Course : Data governance and regulatory compliance

RGPD, NIS2, DORA, IA Act, CRA
Seminar - 2d - 14h00 - Ref. GND
Price : 2120 CHF E.T.

NEW

Against a backdrop of accelerated digital transformation and tougher European regulations (RGPD, NIS2, DORA, IA Act, Cyber Resilience Act), executives are more than ever in the front line of ensuring their organization's compliance. This strategic seminar is aimed at members of general management and executive committees wishing to integrate data governance and cybersecurity issues into their decision-making.

Teaching objectives

At the end of the training, the participant will be able to:

- Understand the business, financial, HR and governance challenges of RGPD and regulatory compliance.
- Identify management's data protection and cybersecurity responsibilities
- Arbitrate projects with regulatory risks or ethical impacts (AI, outsourcing, cloud, etc.).
- Integrating compliance into strategic choices and business models
- Use steering tools and indicators to communicate effectively with business lines and support functions
- Setting risk acceptance and requirement levels

Intended audience
CIOs and CIOs, strategic managers of cloud, data, AI, CSR activities.

Prerequisites
No

Practical details
Case study
Presentations illustrated by real cases (case law, sanctions, press).

Course schedule

1 Data governance, regulation and strategic alignment

- Why is compliance an issue for senior management?
- Compliance is not an end in itself, but a lever for steering and arbitration.
- As with quality, CSR or finance, the manager sets the compliance cursor.
- Business impact: loss of contracts, exclusion from tenders, brand damage.
- Direct responsibility of the manager (RGPD, duty of care, cyber attacks).
- Legal representative of the data controller: non-delegable criminal liability.
- Examples of criminal convictions (articles 226-16 to 226-24 of the French Penal Code, CNIL sanctions).

2 Managing data governance

- Set up a data/processing governance committee.
- Provide the DPO with human and budgetary resources and direct access to management.
- Role of business departments in RGPD responsibility.
- Arbitrate conflicts: marketing versus safety, HR versus innovation, etc.

3 Anticipating emerging regulations

- Overview of regulations with strategic impact: NIS2, DORA, CRA, IA Act, Data Act.
- Examples of effects on value chains: suppliers, customers, subsidiaries.
- Use cases: sovereign cloud, generative AI, resilience management.

4 Positioning the RGPD as a transformation lever

- Compliance by design: integration into digital strategy.
- Competitive benefits: transparency, trust, differentiation.
- Develop a responsible data culture.

5 Steering, arbitration and crisis management

- Managing compliance: metrics and indicators for managers.
- Risk mapping and associated budgets.
- Key indicators to monitor: processing register, DPIA, data breaches, audits, training.
- Manager's responsibility for keeping the register and carrying out PIAs.
- Dialogue with the DPO, CISO and business managers.

6 Arbitrating critical projects

- Launching an AI project: what questions should you ask?
- Outsourcing or cloud: control, auditability, reversibility.
- Sensitive HR processing: how vigilant should you be?

7 Managing a compliance crisis (breach, cyber-attack, litigation)

- Management response to incidents.
- Coordinated management with legal, communications, IT.
- Post-crisis best practices: avoiding the double penalty (legal, reputation).

Dates and locations

REMOTE CLASS
2026 : 29 June, 14 Sep., 7 Dec.