RSECURE

DPO SUPPORT SERVICES

Rely on our experts to help you manage the most complex aspects of your DPO duties

As a DPO, you are the orchestrator of compliance. Faced with the requirements of the CNPD and the constantly evolving landscape (NIS2, DORA, AI Act, ISO 27001, etc.), your workload is becoming increasingly complex. You can't be an absolute expert in all these areas at once. But the role of DPO requires you to have both legal and technical knowledge.

Our experts support you across three fundamental pillars of the DPO role:

Pillar 1 : GDPR Compliance & Data Privacy

- Privacy by Design & Default: integrating compliance from the design phase into your development cycles (Agile, DevOps) and new products—support throughout the data lifecycle and implementation of data management policies.
- Complex Data Protection Impact Assessments (DPIAs): conducting assessments that require a detailed understanding of IT architecture, databases, or high-risk processing activities (biometrics, scoring, surveillance).
- International Data Transfers (IDT): Analysis of third-country legislation (following the Schrems II ruling) and implementation of standard contractual clauses (SCCs) tailored to your cloud service providers.
- Crisis Management & CNPD Audits: emergency response team in the event of a data breach (notification within 72 hours) and preparation for/simulation of audits by the supervisory authority.
- Customized Training and Awareness Programs: programs tailored by business function (HR, Marketing, IT) that go beyond generic training.

Rsecure SARL / www.rsecure.lu
38-40, Parc d'Activités de Capellen L-8308 - Luxembourg

Pillar 2 : Cybersecurity and resilience

- Coordination between the DPO and CISO: Aligning privacy policies with technical security measures (encryption, pseudonymization, access management).
- Security Audits of Third-Party Service Providers: Rigorous assessment of the cybersecurity maturity of your strategic service providers prior to entering into contracts.
- Regulatory Synergy (DORA & NIS2): mapping of cross-cutting requirements. For the financial sector, we help you integrate your GDPR obligations into the ICT risk management framework required by the DORA Regulation. For companies subject to the NIS2 Directive, we help you achieve compliance.
- Incident Response (IRP): Collaborative development of security incident response plans that natively integrate GDPR communication processes.

Pillar 3 : Artificial Intelligence & emerging technologies

- AI Governance and Mapping: Inventory of AI systems used internally (Shadow AI) and classification of their risk levels.
- "AI Act" & GDPR Compliance: Assessment of the overlap between the two regulations. How should personal data ingested by an LLM be managed? How can the right to be forgotten be guaranteed when dealing with a trained model?
- AI Acceptable Use Policy: Drafting clear guidelines for your employees regarding the use of tools such as ChatGPT, Copilot, or Claude in the workplace, while protecting your trade secrets and your customers' data.
- Ethics and Algorithmic Bias: Auditing models to prevent discrimination and ensure the explainability of automated decisions.

OUR MÉTHODOLOGY

After a quick assessment (a 2-hour session to map out your urgent needs, identify your pain points, and define your priorities), you choose a customized service:

- "DPO Desk": Whether you need quick answers or one-time legal or technical advice, we'll provide a response within 24 to 48 hours to resolve complex situations.
- Sparring Partner: Whether you need to challenge an approach, prepare for an executive committee meeting, or review a decision, our regular coaching sessions will strengthen your role as DPO
- "Task Force": To handle a surge in activity (e.g., a major project or post-audit remediation), we'll produce your deliverables (AIPD, policies, audits) to boost productivity.
- Mock Audit: We'll verify the robustness of your system ahead of an external audit and provide you with a detailed report