer questions asked by the regulator, for which they are the first point of contact.
Risk Manager	The Risk Manager helps the organisation to identify its risks. They support management and contribute to the cover and control of these risks. They provide businesses with the methodology to assess risks. They support the business units in the application of the methodology, collect information, validate and report to management. They do not assess the risk themselves.
Internal Audit (IA)	Independent and objective activity to provide assurance that risks are under control and to drive improvements in the organisation's operations.
EXTERNAL STAKEHOLDERS	
Data Protection Authority (DPA)	Supervisory authority, independent public authority responsible for monitoring the application of the GDPR, to protect the fundamental rights and freedoms of natural persons with regard to processing and to facilitate the free flow of personal data within the Union[10].
Data subject	Identified or identifiable natural person[11] to whom personal data relates
Processor (DP)[12]	The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Sub-processor	The Sub-processor which processes personal data on behalf of the Controller, but on the basis of a contract concluded with the Processor.

[9] The basic reference framework is the COSO framework (American internal control framework, broken down into five components). This role exists mainly in large multinational companies, the financial sector... rarely in SMEs.
[10] See Article 51 (1) of the GDPR
[11] See definition in Article 4 (a) of the GDPR
[12] See definition in Article 4 (8) of the GDPR

4. Lines of Defence model

In organisations with control structures, the three lines of defence model helps them to identify the optimal structures and processes to achieve their objectives and strengthen their governance and risk management systems, also with respect to personal data management.

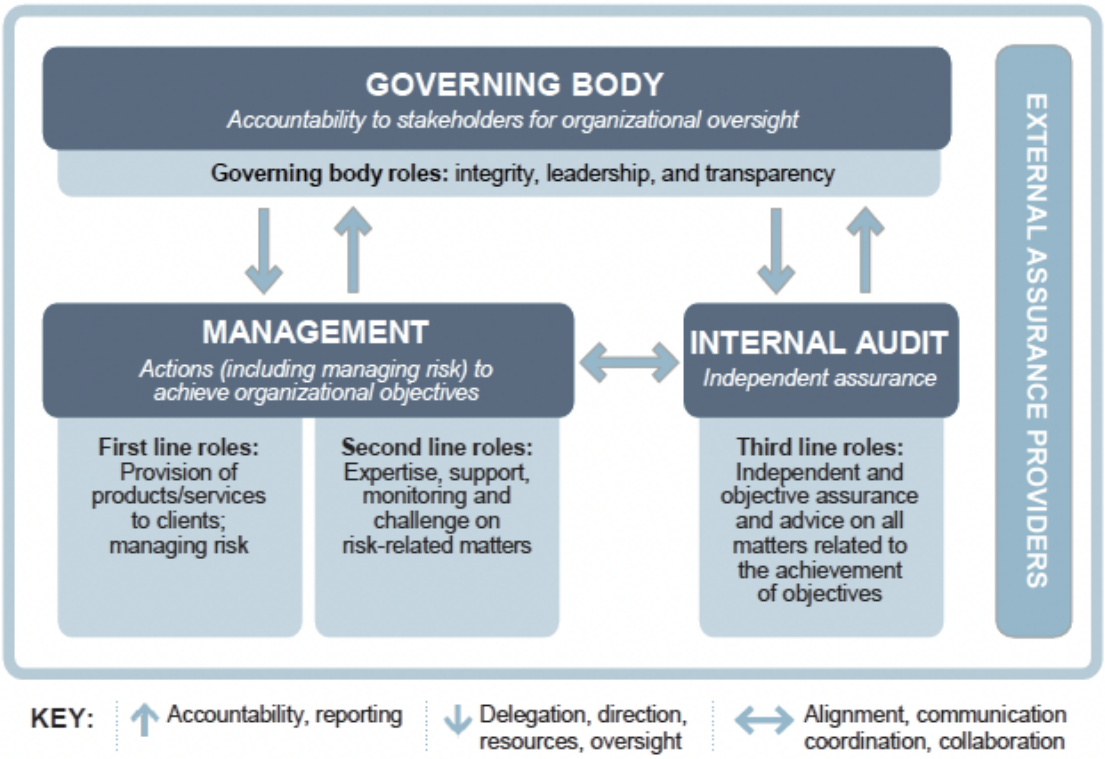


Diagram 1 - Three Lines of Defence model[13]

An organisation's governance must be based on appropriate structures and processes for managing personal data that enable governance bodies to fulfil their duty to be accountable; management to take the actions necessary to achieve objectives, through risk-based decision making and available resources; and an independent audit function.

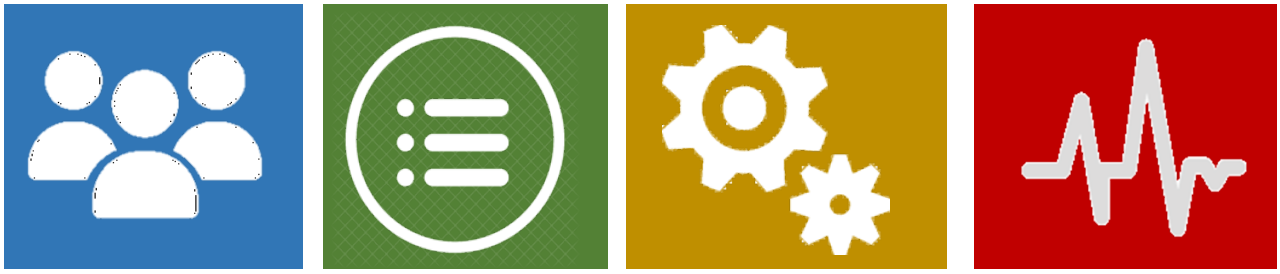
In particular, the approach defines specific tasks and responsibilities for each line of defence:

- control activities defined and implemented by operational staff, allowing, among other things, the control of risks on a day-to-day basis;
- a system structured and coordinated by the second line of defence, made up of functional departments responsible for areas of expertise, and functions dedicated to leading the overall risk control system (risk management, internal control and compliance positions, DPO, CISO[14], quality manager, etc.);
- a comprehensive, independent evaluation of the system by the third line, conducted by the independent internal audit function at the highest level of the organisation.

[13] Cf. *The IIA's Three Lines Model,* **The Institute of Internal Auditors,** 2020.
[14] Chief Information Security Officer (CISO)

5. GDPR processes

The implementation of a GDPR compliance programme involves the establishment of processes by all relevant stakeholders with the objective of ensuring a structured approach that covers the various GDPR requirements. These processes can be structured into four areas[15]:



A. Governance	B. Organisation	C. Operational management	D. Monitoring
Roles and responsibilities, steering bodies, policies and guidelines that enable adequate governance of personal data protection within the organisation.	Measures and processes to be implemented to meet the requirements of the GDPR.	Processes and procedures to be deployed to operationalise the protection of personal data in compliance with the GDPR.	Mechanisms for monitoring, tracking, reviewing and controlling the deployed system according to the requirements of the GDPR and its guidelines. Monitoring is intended to ensure that the system is working as intended and will verify that risk management is effective over time.

Table 2 - GDPR process areas

The four areas are broken down into 21 processes:

A. Governance

- A1. Commitments of the Controller (DC)
- A2. Data protection policies
- A3. Governance bodies, roles and responsibilities
- A4. Data Protection Officer (DPO)

B. Organisation of the system

- B1. Lawfulness of processing (legal basis & purpose)
- B2. Register of processing activities

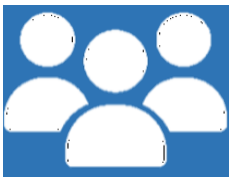
[15] The structure is based on that developed in the publication: *Controlling and Auditing GDPR Risks*, **IFACI GDPR Working Group**, 2021. Document available to IFACI members only.

B3. Data Protection Impact Assessment (DPIA)
B4. Data Protection by Design/Default
B5. Use and retention period of personal data
B6. Management of processing
B7. Transfers outside the European Economic Area (EEA)
C. Operational management
C1. Steering and implementation
C2. Rights of the data subject
C3. Information and transparency
C4. Awareness and training
C5. Business and Service Continuity Management (BCP)
C6. Management and notification of personal data breaches
C7. Protection and security of personal data
D. Monitoring and Review
D1. Monitoring and review of the system (by the DPO)
D2. Review of the GDPR system (by the stakeholders of the lines of defence)
D3. Monitoring by the Data Protection Authority (DPA)

Table 3 - Areas and processes

(Best) practices are proposed for each process, to comply with the requirements of the GDPR. Each practice will need to be broken down into a number of tasks required to perform them. These tasks are not included in this document. They will have to be defined according to the size and internal structure of the organisation, the importance of the processing of personal data, the sector of activity, etc.

A. Area of governance



The roles and responsibilities, governance bodies, policies and guidelines that enable the implementation of adequate governance of personal data protection within the organisation.

A1. Commitments of the Controller (DC)

The implementation of effective data protection governance starts with the governance bodies, including the board of directors and management.

Best practices and responsibility matrix:

Day-to-day management refers to the role that carries out (R) the practices.

Practices \ Roles	Controller (DC)	[D]PO
Determine the need for a DPO.	A	-
Appoint a Data Protection Officer (DPO) in compliance with the requirements of the GDPR (independence, absence of conflict of interest, etc.) or a Privacy Officer (PO)[16]	A	-
Allocate the necessary resources to enable the [D]PO to adequately carry out their GDPR compliance responsibilities	A	C/I
Appropriately position the [D]PO in organisational structures with access (and direct reporting) to the managing bodies and with the authority to exercise their responsibilities.	A	-
Formalise the missions entrusted to the [D]PO: mission letter, confidentiality commitment, budget, workload, protection against penalty for carrying out their missions, etc.	A	C/I
Put the subject of personal data protection on the agenda of the management bodies.	A	C/I
Inform the [D]PO of the topics discussed at governance committees, related to data protection.	A	I
Sign an agreement between the joint responsible parties in the event of joint responsibility for one or more processing operations.	A	C

[16] See the explanation of the difference between "DPO" and "PO" in Section 3 - Roles and Responsibilities, in which the term "Data Protection Officer" is defined

Deliverables

- Analysis of the appointment of a DPO
- Designation of the DPO by the governance bodies
- Statement to the DPA
- Description of the position of [D]PO
- Revised organisation chart (including DPO role)
- Contract with the external DPO or amendment to the employment contract of the internal DPO
- DPO budget
- Extracts from the minutes of the governing bodies and attachments, relating to the topics and processing of personal data
- Co-responsibility agreement(s)

A2. Data protection policies

Art. 24.2

Personal data protection and security governance will be established through appropriate policies approved by management and communicated through the organisational structures within the organisation.

Best practices and responsibility matrix:

Roles / Practices	Governing Body	Controller (DC)	[D]PO	CISO	HRD	Department processing PD
Adopt and implement an internal (general) data protection policy (or equivalent) that defines the organisation's governance in this area.	A	R	C	C	C	
Approve internal policy.	A/R	R	C	C	C	
Establish and implement policies for personal data protection, information systems security (ISSP) and data governance charters	-	A	C	R	R/I	
Publish and communicate policies to stakeholders	-	A	I	C	R/I	R/I
Integrate data protection into employment contracts and internal regulations.	-	A	C	-	R	I

Deliverables

- General personal data protection (governance) policy
- Information Security Systems Policy (ISSP) which reflects the vision of the Controller in terms of information systems security.
- Specific policies related to data protection and information security. The specific policies cover the correct use of IT resources, classification of information, authorisation policy, password management, use of the Internet, email and social media, etc.
- Data governance charter that describes data management responsibilities and practices to ensure data quality, integrity, availability and security.
- Communication plan for charters and policies
- Articles in the employment contract and/or internal regulations that include the obligation to comply with security and personal data protection policies

A3. Governance bodies, roles and responsibilities

Art. 24

Governance bodies "set the tone" in the organisation. They must be committed to data protection and emphasise its importance to all stakeholders who may interact with this data.

Establishing roles and responsibilities for personal data protection through clear channels of communication enables the deployment of appropriate practices at all levels of the organisation.

Best practices and responsibility matrix:

Roles / Practices	Day-to-day management	Controller (DC)	[D]PO	CISO	DSI/PMO	Internal Control	Internal Audit
Create responsibility matrices for the stakeholders involved in activities related to the protection and security of personal data.	R	A	C	C			
Integrate data protection into, for example, the: ○ governance and steering committees for information systems projects ○ data governance committees ○ recurring internal control activities ○ audit activities	-	A	C	 - R - -	 R R - -	 - - R -	 - - - R
Inform the governance bodies of the implementation of data protection compliance.	A	I	R	C	C	C	C/R

Deliverables

- Responsibility Matrix (RACI)
- Extracts from the minutes of the committees, including attachments, relating to the topics and processing of personal data
- Data protection compliance communications to the governance bodies

A4. Data Protection Officer (DPO)

Art. 37-39

Determining and establishing the [D]PO or a personal data protection "champion[17]" within the organisation, reporting regularly to the Controller.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	CISO	IT/PMO	Department processing PD	Internal Control Internal Audit	Data subject	DPA
Communicate the contact information of the DPO to the supervisory authorities.	A/R	I	-	-	-	-	-	I
Communicate the appointment of the DPO to stakeholders (both within and outside the organisation).	A/R	-	I	I	I	I	-	-
Potentially designate GDPR contacts[18]	-	C	I	I	R	I	-	-
Provide the [D]PO with access to all the information necessary for the performance of their function	A	I	R	R	R	R	-	-
Prepare an annual report for the governance bodies.	A	R	C	C		C	-	-
Inform the stakeholders processing personal data about GDPR requirements	I	A/R	I	I	I	I	-	-
Check compliance with the GDPR	C/I	A/R	C/I	C/I	C/I	C/I	-	-
Advise stakeholders on the protection of personal data	I	A/R	I	I	I	I	-	-
Cooperate with the Data Protection Authority and the contact point for data subjects	C/I	A/R	C/I	C/I	C/I	C/I	C/I	C/I

Deliverables

- Notification of the DPO to the DPA
- Inform (internal and external) stakeholders of the appointment of the DPO
- Annual report
- Opinion and advice from the DPO
- GDPR compliance monitoring programme (see also D.1)

[17] See the explanation of the difference between a DPO and a "PO" in Section 3 - Roles and Responsibilities.
[18] See the definition of this role in Section 3 - Roles and Responsibilities.

B. Organisational Area

Measures and processes to be implemented to meet the requirements of the GDPR.

B1. Lawfulness of processing (legal basis and purpose)

Art. 6

All personal data must be processed lawfully, fairly and transparently with respect to the data subject, and collected and processed for specified, explicit and legitimate purposes. Below are the practices related to lawfulness. Transparency is included in section C.3.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	CISO	IT/PMO	Department processing PD
Determine the legal bases (or grounds for lawfulness) and purposes of all personal data processing.	A	C			R
Collect consent in a GDPR compliant manner[19].	A	C	C/I	I/R	R
Organise the safeguarding of evidence of consent.	A	C	C/I	R	R
Document the legal obligation if that is the legal basis for the processing	A	C			R
Justify the public interest if this is the legal basis for the processing	A	C			R
Justify the legitimate interest if this is the legal basis for the processing (triple test[20])	A	C			R
Where necessary, adjust the processing operations to comply with the purposes and legal basis, and stop processing operations that do not comply or have no grounds for lawfulness.	A	C		I/R	R
Implement the principle of minimisation when collecting data (depending on the purpose of the processing). See also B.4.	A	C		I/R	R

Deliverables

- Inventory of processing operations, their purpose and the grounds for legality
- Procedure for obtaining and retaining evidence (and withdrawing consent)

[19] It will also be necessary to provide for the possibility of withdrawing consent at the request of the data subjects (see point C.2)
[20] Purpose, necessity and weighting tests

- Justification of legitimate interest (model)
- Justification of public interest (model) (if applicable)

B2. Register of processing activities

Art. 30

The personal data processing activities are recorded in a register.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	Department processing PD
Inventory the existing personal data processing	A	C	C	R
Create the "Controller" and/or "Processor" register	A	R	C	C
Determine and implement a procedure for updating the register(s)	A	R	I	I
Determine the need to include processing operations in the register (Art. 30.5 GDPR)	A	C	C	R
Determine the assignment of the processing operations to the "Controller" or "Processor" register.	A	C	C	R
Organise the training and possible support of GDPR Contacts[21].	A	R	I	
Collect all the information required for the register	A	C	R/C	R
Implement a procedure for the regular review of the register	A	C	C	R

Deliverables

- Inventory of data processing and all the information regarding it
- Register of the Controller with the information required by Article 30 of the GDPR - updated
- Register of the Processor, where necessary, with the information required by Article 30 of the GDPR - updated
- Procedure for updating the register(s)
- Training of DPO Contacts to help complete the register

[21] The Contacts must be able to advise departments on the identification of processing operations and assist in the collection of the information required in the register

B3. Data Protection Impact Assessment (DPIA)

Art. 35

Ensure that impact assessments are carried out for proposed processing operations that are likely to present a high risk to the rights and freedoms of data subjects, to mitigate the risks of infringing these rights and freedoms.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	Department processing PD	Project Manager[22]	DPA
Determine which processing operations are eligible for a DPIA, based on Article 35 of the GDPR and in particular by applying the criteria laid down by the EDPB[23] and the relevant supervisory authorities (such as the DPA).	A	C/R	R	C	R/C	C	
Determine and implement a methodology for conducting DPIAs	A	R/C	C	R/C			
Possibly select and implement a tool for conducting DPIAs	A/R	C					
Create the schedule for the completion of the DPIAs	A	C/R	C	C	R	C	
Conduct the DPIA[24] and write the report	A	C	C	C	R/C	C/I	
Identify measures to mitigate risks and establish an action plan, if necessary	A	C	I	R	R	R	
Implement and monitor the action plan	A	I	I	R	R	R	
Consult the DPA if there is a high residual risk	A	R					C

Deliverables

- List of processing operations eligible for a DPIA
- DPIA methodology
- DPIA tool, possibly
- Schedule for the completion of the DPIAs
- DPIA, containing the following elements for each analysis performed: presentation of the processing operation(s) considered, list of measures implemented, risk assessment and mapping, reasoned decision, and possibly the action plan
- Action plan and follow-up: measures, responsible persons, deadlines
- DPA opinion, if consulting for high residual risk

[22] As part of a new project.
[23] European Data Protection Board
[24] For a more detailed review of the DPIA steps, see The CNIL's DPIA Guides, 2018, https://www.cnil.fr/fr/guides-aipd (accessed 3 June 2022)

B4. Protection by Design and Default (*Data Protection by Design/Default*)

Art. 25

Ensure that, when personal data processing activities are created, appropriate technical and organisational measures are taken or considered to adequately protect and minimise personal data.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	IT/PMO	Department processing PD	Project Managers	Steering Committee
Define a "Data Protection by Design/Default" procedure/methodology for compliance with the principles of the GDPR by design and by default (including the principle of minimisation, for example)	A	C	C	C	C	R	C	I
Integrate the procedure into the project management methodology	A	I	I	I	R	I	I	I
Train project leaders and key players in the methodology	A	C/I	C/I	I	R	I	I	I
Implement the methodology in projects that process personal data	A	I	I	C	C	C/R	R	I
Review the results of the "Data Protection by Design/Default" analyses[25]	A	I	I	I	I	I	I	R
Determine the actions to be implemented	A	I/C	I/C	R	I	R	R	C/I
Implement and monitor the action plan	A	I	I	R	I	R	R	I

Deliverables

- Data protection by Design/Default" management procedure/methodology
- Training material on the "Data Protection by Design/Default" management approach and procedure, possibly integrated into the project management methodology training material
- Minutes of the meetings with the DPO on the results of the "Data Protection by Design/Default" analyses
- Action plan of the measures to be implemented, by project
- Monitoring of the action plans: measures, responsible persons, deadlines

[25] When a new solution is designed, best practice is to consult the DPO on the correct application of the DPbD/DPbDf principles. In general, a meeting is scheduled with the designers (e.g. IT, the PMO) and the DPO so that they can take note of the analysis carried out in the framework of the project.

B5. Use and retention period of personal data

Art. 5.2 e)

Personal data must be used for the purpose for which it was collected and not further processed in a way that is incompatible with that purpose. It may not be kept in a form that allows the identification of data subjects for a period longer than is necessary for the purposes for which it is processed, unless there is additional justification.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	IT/PMO	Department processing PD
Inventory the (categories of) personal data processed by the organisation - organised by purpose of processing (from the register)	A	C	C	C	R
Determine the data retention periods according to need[26] (fixed duration or dependent on the achievement of a factor)	A	C	C	I	R
Determine what happens to the data after the defined retention period[27]					
Implement the retention periods set (in the computer systems, in the systems for retaining paper documents, in the organisation of data access)	A	C	C	R/C	R
Provide instructions to Processors on how to implement retention periods	A	C	C	R/C	R
Place the retention period information in the register (or refer to this information in the register)	A	C	C		R

Deliverables

- Document(s) listing the data retention periods according to the purposes and the computer systems in which this data is stored
- Implementation instructions for Processors

[26] In accordance with the principle of minimisation
[27] Deletion or retention for another (lawful) purpose

B6. Management of processing

Art. 28

The activities of the Processors and the Sub-processors will be carried out on behalf of the Controller and the responsibilities and obligations will be defined in a processing contract in accordance with Article 28 of the GDPR.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	IT/PMO	Department processing PD	Legal department
Create a model processing contract including the clauses of Article 28 of the GDPR (or use the European model) -	A	C/R					R
Include in the Special Specifications model the provisions relating to the GDPR (only valid for entities subject to public procurement regulations)	A	C/R					R
Inventory the Processors (DP) and identify the processing operations in which these Processors are involved	A	C	C/R			R	
Inventory the contracts with the DPs and the clauses related to the GDPR included in these contracts	A	C	C/R			R	C/R
Determine the security measures to be imposed on DPs according to the nature of the data they process on behalf of the DC, the risks, etc.	A	C		R		(R)	
Ensure the guarantees[28] that the DP offers to comply with the GDPR in the context of the processing in which it is involved, the data it processes on behalf of the DC and the risk to the rights and freedoms of the data subject	A	C	C/R	C		R	
Conclude processing agreements	A	C	C			R	C
Put in place a procedure for verifying and monitoring compliance with the DP's commitments ("sufficient guarantees"), (audit programme)	A	C					
Identify where data is processed by the processor or from where the data can be accessed (identification of transfers to third countries - see B.7)	A	C	C/R			R	
Include the DP in the register ("recipients")	A	C	C/R			R	

[28] The controller "shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." Article 28.1 GDPR.

Deliverables

- Model processing agreement Article 28 GDPR *(Data Processing Agreement)*
- List of technical and organisational security measures that could be imposed on DPs depending on the circumstances (nature of the data, risks, state of the art, costs)
- DP Inventory
- Inventory of contracts with the DPs and data protection clauses included in these contracts
- Inventory of transfers to "third countries" (see B.7)
- DP audit programme

B7. Transfers outside the **European Economic Area (EEA)**[29]

Chap V

Any transfer of personal data to a third country outside the EEA or to an international organisation must comply with the safeguards set out in the GDPR.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	IT/PMO	Department processing PD
Identify transfers of personal data to "third countries" (outside the European Economic Area) - see B.6	A	C	C/R			R
Determine if the data was sent to a DP or a DC	A	C/R	C/R			C
Determine the guarantee that allows the transfer (countries offering adequate protection[30], appropriate guarantees that do not require authorisation from the supervisory authority (standard contractual clauses and additional protection measures; Binding Corporate Rules, etc.)[31], appropriate guarantees that require authorisation from the supervisory authority (specific clauses, etc.)[32], derogations for specific situations[33], or compelling legitimate reasons[34]	A		C/R			R
When using Standard Contractual Clauses • Conduct a transfer impact assessment (DTIA)[35] and adopt additional protective measures based on the result • Check if the new June 2021 model clauses are being used[36] or if the old clauses are still in use • Use the new Standard Contractual Clauses for all new contracts from 27 September 2021[37] • When using the new Clauses, determine the module to be used according to the type of transfer (transfer between a DC and a DP, between DCs, between DPs, or between a DP and an DC)	A	C	C/R	C		R C R

Deliverables

[29] The data protection rules apply to the European Economic Area, which, in addition to the countries of the European Union, includes Iceland, Liechtenstein and Norway. Cf: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en
[30] Article 45 GDPR
[31] Article 46.2 GDPR
[32] Article 46.3 GDPR
[33] Article 49 GDPR
[34] Article 49.1§2 GDPR
[35] TIA or DTIA - (data) transfer impact assessment
[36] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en (accessed 3 June 2022)
[37] The old clauses must be replaced by the new Standard Contractual Clauses before 27 December 2022

- List of transfers to third countries and the guarantees used
- Inventory of contracts where the old standard contractual clauses are still being used
- DTIA model
- DTIA when using standard contractual clauses for the transfer

C. Operational Management Area

Processes and procedures to be deployed to operationalise the protection of personal data in compliance with the GDPR.

C1. Steering and implementation

Art. 24

Setting up a management team with the resources and skills necessary to guarantee the operational implementation of the GDPR system.

Best practices and responsibility matrix:

Practices \ Roles	Controller (DC)	[D]PO	[D]PO Contact	CISO	IT/PMO	Department processing PD
Establish a GDPR compliance programme	A	R/S[38]	C/I	C/I	R	C/I
Designate the programme management team	A/R	I	I	I	I	I
Prioritise and plan the compliance activities	A	R/S[39]	C/I	C/I	R	C/I
Lead the network of GDPR Contacts for the deployment of the compliance system	A	R	C	C	R	
Organise internal processes to ensure that data protection is taken into account	A	C/S	C	C	R/C	R
Manage the risks related to the processing of personal data	A	C/S	C	C	C	R
Determine the indicators and dashboards for monitoring compliance with the GDPR	A	R/S	C/I	C/I	R	C/I

Deliverables

- GDPR compliance programme
- GDPR programme documentation: objective, resources, budget, deadline, risks, follow-up
- Minutes of the steering meetings
- Descriptions and updates of processes and procedures
- Risk register
- Monitoring indicators
- Implementation monitoring dashboard

[38] The CNIL refers to the DPO as a pilot/conductor (https://www.cnil.fr/fr/principes-cles/GDPR-se-preparer-en-6-etapes - accessed 3 June 2022)
[39] Idem

C2. Rights of the data subject

Art. 12-23

The Controller must implement processes and procedures to allow the exercise of the rights of access, rectification, deletion, opposition, and restriction of processing and to ensure the portability of the data subject's personal data.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	IT/PMO	Department processing PD
Determine the applicable rights (according to the legal bases)	A	C			R
Create a directory for recording requests	A	R	C/R		C/R
Define and implement procedures to respond to the exercise of each right, depending on the category of data subjects [40]	A	S/C	C	C	R
Determine the measures to be put in place for the authentication of applicants	A	S/C	C		R
Inventory the systems in which personal data is collected and determine how the request can be met in each system	A	S/C	C	R/C	R/C
In the event of a request for data deletion, determine the procedure for verifying that the data can indeed be deleted and then delete if necessary.	A	S/C	C	R/C	R/C
Train the staff who respond to requests to exercise rights (front office, support service, etc.)	A	S/C	C		R
Establish the procedure for handling a complaint	A	S/C	C		R
Produce key indicators and/or reports on the analysis and monitoring of requests	A	R	C/I		C/I

[40] Where appropriate, implementation of a self-management portal for data subjects.

Deliverables

- Procedure for managing each applicable right for each category of data subject (customers/citizens/patients/employees/suppliers)
  - Access (including disclosure of information and copying of data)
  - Rectification
  - Deletion
  - Right to be forgotten
  - Restriction of processing
  - Portability
  - Opposition
  - Withdrawal of consent
  - Automated individual decision
- Procedure for authenticating the person requesting the exercise of their rights
- Inventory of the systems with modalities for carrying out the requests
- Complaint management procedure
- Staff training materials
- Monitoring indicators and reports

C3. Information and transparency

Art. 12-14

Appropriate measures should be implemented to provide data subjects with the required information on the processing of their personal data.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	HRD	Department processing PD
Determine the categories of data subjects to be informed	A	C	C	R	R
Determine the appropriate collection and communication channels with the data subjects (website, intranet, internal charter, annex to the work contract, work regulations, etc.)	A	C	C	R	R
Identify the processing operations concerning each category of data subject (to be taken from the register)	A	C	C	R	R
Include the data retention period in the information given to the data subject	A	C	C	R	R
Develop a "confidentiality statement" or "privacy charter" that includes the information in Articles 13 and 14 of the GDPR	A	C	C	R	R/I
Publish and communicate charters to stakeholders	A	C	C	R	R/I
In the event of direct collection, inform data subjects of the processing operations at the time of collection (see information to be communicated in Article 13 of the GDPR).	A	C			
In the event of indirect collection, inform the data subject as soon as possible, and at the latest at the time of the first communication, but always within one month (see the information to be communicated in Article 14 of the GDPR)	A	C			

Deliverables

- "Confidentiality Statement" or "Personal Data Protection Charter", published on the website
- List of channels for collection and communication with the data subject
- List of processing operations by data subject
- Internal information (for employees and internal collaborators)

C4. Awareness and training

Art. 24

Organisation of regular awareness-raising and training activities for (internal and external) employees concerning the understanding of processing, risks, data protection measures and the rights of data subjects.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	IT/PMO	HR	Department processing PD
Determine the categories of target audience and define by category: the need for awareness or training in this area	A	R/S	C	C	C	R/C	R/C
Prepare awareness and training sessions	A	R/S	C	R	C	R	C
Organise training by category of target audience	A	R/S	R	I	(R)	I	R
Keep evidence of awareness and training sessions, and a list of those who have attended them	A	R/S	R		C	C	C
Update or repeat awareness/training and retain evidence	A	R/S	C	R	C	R	C
Conduct regular tests or quizzes to verify knowledge	A	R/S	C	C		C	I

Deliverables

- Awareness and training needs matrix - by target audience
- Awareness materials (GDPR and security)
- Training materials (GDPR and security)
- Evidence of training
- Evidence of raising awareness of target audiences
- Evidence of updating and ongoing training/awareness
- Knowledge test results

C5. Business and Service Continuity Management (BCP)

Art. 32

Appropriate measures will be put in place to ensure the continuity of personal data activities with regard to data subjects.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	Business Continuity Manager[41]	Department processing PD
Identify the need for continuity in the processing of PD, in particular by establishing a Business Impact Analysis (BIA)	A	C/I	C	C	R	C
Assess the risks in terms of continuity and establishing maximum service interruptions (RTO) and maximum personal data loss (RPO)	A	C/I	C	C	R	C
Integrate DP continuity and restoration actions into the Business Continuity Plan (BCP)	A	C/I	C	C	R	C
Provide training on the Business Continuity Plan	A	I	I	C	R	I
Develop and test the Business Continuity Plan	A	C/I	C	R	R	R
Review and improve the Business Continuity Plan	A	C/I	C	C	R	C
Manage the backup devices	A	C/I	C	C	R	C
In the event of restoration, perform a post-recovery examination.	A	C/I	C	C	R	C

[41] **The role of Business Continuity Manager is often combined with that of CISO.**

Deliverables

- Business Impact Analysis
- Continuity risk assessment including RTO and RPO
- Business Continuity Plan (BCP)
- BCP training plan
- Notes on the Business Continuity Plan test
- Action to improve the Business Continuity Plan
- Backup plan
- Post-recovery examination report

C6. Management and notification of personal data breaches

Art. 33-34

Measures will be put in place to ensure effective management of personal data breaches.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	Incident Manager[42]	CISO	Department processing PD
Determine and implement a procedure for managing personal data breaches (from the detection, reporting and identification of the breach, to taking measures to limit the consequences and impact, possible notification to the Data Protection Authority and/or to the data subjects, analysis of the causes to try to avoid any further occurrence, and management evaluation)	A	R/S	C	C/I	C/I	C/I
Create and implement (and update) an internal breach register	A	R/S	C	R	R/C	C
Implement incident detection mechanisms through monitoring and reporting [43]	A			R		
In the event of a suspected breach: • gather relevant information • analyse to verify the occurrence of a breach and qualify it (involvement of personal data, severity, extent) • document the incident • determine the responses (measures)	A	C	C	R	C	C
In the event of a breach: • determine the need to notify the DPA and potentially the data subjects • notify the DPA if necessary • notify the data subjects if necessary	A	R C C	C	C R R	C	I (R) R
Ensure that breaches are reported by the DC within the required timeframe for notification	A	R				
Learn from incidents and breaches for continuous improvement	A	R/C	C	R	R	C

[42] The role of incident manager can be assigned to the CISO, an IT expert or a dedicated position depending on the size and structure of the organisation.

[43] Identification must be integrated into the organisation's incident management processes.

Deliverables

- Internal register of breaches
- Method of assessing the risk to data subjects in the event of a personal data breach
- Sample questionnaire for obtaining all the necessary information in the event of a (suspected) data breach
- Sample incident (breach) management report including the actions taken to mitigate the consequences of the incident (and future occurrences).
- Notification to the DPA and/or the data subject

C7. Protection and security of personal data

Art. 32

Appropriate organisational and technical measures will be put in place to protect the personal data of data subjects in an appropriate manner.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	IT/PMO	Department processing PD
Integrate personal data protection measures into the Information Security Management System (ISMS)	A	C	C	R	C	C
Identify the appropriate organisational and technical measures by data processing operation[44]	A	C	C	R	C	C
Establish protection and security measures, including data loss prevention and cyber protection measures	A	C	C	R	C	I
Establish security procedures	A	C	C	R	C	C
Communicate and raise awareness of protection and security measures	A	C/R	R	R	I	I
Implement the traceability of access/modifications/other processing of PD	A	C	C	R	R	I
Monitor the implementation of protection and security measures	A	R	R	R	C	C
Review the protection and security measures	A	C/I	C	R	C	C

Deliverables

- Information Security Management System (ISMS)
- Organisational and technical protection measures by PD processing operation, e.g. housing, data transmission.
- Communication of personal data protection and security measures
- Activity tracking analysis.
- Report of the review of personal data protection and security measures

[44] To be defined taking into account the nature of the data, the risks to rights and freedoms, the costs of implementation, the state of knowledge, the context and the purposes of the processing - Article 32 of the GDPR.

D. Monitoring area and review

Mechanisms for monitoring, tracking, reviewing and controlling the deployed system to meet the requirements of the GDPR and the guidelines adopted on this issue.

Monitoring is intended to ensure that the system is working as intended and will verify that risk management is effective over time.

D1. Monitoring and review of the system (by the DPO)

Art. 39.1

The DPO continuously monitors compliance with the GDPR within the organisation. They organise regular reviews to ensure long-term compliance.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	IT/PMO/ Dep. processing PD	Internal Control[45]	Risk Manager[46]	Compliance Officer[47]	Internal Audit
Conduct regular, planned reviews of the conceptual consistency[48] of GDPR compliance practices	A	R	R	C	C	C	C	C	I
Conduct regular, planned reviews of the (*operational consistency*[49]) GDPR compliance practices (first level controls - operations)[50]	A	R	R	C	C	-	-	-	I
Conduct regular, planned reviews of the activities supporting the implementation of the GDPR (second line of defence)[51]	A	R	R	C	-	C	C	C	I
Determine action and improvement plans	A	R	C	C/I	C/I	C/I	C/I	C/I	I
Report the findings of the reviews to the Controller	A/I	R	C	I	-	I	I	I	I

[45] **See the definition of the Internal Control role in Section 3 - Roles and Responsibilities**
[46] **See the definition of the Risk Manager role in Section 3 - Roles and Responsibilities.**
[47] **See the definition of the Compliance Officer role in Section 3 - Roles and Responsibilities.**
[48] *Conceptual consistency* involves ensuring that practices have been designed in a way that complies with the requirements of the GDPR.
[49] *Operational consistency* consists of ensuring that practices are implemented in a way that complies with the requirements of the GDPR, and that the control measures are functioning in a way that allows for risk control.
[50] See Figure 1 in Section 4 - 3 Lines of Defence Model
[51] See Figure 1 in Section 4 - 3 Lines of Defence Model

Deliverables

- Review documents for design and review effectiveness
- Action and improvement plans for GDPR practices
- Summary report of the reviews for the Controller

D2. Review of the GDPR system (by the stakeholders of the lines of defence other than the DI

Art. 24

Appropriate control activities by the various stakeholders in the second line of defence should be planned to ensure compliance with the GDPR.

The audit provides reasonable assurance of GDPR compliance by assessing the first and second line of defence activities. This third line defence aims to mitigate risks.

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	Audit Committee	[D]PO/[D]PO Contact	CISO	IT/PMO/ Dep. processing PD	Internal Control	Risk Manager	Compliance Officer	Internal Audit
Conduct regular, planned reviews of the GDPR control measures (first level defence - operations)	A		C	C	C	R		I	I
Integrate the GDPR risk assessment into the organisation's risk management	A		C	C	C	C	R	I	I
Determine the defence measures improvement plan	A		C	C/I	C/I	R	I	I	I
Monitor the action plans (by Internal Control)	A		C/I	C/I	C/I	R	C/I	C/I	I
Develop the audit programme of the GDPR compliance system, including for DPs	C	A	C	C	C	C	C	C	R
Perform the GDPR compliance audit	C	A	C	C	C	C	C	C	R
Determine the action plan	I	A/I	R/I	R/I	R/I	R/I	R/I	R/I	S
Monitor the action plan	I	A/I	C/I	C/I	C/I	C/I	C/I	C/I	R
Write the audit report and present the conclusions	I	A/I	I	I	I	I	I	I	R
Monitor the action plans (following the audit)	I	A/I	C/I	C/I	C/I	C/I	C/I	C/I	R

Deliverables

- Conceptual and operational effectiveness review reports (by Internal Control)
- Management of risks related to the protection of personal data
- Control measures improvement plan
- Audit report
- Action plan (following the audit)
- Follow-up report on the implementation of the action plans

D3. Monitoring by the Data Protection Authority

Appropriate measures should be taken to anticipate and enable monitoring and inspections by the Data Protection Authority. This includes the preparation of documentation and evidence of compliance with the GDPR (document management) in accordance with the principle of accountability[52]

Best practices and responsibility matrix:

Roles / Practices	Controller (DC)	[D]PO	[D]PO Contact	CISO	IT/PMO/Dep. processing PD	Internal Control\Risk Manager\Compliance Manager	Internal Audit
Identify potential controls and inspections by the authorities	A	R					
Establish a repository/document management for registers, procedures, contracts, reports, notices and other documents that demonstrate the Controller's compliance with the principles and obligations of the GDPR	A	R/C	C/I	R/C/I	R/C/I	C/I	I
Establish the procedure for on-site inspections by the DPA	A	R	C/I	C/I	C/I	C/I	I
Establish the procedure for responding to a written request from the Data Protection Authority	A	R					
Designation of contact points and site managers	A	R	C/I	C/I	C/I	C/I	I
Define the conduct of employees	A	R	C/I	C/I	C/I	C/I	I
Clarify the roles of the DPO, site managers, and key contacts	A	R	C/I	C/I	C/I	C/I	I
Train people to receive and follow up on a control by the Data Protection Authority	A	R	I	I	I	I	I

[52] Article 5.2 of the GDPR

Deliverables

- List of controls (what the authority could control) and potential inspections
- Directory/Records management of documents and registers
- On-site control procedure
- Procedure for responding to a written request from the Data Protection Authority
- List of contact points and site managers
- Code of conduct for employees
- Roles of the DPO, site managers, and key contacts
- Training material relating to controls by the Data Protection Authority

Appendix 1 - Glossary

The table below lists the acronyms used, together with their meaning in French and English.

Acronym	French term	English term
AI	Audit Interne	Internal Audit (IA)
AIPD	Analyse d'impact relative à la protection des données	Data Protection Impact Analysis (DPIA)
APD	Autorité de Protection des Données	Data Protection Authority (DPA)
BIA	Bilan d'Impact sur l'Activité	Business Impact Analysis
CEPD	Comité Européen à la Protection des Données	European Data Protection Board (EDPB)
CI	Contrôle Interne	Internal Control (IC)
DPbD	Protection des données dès la conception	Data Protection by Design
DPbDf	Protection des données par défaut	Data Protection by Default
DCP	Données à Caractère Personnel	Personal data (PD)
DPO	Délégué à la Protection des Données (DPD)	Data Protection Officer
DRH	Direction des Ressources Humaines	Human Resources department (HR)
(D)TIA	Analyse d'Impact du Transfert des Données	(Data) Transfer Impact Assessment
IT	Direction informatique	Information Technology department
EEE	Espace Économique Européen	European Economic Area (EEA)
PCA	Plan de Continuité d'Activité	Business Continuity Plan (BCP)
PMO	Bureau Projet	Project Management Office
PO	Privacy Officer	Privacy Officer
PSSI	Politique de Sécurité des Systèmes d'Information	Information Security Systems Policy (ISSP)
RACI	Matrice de responsabilités : Réalise, Approuve et assume, Consulté, Informé	Responsibility Matrix: Responsible, Accountable, Consulted, Informed
RGPD	Règlement Général sur la Protection des Données	General Data Protection Regulation (GDPR)
RPO	Perte de Données Maximale Admissible (PDMA)	Recovery Point Objective

Acronym	French term	English term
RSSI	Responsable de la Sécurité des Systèmes d'Information (conseiller en sécurité)	Chief Information Security Officer (CISO)
RT	Responsable du Traitement	Controller (DC)
RTO	Durée Maximale d'Interruption Acceptable (DMIA)	Recovery Time Objective
SGSI	Système de Gestion de la Sécurité de l'Information	Information Security Management System (ISMS)
SSC	Clauses contractuelles types	Standard Contractual Clauses
ST	Sous-Traitant	Processor