Luxgap
DATA PRIVACY PARTNER

EMPOWERING TRUST!

Compliance & Cybersecurity

Master your obligations, secure your growth.

LuxGap is the trusted partner for businesses with high standards in regulatory compliance and cybersecurity. With expertise and a comprehensive, human-centered approach, LuxGap simplifies data governance while strengthening IT security.

2025

Luxgap
DATA PRIVACY PARTNER

Contact:

2 Rue de l'école | L-8376 Kahler
+352 621 583 116

contact@luxgap.com

Visit our website
for more information
www.luxgap.com

Areas of Expertise Summary

Our operational services

LuxGap offers a comprehensive range of services, organized into four main operational categories to address your regulatory compliance and digital security challenges with precision.

Governance and Regulatory Compliance

- Drafting of internal policies
- GDPR, NIS2, AI Act, etc. audits
- Assistance during inspections/audits by competent authorities

Tailored Compliance Implementation

- Outsourced CISO (Chief Information Security Officer) function
- Proactive cyber threat monitoring
- Implementation and follow-up of operational resilience plans (DORA, CRA)

Data Protection and International Data Flow Management

- Data flow mapping
- Secure management of international data transfers
- Conducting Data Protection Impact Assessments (PIA)

Employee Training and Awareness

- General or role-specific training
- Short e-learning modules
- Awareness sessions on incident management and whistleblower protection

EXTERNAL CISO

Secure your information systems with an outsourced Chief Information Security Officer (CISO).

- ✓ Implement an effective cybersecurity strategy
- ✓ Identify and manage risks related to cyberattacks
- ✓ Ensure compliance with standards (ISO 27001, NIS2, etc.)
- ✓ Raise awareness and train your employees

EXTERNAL DPO

Ensure your GDPR compliance with an outsourced Data Protection Officer (DPO).

- ✓ Audit and bring your company into compliance
- ✓ Manage risks related to personal data
- ✓ Oversee relationships with your subcontractors
- ✓ Train and raise awareness among your teams on data protection

EXTERNAL CAIO

Integrate AI into your strategy with an outsourced Chief Artificial Intelligence Officer (CAIO).

- ✓ Develop an AI strategy
- ✓ Identify relevant use cases for artificial intelligence
- ✓ Oversee ethics, governance, and compliance of AI projects
- ✓ Support your teams in building AI skills
- ✓ Assess risks related to automation

Anticipate.
Support.
Secure.

Our vision

Every year, new regulations emerge, new threats arise, and businesses must navigate increasing complexity. We founded LuxGap to meet this challenge: to offer a comprehensive, high-end, and resolutely proactive approach that does not merely react, but anticipates.

Our strength lies in our ability to combine legal expertise, strategic vision, and technological mastery. As trusted partners, we are committed to transforming what is often seen as a constraint—regulatory compliance—into a true competitive advantage for our clients.

We believe in elegant compliance, seamlessly integrated into business strategy without hindrance. We also believe in the importance of human-centered cybersecurity: accessible, understandable, and serving performance.

I am proud of the path LuxGap has taken, and above all, of the trust our clients across Europe place in us. Together, let us continue building a safer, more transparent, and more responsible digital world.

"We have helped numerous companies turn their GDPR compliance into a measurable business advantage."

GDPR General Data Protection Regulation

The GDPR is the legal foundation for personal data protection within the European Union, safeguarding citizens' fundamental rights. It defines the principles, obligations, and rights governing the processing of personal data.

Key Steps for GDPR Compliance:

1. Training and Awareness:

- → Organize general training sessions for employees.
- → Offer role-specific training to raise awareness of new data management policies and practices.
- → Provide micro-trainings of 3–5 minutes via an e-learning platform.

2. Data Analysis:

- → Identify the personal data processed in each department/service.
- → Establish a processing register with an appropriate data retention policy.
- → Conduct a legitimate interest assessment for relevant processing activities.

3. Transparency and Information:

- → Draft a general personal data protection policy.
- → Inform employees, clients, prospects, and other stakeholders about data processing and their rights through specific notices (website, recruitment, employees, etc.).

4. Personal Data Security:

- → Assess existing risks and test current security measures.
- → Propose and implement organizational and technical measures based on identified risks.
- → Document and explain measures in a quality assurance plan, including TOMs (Technical and Organizational Measures).

5. Data Subject Rights:

- → Be able to identify and respond to requests to exercise rights (access, rectification, deletion, etc.).
- → Establish a clear procedure for managing such requests.
- → Document and track requests to ensure timely handling within legal deadlines.

6. Data Protection Impact Assessment (DPIA):

- → Identify processing activities requiring a DPIA based on legal criteria.
- → Document the decision to carry out—or not—a DPIA for each processing activity.
- → Conduct analyses using tailored tools developed to assess risks to individuals' rights and freedoms.

Sectors concerned

All organizations operating in the EU

Companies handling personal data (EU)

7. Data Breach Management:

- → Implement a procedure for managing data breaches, including incident documentation.
- → Prepare a business continuity plan to react effectively in times of crisis.
- → Train teams to respond quickly in the event of a data leak.

8. International Data Transfers:

- → Identify personal data transfers outside the EU/EEA.
- → Draft and implement procedures to govern these transfers in line with regulatory requirements.

OUR SERVICES

1. Creation of data flow maps and detailed audits.
2. Conducting DPIAs tailored to your activities.
3. Development of specific GDPR policies, including data subject rights management.
4. Assistance during inspections or audits by competent authorities
5. Practical training for your teams on GDPR obligations and daily data management.
6. Custom tools to manage impact analyses and international data transfers.

BENEFITS

1. Reduced financial and reputational risks related to non-compliance.
2. Enhanced company value with clients and partners through ethical data management.
3. Improved resilience to new regulatory obligations.
4. Implementation of sustainable and adaptable data governance.

NIS2 Network and Information Security Directive 2

The NIS2 Directive (Network and Information Security) aims to strengthen the resilience and cybersecurity of networks and information systems within the European Union. It replaces the previous NIS Directive and introduces stricter, more harmonized requirements for affected organizations.

What needs to be done to comply with NIS2?

1. Governance and Risk Management:

- → Define clear cybersecurity policies.
- → Identify internal and external roles and responsibilities (including subcontractors).

2. Technical and Organizational Measures:

- → Implement appropriate security controls (e.g., access management, data protection, incident detection).
- → Ensure resilience of critical infrastructures through redundant systems.

3. Incident Notification:

- → Report any major incident to the competent authority within 24 hours.

4. Audit and Compliance:

- → Conduct regular internal and external audits to ensure compliance with applicable standards.

5. Training and Awareness:

- → Train employees and integrate third-party partners into the cybersecurity strategy.

OUR SERVICES

1. Initial Analysis and Assessment:

- → dentification of essential or important entities using specific assessment tools such as provided matrices and tables.
- → Risk and impact level evaluation (high, medium, low).

2. Compliance Implementation:

- → Drafting internal policies aligned with NIS2.
- → Implementing appropriate technical measures (multi-factor authentication, vulnerability detection).

3. Outsourced Services:

- → CISO as a Service function for continuous governance.
- → Management of compliance audits and preparation of reports for competent authorities.

Critical infrastructures | Energy | Transport | Health | Finance | Water

Digital services | Cloud infrastructure | Data centers & hosting | Online platforms

Specific industries | Agri-food | Chemicals | Waste management

Other critical sectors | Postal services and messaging providers | Public services

Electronic communications | Critical technology manufacturers

Size criteria for the entities concerned | > 50 employees | Turnover or Balance sheet: > €10M

These entities are systematically concerned, provided they operate in a sector covered by the directive.

Levels of Application

→ The obligations imposed by NIS2 are defined according to the size, potential impact, and strategic importance of the entity concerned. Here are the four levels:

1. Micro-Entities:

→ Includes very small organizations (fewer than 10 employees or annual turnover below €2 million).
→ Limited applicability, except in high-risk sectors or in cases of critical involvement.

2. Important Entities:

→ Medium and large organizations playing a key role in critical sectors.
→ Enhanced governance and security obligations to mitigate significant incidents.

3. Essential Entities:

→ Large organizations with a critical impact on society, the economy, or national security.
→ Stricter regulation, including frequent audits and reinforced resilience measures.

4. Very High-Impact Entities:

→ Operators of infrastructures or services of national or European strategic importance.
→ Subject to the highest governance and security requirements, due to their disproportionate impact in the event of failure.

4. Training and Awareness:

→ E-learning training on NIS2 requirements and their practical application.
→ Raising awareness among internal teams and suppliers about the new obligations.

5. Incident Management:

→ Establishing an incident response plan in line with NIS2.
→ Support in incident notification and communication with stakeholders.

BENEFITS

LuxGap combines its expertise in governance and IT security to support businesses at every stage of their compliance journey, reducing risks while optimizing resources. We also provide automated, tailored tools for simplified monitoring of your obligations.

Whistleblower Protection Act
(Directive (EU) 2019/1937)

The Whistleblower Protection Act aims to safeguard anyone reporting violations of EU law or national laws in a professional context. It establishes safe and confidential reporting mechanisms while preventing retaliation against whistleblowers.

What are the key obligations??

1. Establishment of Internal Reporting Channels

- → Creation of internal procedures to collect and handle reports confidentially.
- → Appointment of a designated person or team responsible for managing these reports.

2. Protection Against Retaliation

- → Formal prohibition of discriminatory or disciplinary measures against whistleblowers (unfair dismissal, demotion, intimidation, etc.).
- → Implementation of redress mechanisms in case of harm suffered by the whistleblower.

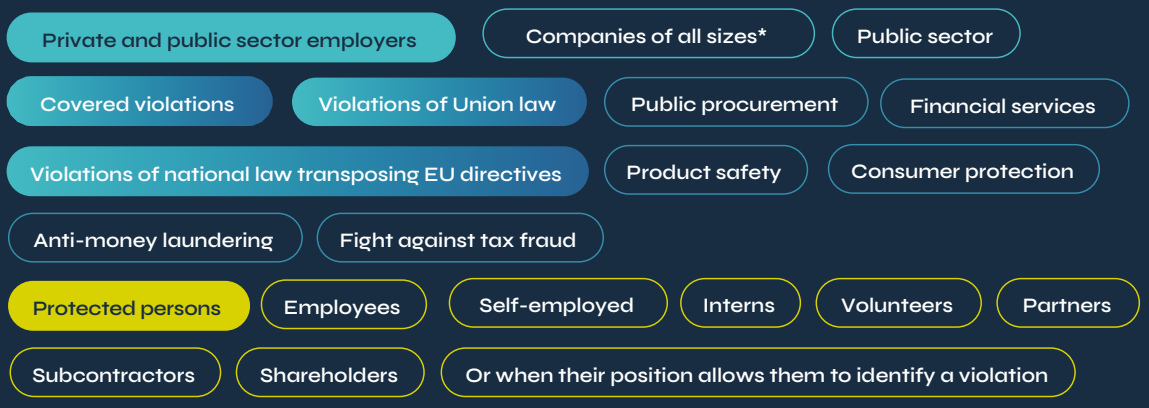
3. External Reporting Channels

- → Possibility for whistleblowers to turn to competent authorities or bodies when internal channels cannot be used or prove ineffective.

4. Information and Training

- → Raising employee awareness and providing clear procedures.
- → Training leadership and HR teams on handling reports and on the legal protection of whistleblowers.

The integration of an effective whistleblower protection policy is now both a regulatory and ethical imperative. LuxGap supports you at every stage—from assessing your current framework to training your teams—to ensure full compliance and foster a corporate culture of transparency and accountability.



*obligations are however adjusted according to the number of employees

OUR SERVICES

1. Audit and Compliance

→ Evaluation of internal procedures and HR policies to verify alignment with current legislation.
→ Development of secure, confidential reporting channels.

2. Drafting Internal Policies

→ Creation or revision of internal whistleblowing policies in line with Directive (EU) 2019/1937 and national law.
→ Integration of ethical charters and adapted codes of conduct.

3. Training and Awareness

→ Training sessions on whistleblower protection for all staff, including leadership, managers, and HR teams.
→ Availability of e-learning materials to explain best practices and legal obligations.

4. Case Management

→ Implementation of listening and support mechanisms for whistleblowers.
→ Partial or full outsourcing of the “reporting channel” function to ensure neutrality and confidentiality.

BENEFITS

1. Reduction of Legal and Reputational Risks

→ Minimizing litigation and sanctions related to the absence or mismanagement of reporting channels.

2. Strengthening Internal Trust

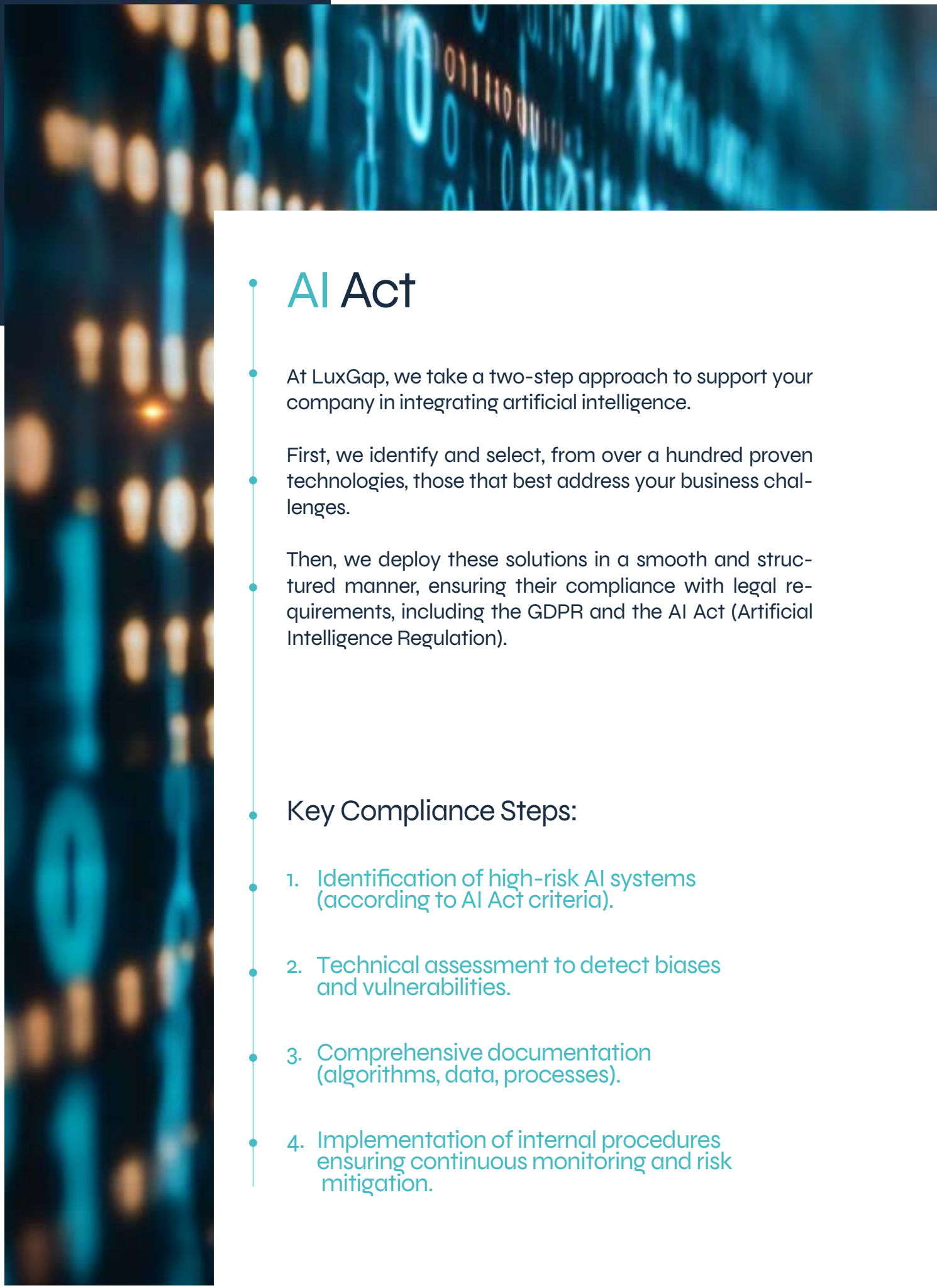
→ Promoting a culture of integrity and transparency, valuing everyone’s contribution to corporate compliance and ethics.

3. Improved Corporate Governance

→ Establishing more effective internal control mechanisms to quickly detect potential violations.

4. Alignment with European Best Practices

→ Reassurance for partners, investors, and regulators, demonstrating a clear commitment to meeting the highest standards of governance and whistleblower protection.



AI Act

At LuxGap, we take a two-step approach to support your company in integrating artificial intelligence.

First, we identify and select, from over a hundred proven technologies, those that best address your business challenges.

Then, we deploy these solutions in a smooth and structured manner, ensuring their compliance with legal requirements, including the GDPR and the AI Act (Artificial Intelligence Regulation).

Key Compliance Steps:

1. Identification of high-risk AI systems (according to AI Act criteria).
2. Technical assessment to detect biases and vulnerabilities.
3. Comprehensive documentation (algorithms, data, processes).
4. Implementation of internal procedures ensuring continuous monitoring and risk mitigation.

The upcoming AI Act aims to regulate artificial intelligence systems to ensure compliance with strict ethical and legal standards. It applies to any organization developing or using AI systems within the EU, particularly when these are considered “high-risk.”

OUR SERVICES

1. Comprehensive audit of AI systems to validate compliance (AI Act, GDPR).
2. Advanced analysis of algorithmic biases and ethical issues.
3. Support in documentation and drafting of compliance reports.
4. Strategic guidance to mitigate legal and reputational risks.

BENEFITS

Regulatory risk management and reduction of potential penalties.

1. **Responsible integration of AI into your processes, strengthening ethics and transparency.**
2. **Enhanced brand image and increased trust among your clients and partners.**

In summary, LuxGap supports you from selecting the most relevant AI technologies to implementing them in full compliance. This gives you access to comprehensive expertise that combines innovation with legal rigor, turning AI into a lasting asset for your competitiveness.

DORA Digital Operational Resilience Act

The DORA Regulation, adopted at the European level, aims to ensure strong digital operational resilience in the financial sector. It imposes standardized and harmonized requirements on financial institutions and critical stakeholders to reduce disruptions and strengthen the security of digital operations against cyber threats and technological disturbances.

What are the main obligations under DORA?

1. Mapping and Managing Technological Dependencies:

- → Identify all critical services, infrastructures, and providers.
- → Document interdependencies between financial operations and technological systems.

2. Implementation of Advanced Operational Resilience testing:

- → Conduct regular tests, such as cyberattack simulations, to assess system robustness.
- → Involve critical third parties (suppliers) in these tests.

3. Business Continuity and Incident Recovery Plans:

- → Develop plans to ensure continuity of digital operations in the event of disruptions.
- → These plans must cover cyber incidents, physical attacks, technical failures, and systemic crises.

4. Continuous Monitoring and Reporting:

- → Implement proactive monitoring systems to detect technological vulnerabilities.
- → Report major incidents to national regulators within strict deadlines.

5. Third-Party Risk Management:

- → Ensure that critical suppliers comply with security and resilience requirements.
- → Draft detailed contractual agreements defining cybersecurity responsibilities.

Financial institutions | Banks | Insurance companies | Asset management companies

Payment service providers | Investment funds | Infrastructures de marché | Clearing houses

Central securities depositories | Trading platforms | Payment infrastructures

Critical technology service providers | IT services | Cloud infrastructure

Cybersecurity for financial institutions

! These sectors are now subject to increased controls, including audits.

OUR SERVICES

LuxGap supports your organization at every stage of DORA compliance with tailored solutions:

1. **Assessment and Diagnosis**

→ Identification of critical systems and vulnerabilities in your technological infrastructures.
→ Initial evaluation of DORA compliance.

2. **Compliance Strategies:**

→ Development and implementation of policies and procedures aligned with DORA requirements.
→ Assistance with the implementation of advanced resilience tests and continuity plans.

3. **Simulations and Practical Testing:**

→ Execution of incident simulations (e.g., cyberattacks) to test the robustness of your systems.
→ Validation of your response and recovery capabilities.

4. **Documentation and Regulatory Monitoring:**

→ Preparation of clear and comprehensive reports to meet regulator requirements.
→ Ongoing updates of compliance records to maintain a high level of resilience.

BENEFITS

1. **Reduction of Operational Disruptions:**

→ Limiting the impact of technological failures and cyber incidents.
→ Maintaining continuity of critical financial services.

2. **Compliance with European Standards:**

→ Alignment with the EU's harmonized requirements, strengthening your position with regulators.

3. **Strengthening Partner Trust:**

→ Assurance of strong technological resilience, increasing the confidence of investors, clients, and financial partners.

4. **Preparedness for Cyber Risks:**

→ Better anticipation and response to emerging threats, ensuring a proactive stance on technological risks.

CRA Cyber Resilience Act

Sectors Concerned – Digital Products

Manufacturers | Importers | Distributors

Key Steps to Comply with the CRA:

1. Risk Assessment of Marketed Digital Products
2. Implementation of Security Measures from the Design Phase
3. Documentation of Security Tests and Safeguards Implemented
4. Continuous Monitoring of Vulnerabilities and Security Updates

The Cyber Resilience Act sets security requirements for digital products to ensure their robustness against cyberattacks.

OUR SERVICES

1. Audit of digital products to identify vulnerabilities.
2. Assistance with CRA compliance.
3. Guidance on best practices in product security.

BENEFITS

1. Enhanced security of digital products.
2. Reduced risk of vulnerabilities and exploitation.
3. Strengthened trust from users and partners.

DSA Digital Services Act

Sectors Concerned | Service Providers | Online Platforms | Search Engines

The Digital Services Act aims to regulate digital platforms to ensure a safe and transparent online environment.

Key Steps to Comply with the DSA :

1. Implementation of content moderation mechanisms.
2. Transparency regarding the recommendation algorithms used.
3. Management of notifications and reports of illegal content.
4. Publication of regular reports on moderation practices.

OUR SERVICES

1. Support in achieving compliance with the DSA.
2. Development of content moderation mechanisms.
3. Training teams on regulatory obligations.
4. Reporting and documentation for competent authorities.

BENEFITS

1. Enhanced security of digital products.
2. Reduced risk of vulnerabilities and exploitation.
3. Strengthened trust from users and partners.

Data Act

The Data Act, adopted by the European Union, aims to establish a legal framework to regulate access to, sharing, and use of non-personal data between businesses, consumers, and public entities. Its main objective is to foster a fair, transparent, and competitive data economy while respecting the rights of the parties involved.

OBJECTIVES

1. **Promote Fair Data Sharing:**

→ Prevent abuse of dominant positions by actors holding massive volumes of data.
→ Ensure fair access to data for SMEs and startups.

2. **Encourage Cross-Sector Innovation:**

→ Enable the use of data beyond industrial and organizational boundaries, creating new economic opportunities.

3. **Ensure Transparency and Protection of Rights:**

→ Define clear rules on access, portability, and security of shared data.

What are the key obligations under the Data Act?

1. Identification and Classification of Data:

→ Inventory non-personal data used, shared, or exchanged, distinguishing sensitive business data from other types of data.

2. Drafting Data-Sharing Contracts:

→ Draft clear, compliant contracts specifying access rights, responsibilities, and conditions of use.
→ Ensure protective clauses against misuse or unauthorized reuse.

3. Implementation of Technical and Interoperability Standards:

→ Adapt systems and digital tools to ensure smooth and secure data exchange between different actors.
→ Apply recognized standards to facilitate technical interoperability.

4. Data Documentation and Governance:

→ Maintain a register of sharing practices, involved partners, and established contracts.
→ Set up internal governance to monitor sharing practices and ensure compliance.

5. Access Mechanisms for the Public Sector:

→ Provide specific procedures to respond to legitimate requests from public authorities, particularly in cases of force majeure or public interest.

Private Companies

Any entity that collects, generates, uses, shares, or monetizes non-personal data, including data from the Internet of Things (IoT), industrial production, or digital services.

Examples: smart machine manufacturers, digital platforms, logistics operators.

Public Sector

Public bodies requesting access to private data for specific needs.

Examples: research, public health, or emergency situations.

Data Service Providers

Data intermediation platforms, data analytics providers, or any actor offering services based on the use of non-personal data.

OUR SERVICES

LuxGap supports companies and public institutions at every stage of their Data Act compliance with tailored solutions:

1. **Strategic Consulting and Initial Assessment:**

→ Identification of relevant data and evaluation of current sharing practices.
→ Analysis of legal and technical risks associated with data exchange.

2. **Development of Compliant Contracts and Policies:**

→ Drafting of data-sharing contracts in line with Data Act requirements.
→ Assistance in creating internal data governance policies.

3. **Technical and Legal Implementation:**

→ Implementation of technical standards for data interoperability and security.
→ Assistance in managing access requests from the public sector or third parties.

4 **Simulations and Audits:**

→ Conducting audits to evaluate compliance and robustness of data management systems.
→ Running scenario simulations to test sharing and response procedures.

BENEFITS

1. **Optimal and Secure Use of Data:**

→ Maximizing the economic value of data while complying with regulatory frameworks.

2. **Improved Cross-Sector Cooperation:**

→ Building strong relationships with business partners through clear and secure data-sharing practices.

3. **Reduction of Legal and Reputational Risks:**

→ Ensuring compliance with European legislation, thereby reducing the risk of disputes or sanctions.

4. **Competitive Positioning:**

→ Facilitated access to innovation opportunities through smooth and compliant data sharing.

DGA Data Governance Act

The Data Governance Act (DGA), adopted at the European level, aims to establish a legal framework that facilitates secure, transparent, and responsible data sharing. It sets out clear mechanisms and standards to encourage data-driven innovation while respecting the rights of stakeholders.

OBJECTIFS

1 **Promote the Reuse of Public and Private Data:**

→ Enable companies and public bodies to make their data available within a secure and legal framework.

2. **Create Standardized Governance Mechanisms:**

→ Facilitate collaborations between public and private actors through harmonized processes.

3. **Promote Transparency and Security:**

→ Strengthen trust in data sharing through clear rules on access, authorization, and data management.

What are the main objectives of the DGA?

1. Structuring Internal Data Governance:

→ Establish clear policies and processes to manage, classify, and structure data to be shared or reused.
→ Appoint a dedicated person or team responsible for data governance.

2. Compliance with Authorization Mechanisms:

→ Adopt authorization processes to ensure data is shared in compliance with stakeholder rights.
→ Ensure sensitive or confidential data is protected against unauthorized use.

3. Documentation of Sharing and Reuse Processes:

→ Maintain full traceability of exchanged data, involved partners, and sharing conditions.
→ Use clear contracts that comply with DGA requirements.

4. Collaboration with Public and Private Partners:

→ Establish strategic partnerships to maximize the value of data while respecting regulatory obligations.
→ Integrate technical standards for interoperability and secure exchanges.

5. Implementation of Data Altruism Mechanisms:

→ Provide data for projects of general interest within the framework set by the DGA.

Private companies

Organizations holding high-value data, such as industrial, environmental, or health data, and wishing to share or monetize it within a secure framework.

Examples: manufacturers, technology companies, digital service providers.

Public sector

Institutions holding non-personal data that can be reused for the development of innovative services or research projects.

Examples: geospatial, environmental, statistical data, or data from public research.

Data intermediation service providers

Platforms facilitating the exchange or monetization of data between parties within a secure and neutral framework.

Data Altruism Organizations

Actors sharing data for purposes of general interest, such as medical research or environmental projects.

OUR SERVICES

LuxGap provides comprehensive support to ensure compliance with the DGA and to optimize data-sharing opportunities:

1. **Structuring Data Governance:**

→ Assistance in creating internal data governance policies.
→ Organizing processes to ensure effective and compliant data management.

2. **Compliance with Authorization Mechanisms:**

→ Development of robust mechanisms to protect sensitive data.
→ Drafting data-sharing and authorization contracts in line with DGA standards.

3. **Support in Public-Private Collaboration:**

→ Establishment of strategic partnerships while respecting transparency and security rules.
→ Integration of the necessary technical standards for smooth and secure exchanges.

4. **Managing Data Altruism:**

→ Assistance in structuring data-sharing initiatives for purposes of general interest.

BENEFITS

1. **Improved transparency and data governance:**

→ Strengthening partner and stakeholder trust in data management.

2. **Maximization of business opportunities:**

→ Leveraging data within a secure framework to generate new economic opportunities.

3. **Reduction of legal and reputational risks:**

→ Ensuring compliance with European requirements, minimizing the risk of sanctions.

4. **Boosting innovation and public interest:**

→ Participation in collaborative projects for innovative applications or societal goals.

DMA Digital Markets Act

The Digital Markets Act (DMA) aims to limit anti-competitive practices in digital markets by imposing strict rules on digital platforms that act as "gatekeepers." Its objective is to promote fair competition, encourage innovation, and protect the rights of businesses and consumers.

What are the key obligations under the DMA?

1. Identification of specific obligations

- → Compliance with positive obligations such as transparency in digital advertising and data portability.
- → Prohibition of abusive practices such as:
  - Favoring their own services.
  - Preventing business users from offering different prices or conditions on other platforms.
  - Forcing the use of certain ancillary services (e.g., internal payment systems).

2. Alignment of business practices

- → Review of contracts and terms of use to eliminate anti-competitive clauses.
- → Adjustment of business practices to comply with the new rules.

3. Documentation and transparency

- → Implementation of internal mechanisms to monitor compliance.
- → Sharing relevant information with regulators and stakeholders.

4. Collaboration with regulatory authorities

- → Cooperation during audits and investigations. Proactive notification of changes that may affect DMA compliance.

THE "GATEKEEPERS" TARGETED BY THE DMA MEET THE FOL-LOWING CRITERIA:

1. **Significant size in the internal market:**

→ Annual EU turnover exceeding €7.5 billion or a market valuation of more than €75 billion.
→ Operation of a platform service with at least 45 million monthly active end users and 10,000 yearly active business users.

2. **Control over market access:**

→ Platforms considered "gatekeepers" are those acting as unavoidable intermediaries between businesses and consumers.

3. **Durable market position:**

→ Maintenance of the above thresholds for at least three consecutive years.

Examples of covered services: search engines, online marketplaces, social networks, operating systems, cloud services, online advertising.

OUR SERVICES

LuxGap provides specialized support to help digital platforms effectively comply with DMA obligations:

1. **Compliance audit:**

→ Assessment of current business practices to identify gaps with DMA obligations.
→ Analysis of platform contracts and terms of use.

2. **Assistance in implementing obligations:**

→ Support in adapting business practices.
→ Development of internal mechanisms to ensure transparency and compliance.

3. **Managing relations with regulatory authorities:**

→ Support in preparing responses to audits and compliance reports.
→ Representation with regulators to minimize sanction risks.

BENEFITS

1. **Reduction of risks related to sanctions**

→ Avoidance of fines that can reach up to 10% of annual global turnover in case of non-compliance.

2. **Compliance with market expectations**

→ Competitive positioning through proactive compliance.

3. **Strengthening reputation**

→ Improved trust from users, business partners, and regulators.

Regulation on the Free Flow of Non-Personal Data

The Regulation on the Free Flow of Non-Personal Data aims to ensure the free movement of data within the European Union while strengthening security and interoperability. It eliminates unjustified data localization restrictions and optimizes cross-border digital operations.

What are the obligations under the regulation?

1. Identification of relevant non-personal data:

→ Classification of non-personal data used or stored (e.g., machine data, statistical analyses, business data).

2. Development of internal policies:

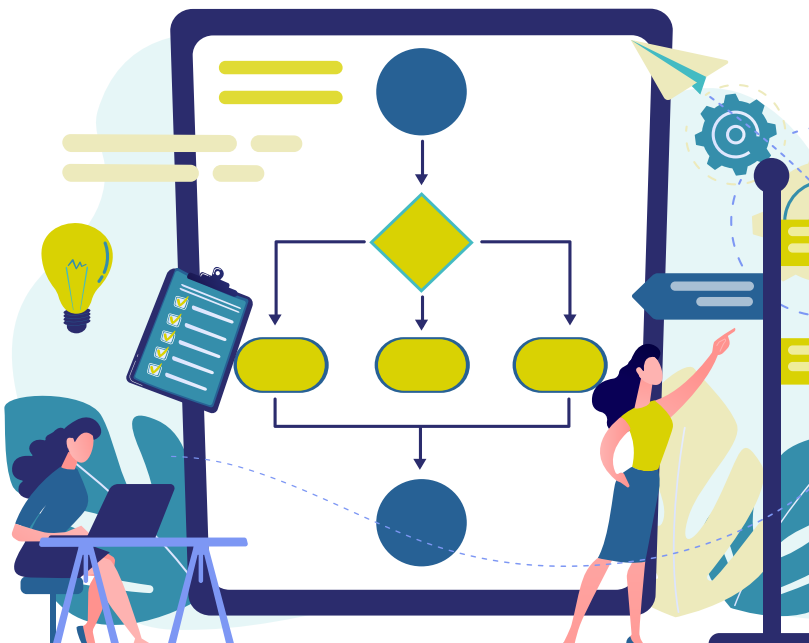
→ Creation of policies on data processing and security, including continuity plans in case of incidents.

3. Mechanisms for data portability:

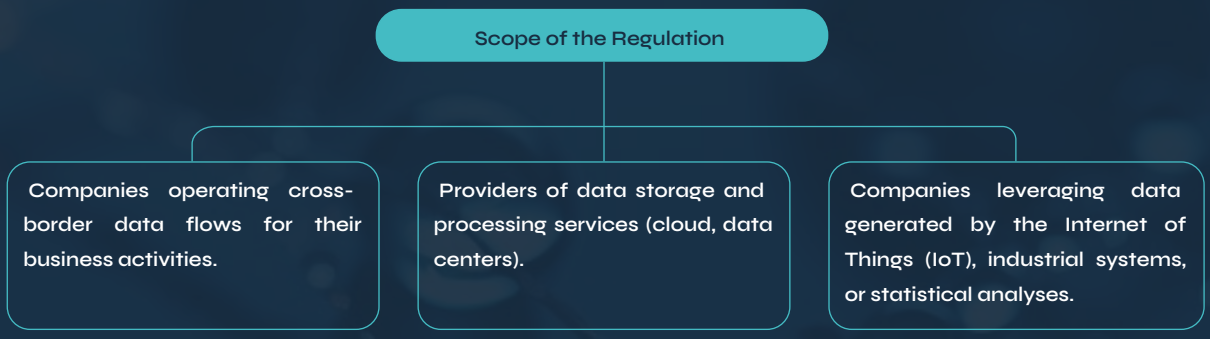
→ Implementation of tools allowing smooth transfer of data between service providers and EU member states.

4 Documentation of cross-border data flows:

→ Full traceability of data flows between countries to ensure compliance with localization and security requirements.



THE REGULATION APPLIES TO ANY ORGANIZATION PROCESSING OR STORING NON-PERSONAL DATA WITHIN THE EU...



OUR SERVICES

LuxGap supports organizations in managing and ensuring compliance with the Free Flow of Non-Personal Data regulation:

1. **Strategic consulting:**

→ Analysis of cross-border data flows and potential local restrictions.
→ Optimization of internal data management policies.

2. **Technical and legal compliance:**

→ Development of mechanisms to guarantee data security and interoperability.
→ Assistance in implementing compliant processing and hosting contracts.

3. **Operational support:**

→ Help in optimizing data flows to reduce costs and increase operational efficiency.

BENEFITS

1. **Simplification of operational processes:**

→ Unrestricted access to cloud services and data processing solutions within the EU.

2. **Reduction of technical and legal constraints:**

→ Elimination of obstacles related to data localization.

3. **Cost optimization:**

→ Reduced expenses for data management and storage through unified practices.

The eIDAS Regulation establishes a legal framework for electronic identification and trust services in the European Union. Its objective is to ensure secure and reliable digital interactions between citizens, businesses, and public authorities.

eIDAS Electronic Identification and Trust Services Regulation

What are the key obligations under the eIDAS Regulation?

1. Assessment of needs in electronic identification and trust services:

→ Identify the use cases of eIDAS solutions in digital interactions (online transactions, electronic signatures).

2. Implementation of compliant solutions:

→ Integrate technical solutions meeting eIDAS standards, such as qualified electronic signatures or electronic seals.
→ Ensure interoperability of identification systems with those of other EU member states.

3. Training of end users:

→ Train employees and users to ensure effective adoption of deployed solutions.

4. Documentation and audits:

→ Document processes and policies related to trust services to respond to regulators in case of inspection.

Qualified trust service providers

Electronic signature

Timestamping

Electronic seal

Website authentication certificates

Organizations using electronic identification systems

Companies

Public institutions

Certification authorities

Entities issuing electronic certificates guaranteeing the identity of signatories

OUR SERVICES

1. **Audit and compliance of eIDAS solutions:**

→ Assessment of current practices to identify gaps with eIDAS requirements.
→ Recommendations to achieve compliance.

2. **Support in integrating trust services:**

→ Assistance with the implementation of services such as qualified electronic signatures and website authentication certificates.

3. **Team training:**

→ Training sessions to ensure effective and compliant use of eIDAS tools.

BENEFITS

1. **Strengthening security:**

→ Enhanced protection of digital transactions and reduced risk of fraud.

2. **Reduction of legal risks:**

→ Compliance with a clear and harmonized regulatory framework across the EU.

3. **Increased trust of end users:**

→ Improved perceived reliability among partners, clients, and regulators.

ePrivacy Regulation

The ePrivacy Regulation complements the GDPR by specifically regulating the confidentiality of electronic communications and the processing of related data. Its aim is to protect users' rights while promoting transparent and ethical business practices.

What are the key obligations under the ePrivacy Regulation?

1. Compliance in data collection practices:

→ Adapt data collection practices related to electronic communications to meet confidentiality requirements.

2. Development of cookie and consent policies:

→ Implement compliant cookie banners and policies with clear consent management.

3. Team training:

→ Raise awareness among marketing and IT teams about the specific rules for processing electronic data.

4. Documentation and proof of compliance:

→ Maintain records of data processing practices to demonstrate compliance during audits.

5. Implementation of mechanisms for data altruism:

→ Provide data for projects of general interest within the framework set by the DGA.

OUR SERVICES

1. Compliance of digital marketing practices:

→ Audit of data collection and usage practices.
→ Implementation of compliant solutions for cookie and consent management.

2. Support in cookie and consent management:

→ Technical and legal assistance to develop compliant tools for managing trackers.

3. Team training:

→ Sessions on best practices for privacy and data processing.

Electronic communications service providers

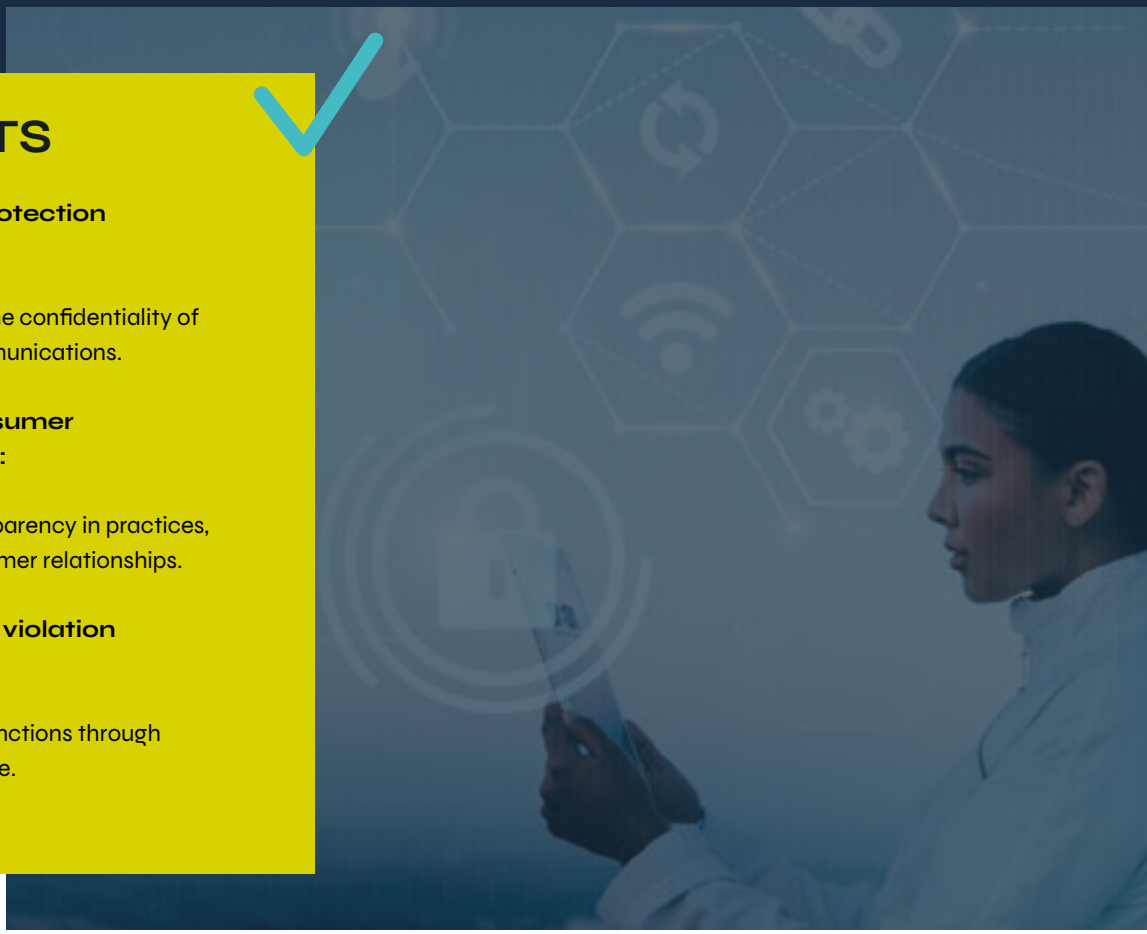
Telecom operators, online messaging platforms, and VoIP services.

Organizations processing metadata

Companies using data related to electronic communications for analysis or marketing.

Websites and applications

Actors using cookies, trackers, or other similar technologies to collect user information.



BENEFITS

1. **Enhanced protection of user data:**

→ Strengthening the confidentiality of electronic communications.

2. **Meeting consumer expectations:**

→ Increased transparency in practices, improving customer relationships.

3. **Reduction of violation risks:**

→ Avoidance of sanctions through strict compliance.

Luxgap
DATA PRIVACY PARTNER

NOW THAT YOU KNOW IT ALL...

WHAT IF COMPLIANCE BECAME YOUR STRATEGIC ADVANTAGE?

At LuxGap, we don't just help you tick regulatory boxes. We support you in gaining peace of mind, strengthening your credibility, and preparing for the future with confidence.

- ☑ Robust data governance
- ☑ Proactive cybersecurity
- ☑ International expertise serving your compliance
- ☑ A trusted partner, committed by your side
- ☑ Ready to take action?

Let's discuss your challenges. Together, we'll build an effective, clear, and sustainable compliance strategy.

+352 621 583 116
contact@luxgap.com ▪ www.luxgap.com

EMPOWERING TRUST!

CREDITS

TEXT : LUXGAP

DESIGN: PARASOL STUDIO

ILLUSTRATIONS & IMAGES: FREEPIK, ADOBE STOCK

Luxgap
DATA PRIVACY PARTNER

Contact:

2 Rue de l'école | L-8376 Kahler
+352 621 583 116

contact@luxgap.com

Visit our website
for more information:

www.luxgap.com