Luxgap
DATA PRIVACY PARTNER

Luxgap

Compliance • Cybersecurity • Resilience

We translate regulatory requirements into operational measures: governance, tooling, evidence, and continuous monitoring. From personal data protection to digital resilience and artificial intelligence governance, Luxgap supports European organizations in fulfilling all their obligations — with pragmatism, rigor, and independence.

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

OVERVIEW

Our mission: secure your compliance, end-to-end

In a constantly evolving regulatory landscape — GDPR, NIS2, DORA, AI Act, whistleblower — organizations must demonstrate not only formal compliance, but also their operational capacity to protect data, manage cyber risks, and ensure business continuity. Luxgap positions itself as a trusted partner to orchestrate this global compliance.

GDPR / DPO

Personal data governance, register, rights, evidence, and accountability

NIS2 & DORA / CISO

Cybersecurity, operational resilience, ICT risk management, and reporting

BCP / ISO 22301

Monthly business continuity program: BIA, plans, exercises, and continuous improvement

Whistleblower

Secure portal, confidentiality, traceability, and signal monitoring

EEM / Monitoring

Dark Web monitoring, data leaks, compromised credentials, brand impersonation, external attack surface, and Shadow IT

AI Act

Compliance with Regulation (EU) 2024/1689: risk classification, AI governance, technical documentation, and transparency obligations

HRIS & E-Learning Platform

Employee-oriented software: HR, training, AI, integrated compliance, and security

Short formats available (diagnostic / scoping) — long formats upon request (complete program).

SUMMARY

Summary Table: Our Services by Regulatory Framework

This table provides a consolidated view of all Luxgap services, linking them to the European regulatory obligations they address. It allows decision-makers to quickly identify relevant services based on their scope of subjection.

Luxgap Service	GDPR	NIS2	DORA	AI Act	Whistleblower
External DPO / DPO Assistance	✅ Art. 37-39, 5, 24, 25, 28, 32	—	—	—	—
Register, DPIA, Data Subject Rights	✅ Art. 30, 35, 15-22	—	—	—	—
Clauses & Subcontractor Due Diligence	✅ Art. 28	✅ Art. 21	✅ Ch. V (ICT third-party risk)	✅ Art. 25 (value chain)	—
External CISO / Security Governance	✅ Art. 32	✅ Art. 20-21	✅ Ch. II (ICT risk mgmt)	✅ Art. 9 (cybersecurity)	—
Incident Plan & Reporting	✅ Art. 33-34	✅ Art. 23	✅ Ch. III (incident reporting)	✅ Art. 62 (serious incidents)	—
Resilience Tests (TLPT, Exercises)	—	✅ Art. 21	✅ Ch. IV (tests)	✅ Art. 9, 15 (robustness)	—
Dark Web / EEM Monitoring	✅ Art. 32	✅ Art. 21	✅ Ch. II	—	—
BCP / Business Continuity	—	✅ Art. 21	✅ Ch. II & IV	—	—
Whistleblower Portal	✅ (data processing)	—	—	—	✅ Dir. (EU) 2019/1937
HRIS Platform / E-Learning / AI	✅ Art. 5, 24, 25, 32	✅ (awareness Art. 20)	✅ (training Art. 13)	✅ Art. 4 (AI control), Art. 26 (deployers)	✅ (training)
Compliance Document Management	✅ Accountability	✅ Art. 21	✅ Ch. II	✅ Art. 11, 18 (technical documentation)	✅ Traceability
AI Act Compliance	✅ (AI DPIA, Art. 35)	—	—	✅ Reg. (EU) 2024/1689	—

✅ = service directly applicable to the regulatory framework. Article references are indicative and vary depending on the scope of the organization. Luxgap adapts its services according to the actual subjection of each client.

CHAPTER 1

GDPR

Governance and Protection of Personal Data

GDPR

GDPR — A structured and demonstrable compliance program

The General Data Protection Regulation requires organizations to actively demonstrate their compliance (*accountability*). Luxgap offers two complementary levels of intervention: an **external DPO mandate** for organizations wishing to delegate the function, or **assistance to an existing DPO** to temporarily strengthen internal capabilities. In both cases, our objective is clear: to produce demonstrable compliance, at all times, before an authority, a client, or an audit.

External DPO Mandate

- Full management of the GDPR program
- Interface with the supervisory authority and audit management
- Documented advice and arbitration on sensitive processing
- Proactive risk reduction: fines, incidents, damage to reputation

DPO Assistance

- Ad-hoc support for specific high-stakes projects (migration, new product, partnership)
- Continuous updating of compliance evidence
- Preparation for authority controls and client audits
- Support on DPIAs and targeted risk analyses

GDPR

What we address: the pillars of GDPR compliance

Our approach covers all the structuring requirements of the regulation, from processing mapping to continuous demonstration of compliance. Each pillar is designed to produce tangible and auditable evidence.

1

Data Processing Control

Exhaustive register, documented legal bases, defined and applied retention periods. This foundation forms the basis of any demonstration of compliance (Art. 5, 6, 30).

2

Rights & Transparency

Operational processes to respond to requests for exercising rights (access, rectification, erasure, portability) within legal deadlines, with full traceability (Art. 15-22).

3

Processors & Security

Compliant contractual clauses, supplier due diligence, framing of transfers outside the EU and proportionate technical and organizational security measures (Art. 28, 32, 44-49).

4

Governance & Accountability

Formalized roles and responsibilities, steering committees, documented decision-making processes, and consolidated evidence to demonstrate compliance at all times (Art. 5.2, 24, 25).

GDPR

Deliverables: "Ready-to-Demonstrate" Compliance

Our deliverables are designed to be immediately usable and auditable. They form the documentary and operational foundation of your GDPR program, whether as part of an initial diagnostic (short format) or a full support package.

"Ready-to-Demonstrate" Compliance

- Complete documentary framework: policies, procedures, roles and committees
- Data subject rights processes: reception, processing, response, archiving
- Incident processes: detection, qualification, notification, evidence
- Contractual clauses and subcontractor due diligence
- Management dashboard: risks, actions, deadlines, KPIs

Short Format Deliverables (diagnostic / scoping)

- Maturity diagnosis and prioritized roadmap
- Structured processing register + policy templates
- Targeted DPIAs for high-risk processing with actionable recommendations
- Incident plan and implementation support
- Gap analysis and remediation plan

CHAPTER 2

NIS2 & DORA

Cybersecurity Governance and Operational Resilience

NIS2 & DORA

NIS2 & DORA — Aligning Governance, Technology, and Response Capability

The NIS2 directives and the DORA regulation impose unprecedented cybersecurity and operational resilience requirements on essential and important organizations, as well as the financial sector. The challenge goes beyond implementing technical measures: it's about aligning governance, controls, incident management, and third-party oversight—with auditable evidence at every step.

Luxgap offers an **external CISO mandate** or **CISO assistance** tailored to each organization's scope, covering initial compliance, recurring controls, and reporting to authorities.

External CISO

Security strategy and governance, risk management and continuous controls, animation of security committees, definition of KPIs and monitoring of action plans. The external CISO acts as a true Chief Information Security Officer, integrated into your governance.

NIS2 Program

Scoping of the entity and its essential/important activities, implementation of organizational and technical measures (Art. 21), incident management plan with reporting to authorities (Art. 23), and supply chain management.

DORA Program

ICT risk management (policies, controls, documentation compliant with Ch. II), resilience tests and exercises including TLPT according to the applicable scope (Ch. IV), and management of ICT third-party risk with a register of agreements (Ch. V).

Optional: risk mapping, SOC/monitoring, vulnerability management, awareness campaigns, and preparation for client and competent authority audits.

CHAPTER 3

Business Continuity

Monthly ISO 22301 program: impact analysis, continuity strategies, plans, exercises, and continuous improvement

BCP

Business Continuity — Monthly and Turnkey ISO 22301 Program

Luxgap offers a comprehensive Business Continuity Program (BCP) aligned with the ISO 22301 standard. Deployed progressively and billed monthly, this program covers the entire business continuity cycle: impact analysis, strategy definition, plan development, practical exercises, and continuous improvement.

Business Impact Analysis (BIA)

Identification of critical processes, Recovery Time and Point Objectives (RTO/RPO), dependencies, and potential disruption scenarios.

Continuity Strategies

Definition of recovery strategies, alternative solutions, and allocation of critical resources to maintain essential business functions.

Continuity & Crisis Management Plans

Drafting of detailed BCP/DRP plans, crisis procedures, escalation chains, and communication for a coordinated response in the event of an incident.

Exercises & Tests

Annual program of exercises (tabletop, simulation, real-life test), measurement of plan effectiveness, and collection of feedback for adjustment.

Continuous Improvement & Audit

Periodic reviews, monitoring of performance indicators, and preparation for ISO 22301 certification audits for lasting resilience.

A predictable budget, a structured program: our monthly approach allows for the progressive deployment of ISO 22301 compliance without mobilizing a massive project budget, while ensuring concrete deliverables at each stage.

CHAPTER 4

Whistleblower

Secure portal, confidentiality, traceability and system management

WHISTLEBLOWER

Whistleblower — Secure Internal Channel and Comprehensive System Management

The European Directive (EU) 2019/1937 requires organizations to establish a secure internal reporting channel, guaranteeing the confidentiality of the whistleblower, the traceability of exchanges, and the monitoring of corrective actions. Luxgap provides a ready-to-use online portal, combined with methodological support to ensure the operational compliance of the system.

Whistleblower Portal (online)

- Internal reporting channel (web) with automatic acknowledgment of receipt within legal deadlines
- Enhanced confidentiality and strict separation of roles (investigator, decision-maker, DPO)
- Complete workflow: triage, secure exchanges with the whistleblower, corrective actions, closure
- Full traceability: event log, timestamped evidence, compliance with regulatory deadlines
- Anonymized reporting for governance and control bodies

Engagement Model

01

Quick Diagnosis

Scope, applicable obligations, current maturity level

02

Framing

Roles, planning, monitoring indicators, expected evidence

03

Implementation

Policies, processes, technical tools, training

04

Run

Monitoring, controls, incident management, audits

Option: outsourcing of report processing (guarantee of independence) and articulation with GDPR / security for consistent management of sensitive data.

CHAPTER 5

AI Act

Compliance with the European Artificial Intelligence Regulation: classification, governance, documentation, and transparency

AI ACT

AI Act — Structured support for compliance with Regulation (EU) 2024/1689

The European Artificial Intelligence Regulation (AI Act) came into force on August 2, 2024, with progressive application until August 2027. It imposes a risk-based approach on providers and deployers of AI systems: prohibited practices, high-risk systems subject to reinforced obligations, and transparency obligations for all. Luxgap supports organizations in the operational compliance of their AI systems, from initial inventory to continuous governance.

Inventory & classification of AI systems

Exhaustive mapping of AI systems used or developed, classification according to risk levels (unacceptable, high, limited, minimal), identification of applicable obligations per system.

Technical documentation & compliance

Drafting of technical documentation (Art. 11), compliance assessments, fundamental rights impact assessments (Art. 27), coordination with existing GDPR DPIAs.

AI governance & organization

Implementation of the internal governance framework: roles and responsibilities, AI usage policies, validation processes before deployment, human oversight (Art. 14).

Transparency & information

Obligations to inform users (Art. 13, 50), marking of AI-generated content (deepfakes, texts), register of high-risk systems, traceability of automated decisions.

Post-market surveillance & continuous improvement

Continuous monitoring of performance and risks, management of serious incidents (Art. 62), documentation updates, preparation for audits and controls by national authorities.

Engagement Model

01

AI Diagnosis

Systems inventory, risk classification, gap analysis

02

Framing

Compliance plan, prioritization, target governance

ĆĊ

Implementation

Documentation, processes, training, tooling

ĆÇ

Run

Continuous monitoring, incidents, audits, improvement

GDPR / AI Act Interoperability: when AI systems process personal data, we ensure consistency between the obligations of the AI Regulation (documentation, transparency, human oversight) and those of the GDPR (DPIA, legal basis, data subject rights) — an integrated approach to avoid redundancies and blind spots.

CHAPTER 5

HRIS Platform

E-Learning, integrated AI, and a secure ecosystem — our ultra-secure employee-oriented software

HRIS

Global Architecture: A Secure and Modular HRIS

The platform is not just a training tool. It is part of a complete **HRIS** (Human Resources Information System) architecture, integrating administrative management, regulatory compliance, and artificial intelligence in a highly secure environment. This unified approach transforms the platform into a **cross-functional governance** tool, linking HR, compliance, and operational security.

Comprehensive HR Management

- Payroll and administrative personnel management
- Leave, absence, and planning management
- Centralized contractual and document tracking
- Employee portal for employee autonomy

Fleet Management

- Vehicle allocation and user tracking
- Contract, insurance, and deadline tracking
- Documentation related to employer responsibilities
- Automatic alerts for renewals

Compliance Document Management

- Centralization of internal policies and procedures
- Integrated processing register and DPIA
- Management of subcontractors and corrective action plans
- Audit tracking with full audit trail

E-LEARNING AI

Integrated E-Learning and Artificial Intelligence

E-Learning Module

The training module is natively integrated into the HRIS ecosystem, allowing for fluid management of awareness and certification pathways.

- **Short video capsules** adapted to employees' operational constraints
- **Validation questionnaires** with configurable scoring and success thresholds
- **Monitoring certification** with downloadable attestations
- **Probative traceability** of pathways: exportable data for audits
- Automatic invitations: the employer selects modules and sends emails

Integrated Artificial Intelligence

AI acts as a **permanent internal assistant**, integrated at the heart of the HRIS to reinforce regulatory dissemination and reduce the risk of internal errors.

- **Automated responses** to employee questions on internal policies and regulatory obligations
- **Dynamic adaptation** to legal and organizational changes in real-time
- **Interactive educational support** integrated into training pathways
- Homogeneous dissemination of regulatory interpretation throughout the organization

SECURITY

Security, Compliance, and Independent ISAE 3000 Type 2 Audit

The platform has undergone an **independent ISAE 3000 Type 2 audit**, certifying the compliance of security and data protection controls over time. This audit provides a guarantee of trust for organizations subject to strict due diligence obligations on their subcontractors.

Information of Individuals

Complete transparency on processed data

Data Security

Audited technical and organizational measures

Minimization

Collection limited to what is strictly necessary

Rights Management

Operational rights exercise processes

Data Deletion

Automated purging according to defined retention periods

Data processing is governed by a **specific registry** distinguishing between service provision and security improvement. The environment is designed to meet the requirements of **GDPR (Art. 5, 24, 25, 32)**, as well as organizational obligations arising from **NIS2** and **DORA** where applicable.

INTEGRATION

Complete Integration and Strategic Positioning

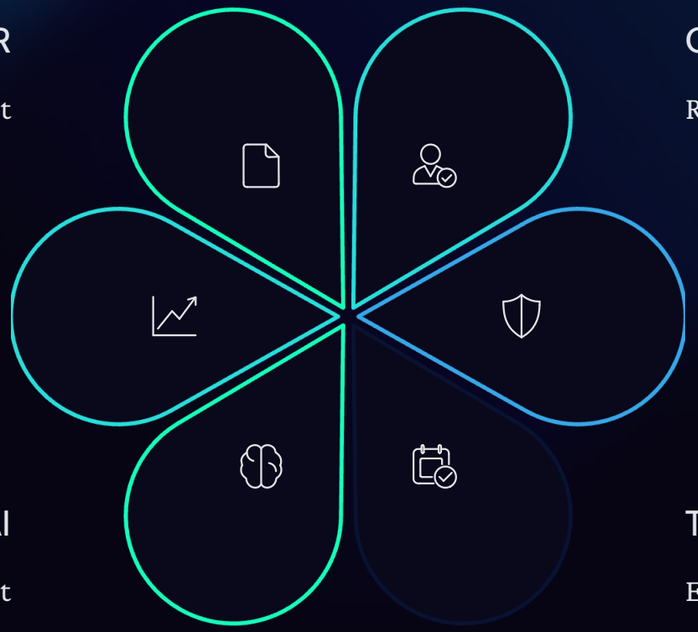
The platform integrates all LuxApps application bricks to form a **unified digital infrastructure** combining HR, compliance, security, training, and artificial intelligence. It provides management with a consolidated and secure overview of all organizational obligations.

HR

Complete administrative management

Compliance

Register, DPIA, subcontractors



Reporting

Real-time executive monitoring

Security

Vulnerability scanner, controls

AI

Integrated regulatory assistant

Training

E-Learning and certification

Centralization

Unified HR and compliance data

Reduced Risk

Reduction of legal risk

Traceability

Probative evidence of actions

Automation

Internal regulatory responses

OUR APPROACH

A Simple and Proven Engagement Model

Regardless of the regulatory scope — GDPR, NIS2, DORA, or whistleblower protection — our methodology follows a structured four-phase cycle. This framework ensures progressive, documented, and measurable compliance, adapted to each organization's maturity and resources.

1. Diagnosis

Rapid assessment of the scope, applicable obligations, and current maturity level. Identification of critical gaps and quick wins.

2. Framing

Definition of roles, planning, monitoring indicators, and expected evidence. Prioritized roadmap validated by management.

3. Implementation

Deployment of policies, processes, technical tools, and training. Production of initial auditable deliverables.

4. Continuous Operation

Continuous monitoring, recurrent controls, incident management, audits, and ongoing improvement of the system.

Short formats available (diagnosis / framing) — long formats on request (full program by regulation and by sector).

Next Steps — Contact Us

Would you like the detailed version? We have long formats — playbooks, templates, evidence, complete programs — by regulation and sector.

Julien Winkin

julien.winkin@luxgap.com+352 621 583 116

Luxgap SARL

2 rue de l'école

L-8376 Kahler, Luxembourg

Compliance • Cybersecurity • Resilience — We translate regulatory requirements into operational frameworks.