Luxgap
DATA PRIVACY PARTNER

The Role of the Data Protection Officer (DPO)

Legal Framework, Missions, Deliverables, and Continuous Compliance Management

Version 27/02/2026 — Operational reference document for executives, business units, IT & security.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116

NAVIGATION

Summary

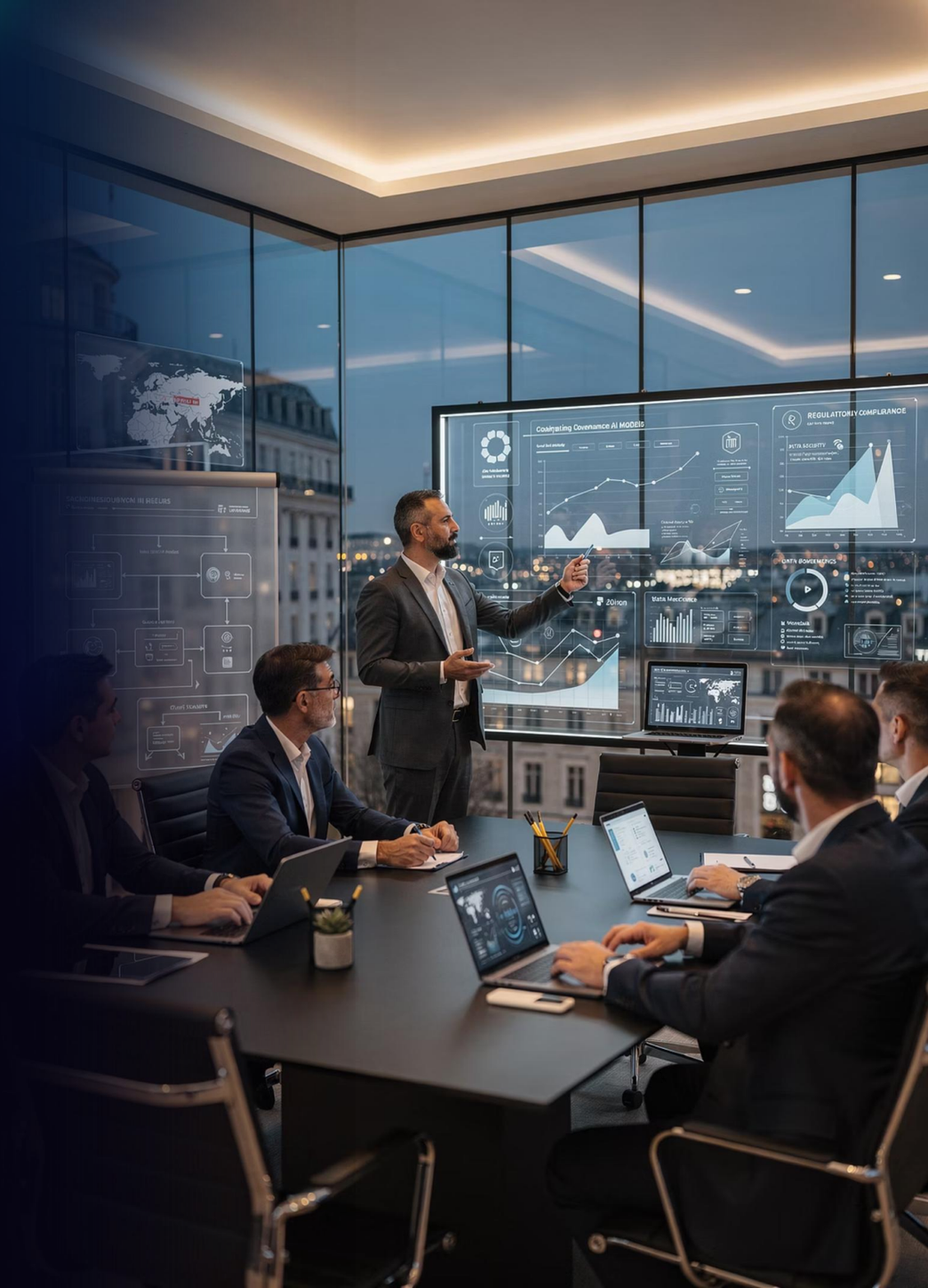
This document complements and structures the GDPR compliance roadmap (9 axes) presented in our proposed approach.

CHAPTER 1

The DPO in practice

The DPO (Data Protection Officer) is the internal or external body responsible for **orchestrating GDPR compliance**, advising and monitoring the system, without substituting for the data controller (principle of accountability — Art. 5(2) and 24 GDPR).

Key point: the DPO is not the legal "controller" of compliance. They advise, alert, document, monitor, and facilitate decision-making. The decision (purposes, means, trade-offs) remains the responsibility of management and business units.



What the DPO concretely brings

Mapping of processing activities

A reliable mapping of processing activities and data flows, aligned with purposes and legal bases (Art. 6, 9, 10 and 30). The DPO identifies each processing activity, its recipients, its flows and its legal grounds to offer a complete vision of the data assets.

Documented rules & evidence

Operational rules and documented evidence (policies, procedures, registers) to demonstrate compliance (Art. 5(2) and 24). This body of documentation forms the basis of the accountability required by the GDPR.

Privacy risk management

A "privacy" risk management mechanism focused on individuals (DPIA — Art. 35) and security (technical and organizational measures — Art. 32). The risk-based approach allows prioritizing efforts where the impact is highest.

Continuous monitoring

Reviews, audits, indicators, change management (privacy by design — Art. 25) and coordination in case of incidents (Art. 33-34). The DPO ensures permanent monitoring and adapts the system to organizational changes.

Single point of contact

A single, competent point of contact for the supervisory authority and data subjects (Art. 38(4) and 39(1)(d)-(e)). The DPO centralizes exchanges and ensures the organization's responsiveness.

Internal DPO vs External DPO

The choice between an internal DPO and an external DPO depends on the organization's size, maturity, and resources. Each option has specific advantages and constraints.

1

🏢 Internal DPO

Advantages: in-depth knowledge of the organization, proximity to business lines, immediate availability.

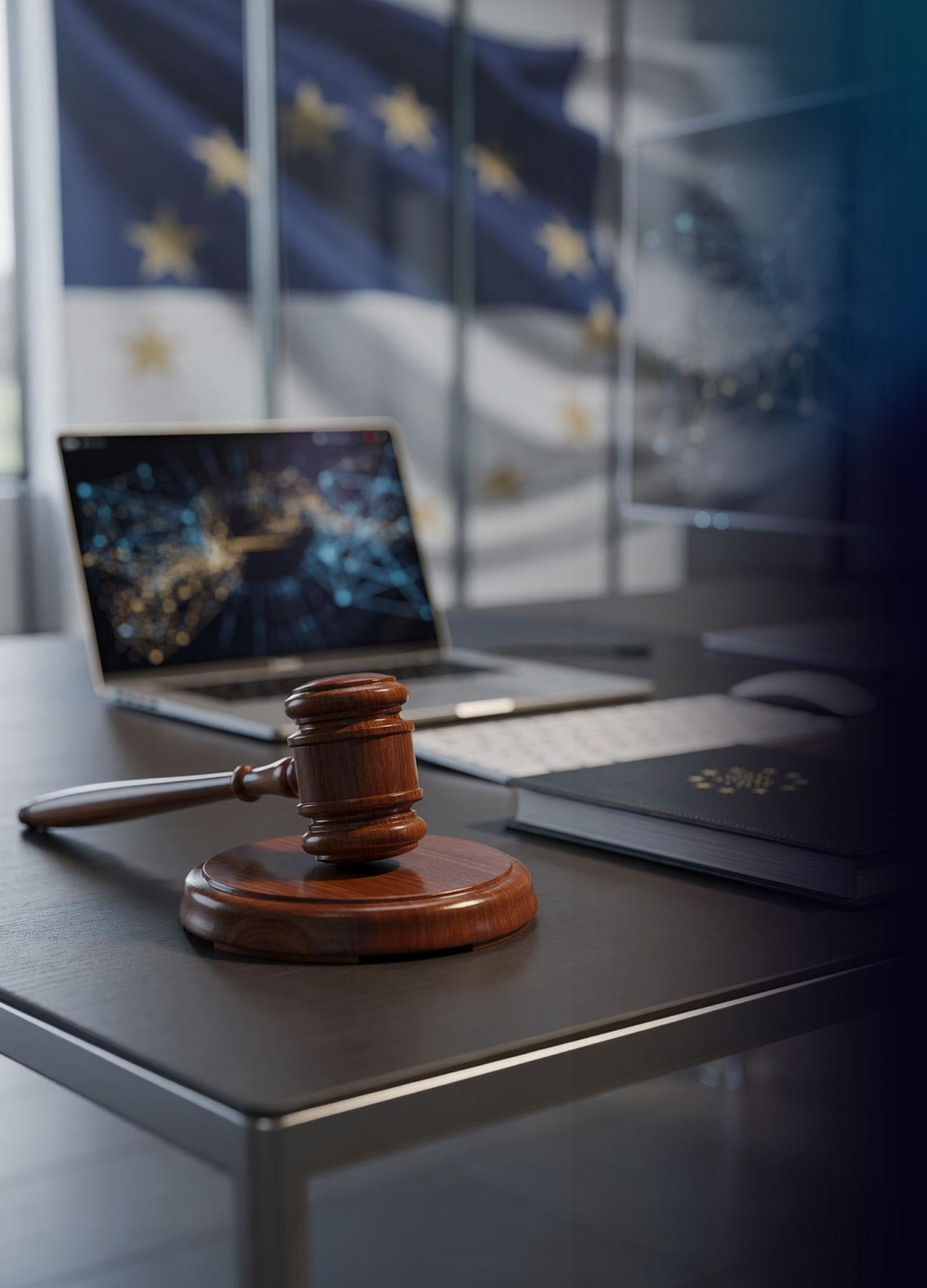
Constraints: requires effective independence, dedicated resources, and absence of conflicts of interest (Art. 38). The internal DPO cannot hold a position that determines the purposes and means of processing.

2

🌐 External DPO

Advantages: pooling of expertise (legal, security, business), faster maturity growth, intervention and audit capability, objective external perspective.

Constraints: requires clear governance and access to information (Art. 38(2)). The contract must precisely define the scope, reporting methods, and escalation rules.



CHAPTER 2

When and how to appoint a DPO

The appointment of a DPO is **mandatory** in the cases listed in Article 37(1) GDPR:

Public Authorities

Public authorities or bodies (except for courts acting in their judicial capacity)

Large-scale monitoring

Core activities involving regular and systematic monitoring of individuals on a large scale

Sensitive data

Core activities involving large-scale processing of sensitive data (Art. 9) or data relating to criminal convictions and offenses (Art. 10)

Practical Decision Grid

To determine if the designation of a DPO is mandatory, four criteria must be analyzed on a case-by-case basis:

1

Core Activities

Is the processing inseparable from the main mission? Examples: online platform, centralized HR, health, insurance, fintech, telematics, data-driven marketing. If the processing is ancillary, the criterion is not met.

2

Regular and Systematic Monitoring

Profiling, scoring, geolocation, tracking, surveillance (online/offline), continuous monitoring (e.g., IoT, apps, smart CCTV). "Regular" implies recurrence; "systematic" implies an organized system.

3

Large Scale

Volume of individuals, volume of data, duration, geographical extent. The assessment is made on a case-by-case basis by combining these factors. A single doctor does not process on a large scale; a hospital network does.

4

Sensitive / Criminal Data

Special categories (health, biometrics, political opinions, sexual orientation, etc.) or criminal data processed in the core activity. The combination with the large-scale criterion triggers the obligation.

Even without a strict obligation, designating a DPO (or an equivalent function) is a **good governance practice** and facilitates the demonstration of compliance, especially for exposed organizations (B2B clients, tenders, audits, cybersecurity).

Formalities and designation deliverables

The DPO's designation must be formalized and communicated. Three essential deliverables structure this step:

📋 Act of Designation

Letter or mandate specifying the scope of intervention, hierarchical reporting, allocated resources, and escalation rules (Art. 37(5) and 38(2)). This document formalizes the organization's commitment and the means made available to the DPO.

📢 Publication of Contact Details

The DPO's contact details must be published (website, information notices, email signature, etc.) and communicated to the supervisory authority (Art. 37(7)). This publicity ensures the DPO's accessibility for data subjects and the authority.

📄 DPO Charter (recommended)

Document defining rules of independence, access to information, conflict of interest management, confidentiality, and reporting procedures (Art. 38). The charter constitutes the reference framework for the DPO function within the organization.

CHAPTER 3

Guarantees of Independence and Governance

The effectiveness of the DPO relies on **formal guarantees**: absence of instructions regarding the exercise of duties, absence of sanctions related to these duties, direct access to the highest level of management, sufficient resources, and prevention of conflicts of interest (Art. 38 GDPR).

Non-negotiable Requirements (Art. 38)

Independence

The DPO informs and advises, but does not receive instructions on how to perform their duties (Art. 38(3))

Reporting Line

The DPO reports directly to management (Art. 38(3))

Resources

Time, budget, tools, access to systems and stakeholders (Art. 38(2))

Early Involvement

Involvement from the design stage of projects/processing operations (privacy by design — Art. 25 and Art. 38(1))

Confidentiality

Secrecy or confidentiality regarding the performance of duties according to EU/national law (Art. 38(5))

Conflict of Interest Management

The DPO **cannot** be placed in a position that determines the purposes and means of processing. The following functions are incompatible with the DPO role:

- General Management
- IT Management
- HR Management
- Marketing/Sales Management
- Security Management (if it arbitrates purposes/means)

A **documented conflict of interest analysis** is recommended, especially in cases of dual roles.

Recommended Deliverable: matrix of incompatible roles + conflict resolution procedure (declaration, arbitration, compensatory measures).

Typical Governance

Privacy Committee

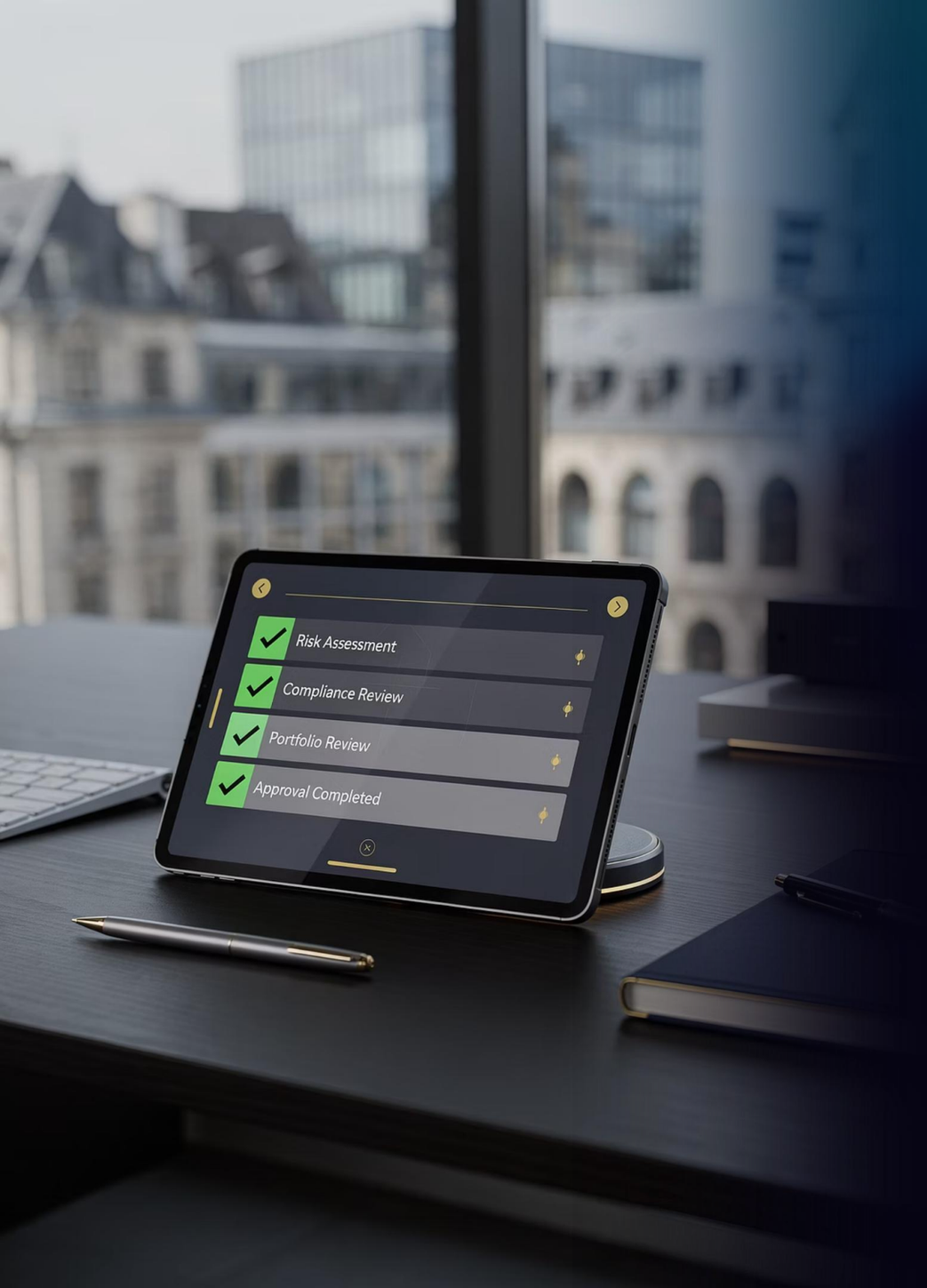
Monthly or quarterly: arbitrations, priorities, policy validation, incident and risk monitoring.

Network of "Privacy Champions"

Per department: information collection for the register, training relay, project detection.

Change Process

Any new processing/project (tool, service provider, marketing campaign, AI, CCTV) triggers a privacy analysis (Art. 25 and 35).



CHAPTER 4

Legal missions and expected deliverables (Art. 39)

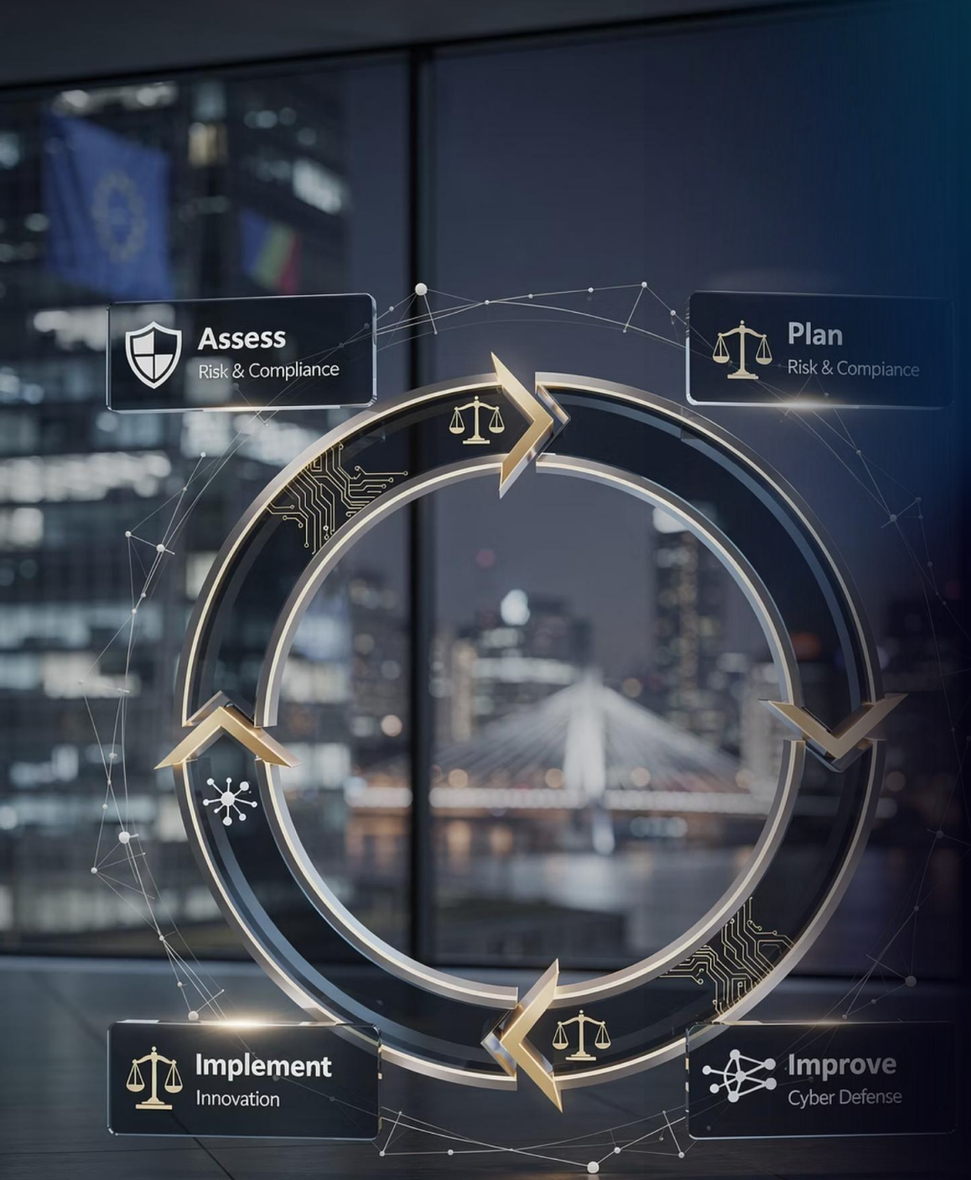
Article 39 of the GDPR defines the DPO's minimum missions. In practice, these missions translate into measurable deliverables and steering routines. The DPO must have effective access to information (register, contracts, incidents, projects) to be able to robustly produce this evidence (Art. 38(2)).

Inform, Advise & Monitor

Mission (Art. 39)	Operational Translation	Evidence / Deliverables
Inform & Advise (Art. 39(1)(a))	Business/management assistance: legal bases, clauses, cookies, transfers, AI, HR.	Dated DPO opinions, position papers, processing records, documented decisions
Monitor Compliance (Art. 39(1)(b))	Compliance program: policies, controls, audits, indicators, action plan.	Annual plan, KPI dashboard, audit reports, action log
Raise Awareness & Train (Art. 39(1)(b))	Initial training + refresher training + targeted awareness by business unit.	Training plan, content, completion rates, quizzes/certifications

Advise, Cooperate & Coordinate

Mission (Art. 39)	Operational Translation	Evidence / Deliverables
Advise on DPIAs (Art. 39(1)(c))	Risk analysis method for individuals; follow-up on measures.	DPIA Register, screening, DPIA reports, periodic reviews
Cooperate with the authority (Art. 39(1)(d))	Exchange management: requests, controls, notifications, consultations.	Exchange log, control files, decisions/measures
Contact point (Art. 39(1)(e))	Individuals/authority channel; request triage; internal coordination.	DPO channel, escalation procedure, request register



CHAPTER 5

Compliance Cycle: Implementation, Monitoring, Improvement

Sustainable compliance is not limited to producing documents. It is based on a **documented lifecycle**, regular reviews, and structured change management. The cycle is broken down into three complementary phases.

The three phases of the compliance cycle

1. Implement

Initial phase:

- DPO Governance (mandate, committee, RACI)
- Mapping & register (Art. 30)
- Legal bases & tests (LIA, consent)
- Notices & cookies (Art. 12-14)
- Policies & procedures
- Contracts (Art. 28/26)
- DPIA Screening (Art. 35)
- Training plan

2. Operate daily

« Run » phase:

- Project triage (privacy by design — Art. 25)
- Rights management (Art. 15-22)
- Third-party and security monitoring
- Incidents & breaches (Art. 33-34)
- Notices/register updates
- Business support (advice)
- Reporting to management

3. Improve & prove

Assurance phase:

- Quarterly KPI reviews
- Targeted audits and corrective actions
- Tests (phishing, vulnerabilities)
- Annual register & policies review
- Review of transfers (Art. 44+)
- DPO report & N+1 action plan

Triggers Requiring a Review

Certain events require an immediate review of the compliance framework, regardless of the periodic review schedule:

1

New Processing Activities

New tool/software, new data collection, new marketing channel, new HR processing, or video surveillance. Each new processing activity must be integrated into the register and undergo a DPIA screening.

2

New Third Parties

New service provider or transfer outside the EU/EEA, change of host, cascading subcontracting. Due diligence and contractual updates are required before any go-live.

3

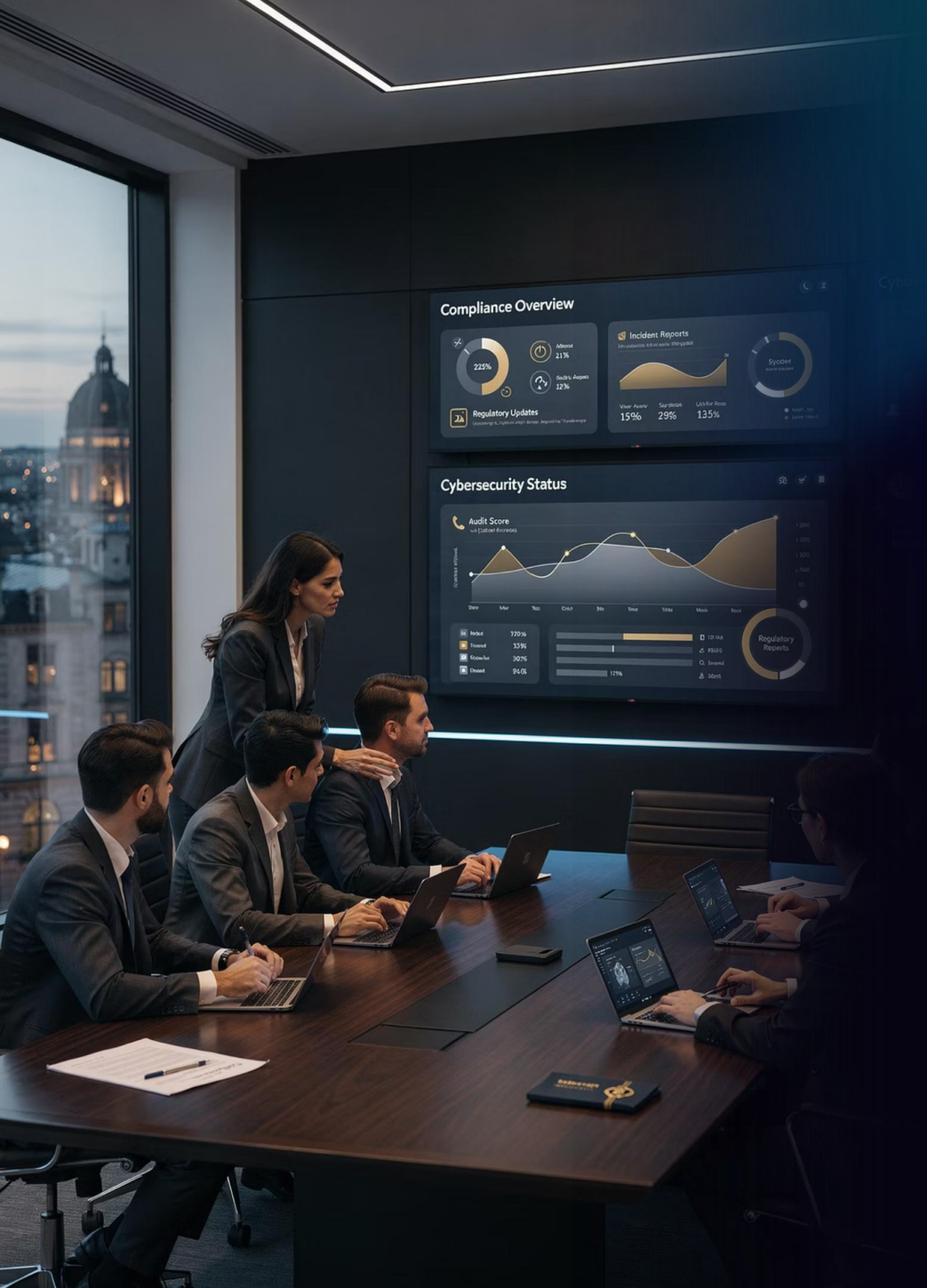
AI & Profiling

New AI/profiling/scoring project, automated decision-making (Art. 22), or substantial evolution of processing. These projects systematically require an in-depth DPIA.

4

Incidents

Security incident, suspected leak, recurring anomaly, client audit, or regulatory authority control. Responsiveness and documentation are essential to demonstrate compliance.



CHAPTER 6

Operational Compliance Axes

The following sections detail the **9 operational axes** of the GDPR compliance framework, each with its implementation actions, periodic reviews, and monitoring triggers.

AXIS 6.0

Governance and Accountability (DPO Foundation)

Legal Framework: Principles Art. 5; Accountability Art. 5(2) & 24; Privacy by Design Art. 25; DPO Obligations Art. 37-39 GDPR.
Objective: Implement a manageable compliance framework, proportionate to risks, and demonstrable at all times.

Implementation

- DPO Mandate/Charter: scope, reporting structure, resources, access, escalation
- Stakeholder mapping + RACI
- Privacy Committee + network of relays
- Documentary repository: policies, procedures, templates
- Prioritized compliance plan + action register
- Privacy decision validation mechanism

Monitoring & Triggers

- Escalation to management if residual risk is high
- Monitoring new projects via "privacy intake"
- Traceability: decisions, arbitrations, exceptions

1 2 3

Periodic Reviews

- Annual governance review (mandate, resources, conflicts)
- Quarterly review of action plan and risks
- Annual review of policies/procedures corpus

Evidence to retain: DPO designation letter / external DPO contract + signed charter; Committee minutes and arbitration decisions; dashboard (KPI, risks, incidents) + annual DPO report; documentary repository with version management.

AXIS 6.1

Training and Awareness

Legal framework: Art. 39(1)(b) GDPR (awareness/training); Art. 24 GDPR (appropriate measures).

Objective: Create a data protection culture: reduce human errors, make policies applicable and measurable.

Implementation

- Needs analysis by department (HR, IT, support, marketing, sales, finance, management)
- General GDPR training (foundation) + targeted modules (recruitment, prospecting, CCTV, IT support)
- Privacy onboarding journey for new hires
- Short micro-trainings (3-5 min) for new policies or recurring incidents
- Proof procedure: participation, quizzes, certificates, and archiving

Reviews & Monitoring

- Annual retraining (or biannual depending on risk) + updates during process/tool changes
- Quarterly review of completion rates and untrained populations
- Annual review of content library
- Monthly monitoring of completions (KPI) and automated reminders
- Ad-hoc campaigns: phishing simulation, password focus, file sharing
- Analysis of incidents/DSAR to identify subjects for (re)training

Evidence: Training plan and schedule; versioned content; list of participants, certificates, scores/quizzes; campaign reports and corrective actions.

AXIS 6.2

Data Analysis: Mapping, Register, and Retention

Legal Framework: Art. 30 GDPR (register); Art. 5(1) (minimisation, purposes, retention); Art. 6, 9, 10 (legal bases); Art. 25 (privacy by design).

Objective: To understand, justify, and control processing activities: purposes, legal bases, data, recipients, durations, transfers, risks.

Implementation

- Inventory of processing activities by department/service (structured register)
- Validation of legal bases and conditions Art. 9/10
- Legitimate Interest Assessment (LIA) for concerned processing activities
- Retention policy: durations + archiving/deletion rules
- Data flow mapping (systems, access, internal/external recipients)

Periodic Reviews

- Minimum annual review of the register and durations; update with every substantial change
- Quarterly review of new processing activities/projects and integration into the register
- Bi-annual control of deletion/archiving on critical systems

Monitoring & Triggers

- New processing activity, new purpose, new system, merger/acquisition, new service provider
- Monitoring of discrepancies: unregistered processing activities, questionable legal bases, unapplied durations
- Correlation with DPIA: early detection of high-risk processing activities (Art. 35)

Evidence: Up-to-date processing register (Art. 30); data dictionary and flow diagrams; documented LIAs; proof of consent; retention policy + proof of execution (purge logs, tickets, configurations).

PILLAR 6.3

Transparency and Information (Notices, Cookies)

Legal framework: Art. 12 to 14 GDPR; Art. 5(1)(a); Art. 7 and 21; cookie/ePrivacy rules according to the States.

Objective: Clearly inform individuals (clients, prospects, candidates, employees, visitors) and manage cookies/trackers.

Implementation

General policy + notices by population: website, clients/prospects, employees, candidates, CCTV. Notices register (versioning). Cookies/trackers framework: inventory, categorization, banner/consent, proof of choices. Information models for indirect collection (Art. 14). Visible and operational DPO channel (Art. 37(7) and 38(4)).

Periodic Reviews

Annual review of notices and immediate review in case of processing change. Quarterly review of cookies/trackers (technical scan, script verification). Consistency check: register (Art. 30) vs notices (Art. 13-14) vs contracts (Art. 28/26).

Monitoring & Triggers

New marketing campaign, new tracker, new SaaS analytics/CRM, new form. Monitoring of consent withdrawal and marketing objections (Art. 7(3) and 21). Monitoring of complaints/questions received via the DPO channel.

Evidence: Dated and versioned notices; cookie banner captures; tracker scan reports; consent register + proof of withdrawal; marketing objection log; dissemination proofs.

AXIS 6.4

Security of Personal Data (TOMs, risks, maturity)

Legal framework: Art. 32 GDPR; Art. 5(1)(f); Art. 25; Art. 24 (appropriate measures).

Objective: Reduce the risk of harm to rights and freedoms through security proportionate to risks, tested and documented.

Security: Actions and Operational Monitoring

Implementation

- Review of existing measures and risk analysis (threats, vulnerabilities, impacts)
- Definition of a list of TOMs: access, MFA, encryption, backups, logs, segmentation, DLP
- IT Policies: access management, workstations, mobile devices, passwords, backups, remote work, BYOD
- Alignment with ISO 27001/27002 to drive maturity development
- Testing plan: vulnerability scans, patches, access reviews, exercises

Periodic Reviews

- Annual review of risk analysis and TOMs; adjustment in case of major evolution
- Weekly vulnerability scans (or according to criticality) + remediation follow-up
- Quarterly review of authorizations on sensitive systems

Monitoring & Triggers

- Vulnerability monitoring: remediation SLAs, documented exceptions, accepted residual risks
- Trigger: security incident, new cloud, API integration, supplier access
- Monitoring of security awareness campaigns (phishing) and recurring discrepancies

Evidence: TOMs Register; IT policies; implementation evidence (tickets, logs, configurations); scan/pentest reports; remediation plans; access review reports; risk analysis; risk acceptance decisions; BCP/DRP if applicable.

AXIS 6.5

Processing Actors: Controllers, Processors, and Partners

Legal Framework: Art. 28 (processors); Art. 26 (joint controllers); Art. 29; Art. 32; Art. 44+.
Objective: To master the processing chain: who does what, on what basis, with what guarantees, and with what level of risk.

Third-Party Register

Inventory of all suppliers, partners, and clients handling personal data

Legal Qualification

Controller, processor, joint controller or recipient — each third party must be qualified

Contract Updates

Art. 28 clauses, security, data subject rights/DPIA assistance, audit, sub-processing in cascade

Due Diligence

Risk-based privacy & security: questionnaire, evidence, technical analysis if necessary

Vendor Onboarding

DPO + IT/Security + Procurement validation before signing any new contract

Reviews: Annual review of at-risk suppliers and before contract renewal. Periodic review of subsequent processors (list, changes, notifications). Ad-hoc controls: audits, evidence reviews, verification of announced measures.

Evidence: Third-party register + qualification forms; signed DPAs/Art. 26 agreements; due diligence reports, risk scoring; traceability of validations and approved subsequent processors.

AXIS 6.6

Data Subject Rights (DSAR): Organization, Deadlines, Evidence

Legal Framework: Art. 12; art. 15-22; art. 7(3); art. 19; art. 21(2) GDPR.

Objective: To respond securely, completely, and within deadlines to any request for the exercise of rights (clients, prospects, employees).

Implementation

- DSAR procedure: channels, triage, identity verification, roles, escalation, deadlines, exemptions
- Response templates + request register
- Search/extraction mechanism: system mapping, data collection owners, secure extraction
- Marketing procedure: unsubscribe, objection, exclusion lists
- Training of front-office/HR teams to recognize a request (even implicit)

Deadlines & Monitoring

Response within 1 month (extendable by 2 months) — art. 12(3)

- Monthly/quarterly review: deadlines, quality, incidents (KPI)
- Annual end-to-end DSAR test
- Update templates/register in case of evolution
- Suspicion of identity theft, repetitive request, conflict with legal retention obligation
- Erasure follow-up and evidence; notification to recipients if required (art. 19)

Evidence: DSAR Register: dates, verified identity, right invoked, decision, response date, documents transmitted. Copies of responses; extraction/erasure logs; marketing objection lists. DSAR test report and improvement actions.

AXE 6.7

Privacy by design & AIPD (DPIA)

Legal Framework : Art. 25 ; art. 35 ; art. 36 ; art. 22 ; art. 9-10 GDPR.

Objective : Detect high-risk processing, analyze impacts on individuals, define and monitor risk reduction measures.

1

DPIA Screening

Process integrated into project management (short, traceable questionnaire) with alert criteria based on EDPB guidelines (9 criteria)

2

DPIA Model

Description, necessity/proportionality, risks, measures, residual risk, decision. Validation by business, IT/security, DPO

3

Register & decisions

DPIA Register + register of decisions (DPIA performed / not necessary). Prior consultation if high residual risk (Art. 36)

4

Periodic Reviews

Review in case of substantial change. Periodic review (1 to 3 years) of DPIAs for critical processing. Review of the effectiveness of measures

Triggers : AI/profiling, biometrics, geolocation, CCTV, employee monitoring, database sharing. Monitoring of the DPIA action plan: measures, milestones, evidence. Traceability of DPO opinions and final management decisions.

Evidence : Screening questionnaires; signed DPIA reports; prior consultation decisions; action plans and evidence of implementation; dated DPO opinions, arbitration and acceptance of residual risk.

AXIS 6.8

Data Breaches: Preparation, Reaction, Documentation

Legal Framework: Art. 33 (notification within 72h); Art. 34; Art. 32; Art. 33(5) GDPR.
Objective: Be ready to detect, qualify, and manage a breach, limit impact, notify if necessary, and prove compliance.

The procedure must define roles and the contact list (DPO, IT/Security, Management, Communication, Legal), notification templates and decision criteria (authority / individuals), as well as the incident/breach register (systematic documentation, even without notification). An annual "72h" exercise (table-top) and a systematic post-incident review are essential.

Evidence: Breach register: chronology, data, volume, causes, measures, decision to notify or not (Art. 33(5)). Notifications/exchanges; proof of communication to individuals. Exercise reports and remediation evidence.

AXIS 6.9

International Transfers (outside EU/EEA)

Legal Framework: Art. 44-49 GDPR; Art. 45 (adequacy); Art. 46 (safeguards, e.g. SCC); Art. 49 (derogations).
Objective: Identify and frame any transfer or access from a third country (including remote access, support, subcontracting).

Implementation

- Mapping of transfers: providers, subsidiaries, support, backups, non-European tools
- Qualification: adequate country vs safeguards vs derogation
- Appropriate contractual clauses (SCC) or other mechanisms + management of subsequent subcontractors
- TIA process and additional measures (encryption, pseudonymization, access control)
- Update notices and client contracts if necessary

Periodic Reviews

- Annual review of the transfer register and TIAs; re-qualification if provider changes
- Monitoring of changes impacting transfers (SCC versions, location, subcontracting)
- Periodic review of additional measures (effectiveness, logs, keys, access)

Monitoring & Triggers

- New SaaS, cloud region change, non-EU support, third-party admin access
- Monitoring of requests for access from foreign authorities (if applicable) and internal procedure
- Monitoring of client audits related to data localization

Evidence: Transfer register + flow diagrams; signed SCC/clauses; TIAs; evidence of additional measures (encryption, key management, logs); versions of notices and client communications.

AXIS 6.10

Control, Audit, and Continuous Improvement

Legal Framework: Art. 5(2) and 24 (accountability); Art. 32; Art. 39(1)(b); Art. 30 and 33(5).

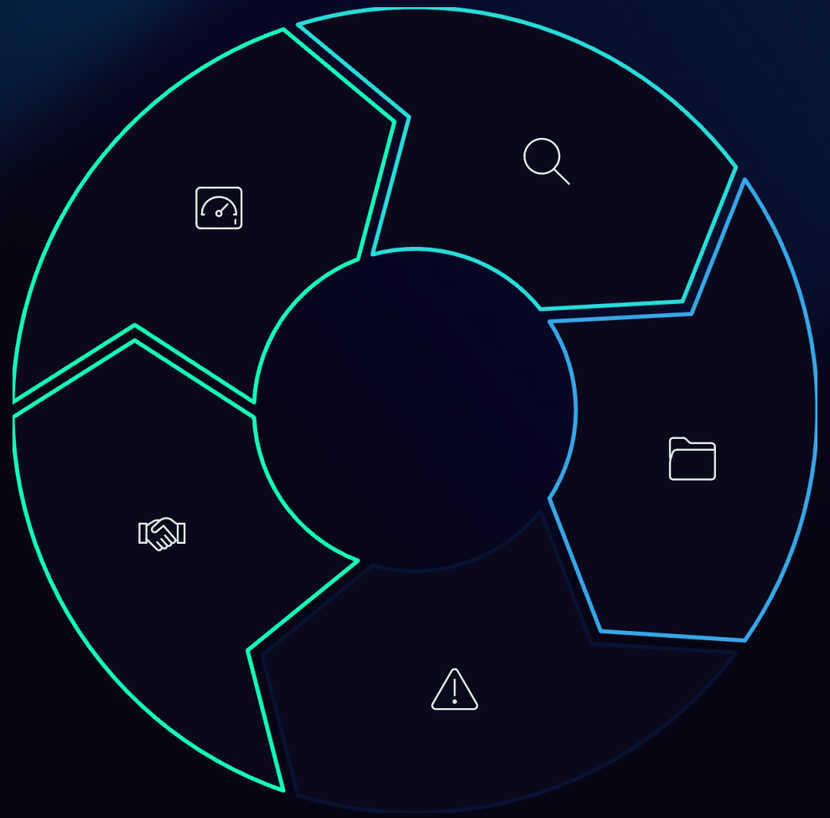
Objective: Transform compliance into a management system: indicators, controls, reviews, audits, corrective actions.

Dashboard

Register, training, DSAR, DPIA, evaluated suppliers, incidents, vulnerabilities, audits

Client/Third-party Audits

Standardized responses, security & privacy pack



Internal Audit

Annual plan focused on risks and critical processing

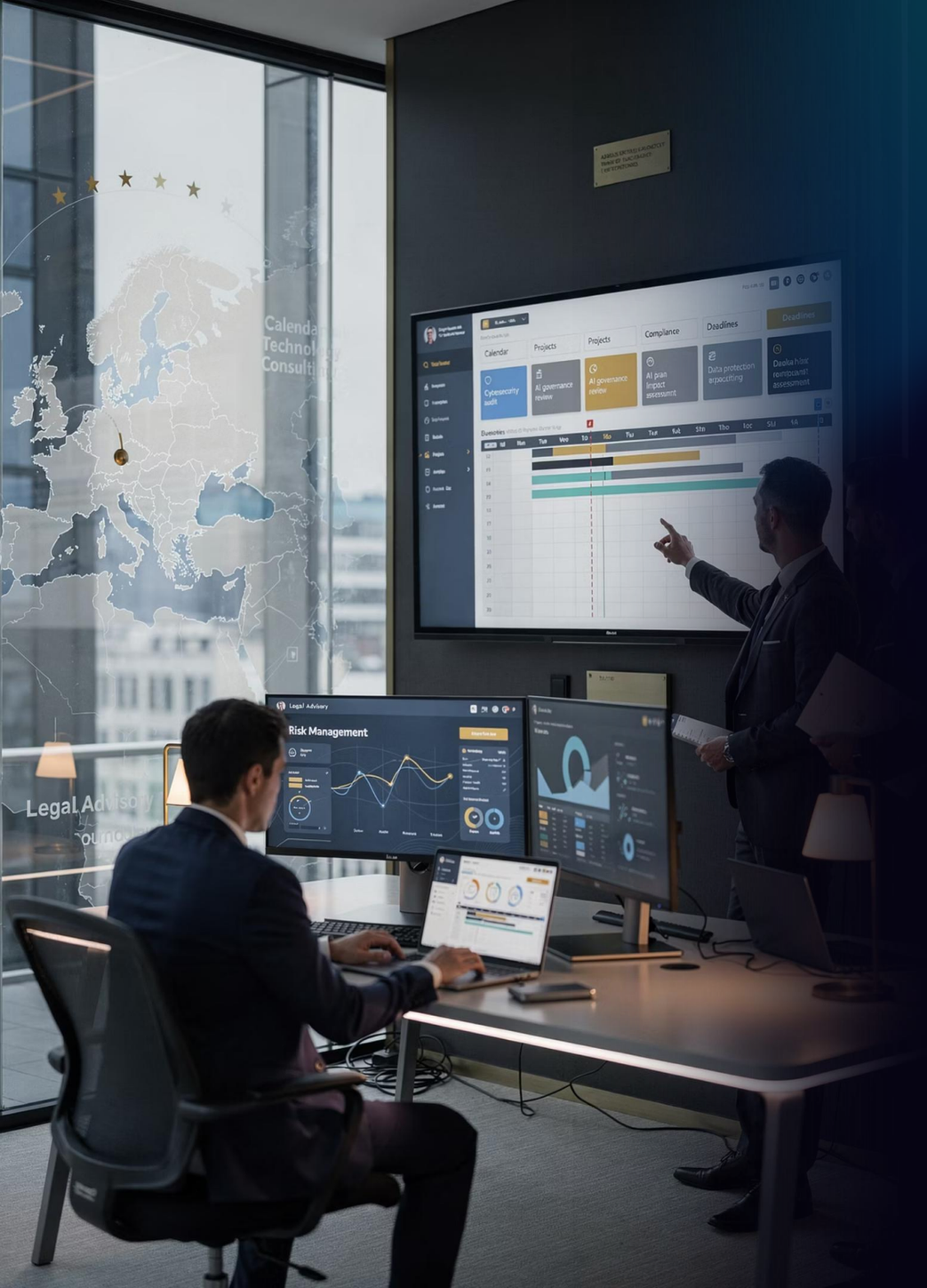
Evidence Pack

Localization of documents and proof of effectiveness

Non-conformities

Detection, analysis, corrective action, validation, closure

Cadence: Monthly/quarterly KPI review in committee; annual management review (assessment, maturity, incidents, N+1 plan); annual or biannual audit (register, contracts, rights, incidents, transfers). Action tracking: deadlines, responsible parties, evidence, residual risks. Continuous improvement via feedback and policy updates.



CHAPTER 7

Management: Recommended Review Cadence

The exact frequency depends on the risk, the volume of processing, and the level of maturity. The table below suggests an **operational cadence generally suited for SMEs and groups**.

Weekly and Monthly Reviews

Frequency	Review / Activity	Indicators / Deliverables
Weekly	Vulnerability scans / patch monitoring; new project and request triage; ongoing incident monitoring	Scan report & backlog; privacy intake log; incident ticketing
Monthly	Monitoring of data subject access requests (DSAR); monitoring of onboarding suppliers; DPO operational reporting	DSAR delay KPIs; % suppliers evaluated; DPO opinions/notes

Quarterly and Semi-annual Reviews

Frequency	Review / Activity	Indicators / Deliverables
Quarterly	Privacy Committee (management); risk & actions review; cookies/trackers review; critical authorizations review	Committee minutes + decisions; risk register; cookie scan report; access review log
Semi-annual	End-to-end DSAR test; incident exercise (partial); retention control (sample)	DSAR test report; exercise report; purge/archiving proofs

Annual Review

Register & notices

Review of the register (Art. 30) and information notices — versioning and updating

Critical DPIAs

Review of DPIAs on the most sensitive processing operations — DPIA register & periodic reviews

Targeted Internal Audit

Audit focused on critical risks and processing operations — audit reports and action plans

N+1 Training Plan

Development of the training plan for the following year — content, target audiences, schedule

DPO Annual Report

Comprehensive annual review: maturity, incidents, KPIs, recommendations, and N+1 action plan

Document Compliance Checklist

This quick appendix summarizes all the documents and evidence to maintain to demonstrate compliance at all times:

- Record of Processing Activities (Art. 30)
  Up-to-date + associated retention policy
- Notices (Art. 12-14)
  + cookies/trackers policy and proof of consent if applicable
- Third-Party Register + DPAs (Art. 28)
  Art. 26 agreements + proof of due diligence
- DSAR Procedure + Register
  Proof of timely response (Art. 12, 15-22)
- DPIA Register + Screening + Reports (Art. 35)
  Decisions (Art. 36 consultation if necessary)
- Incidents/Breaches Procedure + Register (Art. 33(5))
  Proof of simulation exercises
- Transfer Register + SCC/TIA (Art. 44-49)
  Documented supplementary measures
- IT/TOMs Policies + Proof of Tests (Art. 32)
  Scans, pentests, access reviews
- Training Program + Completion Rate (Art. 39)
  Certifications and scores
- DPO Dashboard and Reports
  Accountability Art. 5(2)/24 — proof of continuous monitoring

Main Legal References

Regulation (EU) 2016/679 (GDPR) — most frequently used articles in a DPO system:

Principles & Accountability

Art. 5 (principles) and 5(2) (accountability). Art. 24-25 (responsibility and privacy by design). Art. 28-29 (subcontracting and authorized persons).

Legal Bases & Sensitive Data

Art. 6, 7 (legal bases and consent). Art. 9-10 (sensitive/criminal data).

Transparency & Rights

Art. 12-14 (transparency). Art. 15-22 (rights of data subjects).

Registry & Security

Art. 30 (record of processing activities). Art. 32-34 (security and breaches).

DPIA & DPO

Art. 35-36 (DPIA and prior consultation). Art. 37-39 (designation, position, and tasks of the DPO).

International Transfers

Art. 44-49 (international transfers of personal data).

For a robust implementation, it is recommended to rely on the **guidelines of the European Data Protection Board (EDPB)** concerning the DPO, DPIAs, and transfers, as well as security frameworks (**ISO 27001/27002**) where relevant.

In summary: keys to success

Clear Governance

A formalized mandate, an active privacy committee, and a network of departmental relays constitute the essential foundation of the DPO system.

Continuous Cycle

Compliance is not a one-time project but a permanent cycle: implementation, daily operation, improvement, and proof.

Documented Proof

Accountability requires being able to demonstrate compliance at all times: registers, opinions, reports, tests, and versioned dashboards.

Privacy Culture

Training, awareness, and the involvement of all departments transform compliance into a sustainable organizational reflex.

Note: this document is an operational brochure. It must be adapted to the sectoral context, applicable national law, and contractual requirements of each organization.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116