Luxgap

DATA PRIVACY PARTNER

Luxgap

Conformité • Cybersécurité • Résilience

Nous traduisons les exigences réglementaires en dispositifs opérationnels : gouvernance, outillage, preuves et pilotage continu. De la protection des données personnelles à la résilience numérique et l'encadrement de l'intelligence artificielle, Luxgap accompagne les organisations européennes sur l'ensemble de leurs obligations — avec pragmatisme, rigueur et indépendance.

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

VUE D'ENSEMBLE

Notre mission : sécuriser votre conformité, de bout en bout

Avec un paysage réglementaire en constante évolution — RGPD, NIS2, DORA, AI Act, lanceur d'alerte — les organisations doivent démontrer non seulement leur conformité formelle, mais aussi leur capacité opérationnelle à protéger les données, gérer les risques cyber et assurer la continuité de leurs activités. Luxgap se positionne comme un partenaire de confiance pour orchestrer cette mise en conformité globale.

RGPD / DPO

Gouvernance des données personnelles, registre, droits, preuves et accountability

NIS2 & DORA / CISO

Cybersécurité, résilience opérationnelle, gestion des risques ICT et reporting

BCP / ISO 22301

Programme mensualisé de continuité d'activité : BIA, plans, exercices et amélioration continue

Lanceur d'alerte

Portail sécurisé, confidentialité, traçabilité et suivi des signalements

EEM / Surveillance

Surveillance Dark Web, fuites de données, identifiants compromis, usurpation de marque, surface d'attaque externe et Shadow IT

AI Act

Conformité au règlement (UE) 2024/1689 : classification des risques, gouvernance IA, documentation technique et obligations de transparence

Plateforme SIRH & E-Learning

Logiciel orienté salarié : RH, formation, IA, conformité et sécurité intégrées

Formats courts disponibles (diagnostic / cadrage) — formats longs sur demande (programme complet).

SYNTHÈSE

Tableau récapitulatif : nos services par cadre réglementaire

Ce tableau offre une vue consolidée de l'ensemble des services Luxgap, en les reliant aux obligations réglementaires européennes qu'ils adressent. Il permet aux décideurs d'identifier rapidement les prestations pertinentes selon leur périmètre d'assujettissement.

Service Luxgap	RGPD	NIS2	DORA	AI Act	Lanceur d'alerte
DPO externe / Assistance DPO	✅ Art. 37-39, 5, 24, 25, 28, 32	—	—	—	—
Registre, DPIA, droits des personnes	✅ Art. 30, 35, 15-22	—	—	—	—
Clauses & due diligence sous-traitants	✅ Art. 28	✅ Art. 21	✅ Ch. V (risque tiers ICT)	✅ Art. 25 (chaîne de valeur)	—
CISO externe / Gouvernance sécurité	✅ Art. 32	✅ Art. 20-21	✅ Ch. II (ICT risk mgmt)	✅ Art. 9 (cybersécurité)	—
Plan incidents & reporting	✅ Art. 33-34	✅ Art. 23	✅ Ch. III (incident reporting)	✅ Art. 62 (incidents graves)	—
Tests de résilience (TLPT, exercices)	—	✅ Art. 21	✅ Ch. IV (tests)	✅ Art. 9, 15 (robustesse)	—
Surveillance Dark Web / EEM	✅ Art. 32	✅ Art. 21	✅ Ch. II	—	—
BCP / Continuité d'activité	—	✅ Art. 21	✅ Ch. II & IV	—	—
Portail lanceur d'alerte	✅ (traitement données)	—	—	—	✅ Dir. (EU) 2019/1937
Plateforme SIRH / E-Learning / IA	✅ Art. 5, 24, 25, 32	✅ (sensibilisation Art. 20)	✅ (formation Art. 13)	✅ Art. 4 (maîtrise IA), Art. 26 (déployeurs)	✅ (formation)
Gestion documentaire conformité	✅ Accountability	✅ Art. 21	✅ Ch. II	✅ Art. 11, 18 (documentation technique)	✅ Traçabilité
Conformité AI Act	✅ (DPIA IA, Art. 35)	—	—	✅ Règl. (UE) 2024/1689	—

✅ = service directement applicable au cadre réglementaire. Les références d'articles sont indicatives et varient selon le périmètre de l'organisation. Luxgap adapte ses prestations selon l'assujettissement réel de chaque client.

CHAPITRE 1

RGPD

Gouvernance et protection des données personnelles

RGPD

RGPD — Un programme de conformité structuré et démontrable

Le Règlement Général sur la Protection des Données impose aux organisations de démontrer activement leur conformité (*accountability*). Luxgap propose deux niveaux d'intervention complémentaires : un **mandat de DPO externe** pour les organisations souhaitant déléguer la fonction, ou une **assistance au DPO existant** pour renforcer ponctuellement les capacités internes. Dans les deux cas, notre objectif est clair : produire une conformité prête à démontrer, à tout moment, face à une autorité, un client ou un audit.

Mandat DPO externe

- Pilotage intégral du programme RGPD
- Interface avec l'Autorité de contrôle et gestion des audits
- Avis et arbitrages documentés sur les traitements sensibles
- Réduction proactive du risque : amendes, incidents, atteinte à la réputation

Assistance au DPO

- Renfort ponctuel sur des projets spécifiques à enjeux (migration, nouveau produit, partenariat)
- Mise à jour continue des preuves de conformité
- Préparation aux contrôles des autorités et aux audits clients
- Accompagnement sur les DPIA et analyses de risques ciblées

RGPD

Ce que nous adressons : les piliers de la conformité RGPD

Notre approche couvre l'ensemble des exigences structurantes du règlement, depuis la cartographie des traitements jusqu'à la démonstration continue de conformité. Chaque pilier est conçu pour produire des preuves tangibles et auditables.

1

Maîtrise des traitements

Registre exhaustif, bases légales documentées, durées de conservation définies et appliquées. Ce socle constitue le fondement de toute démonstration de conformité (Art. 5, 6, 30).

2

Droits & transparence

Processus opérationnels pour répondre aux demandes d'exercice des droits (accès, rectification, suppression, portabilité) dans les délais légaux, avec traçabilité complète (Art. 15-22).

3

Sous-traitants & sécurité

Clauses contractuelles conformes, due diligence fournisseurs, encadrement des transferts hors UE et mesures de sécurité techniques et organisationnelles proportionnées (Art. 28, 32, 44-49).

4

Gouvernance & accountability

Rôles et responsabilités formalisés, comités de pilotage, processus décisionnels documentés et preuves consolidées pour démontrer la conformité à tout moment (Art. 5.2, 24, 25).

RGPD

Livrables : une conformité « prête à démontrer »

Nos livrables sont conçus pour être immédiatement exploitables et auditables. Ils constituent le socle documentaire et opérationnel de votre programme RGPD, que ce soit dans le cadre d'un diagnostic initial (format court) ou d'un accompagnement complet.

Conformité « prête à démontrer »

- Cadre documentaire complet : politiques, procédures, rôles et comités
- Processus droits des personnes : réception, traitement, réponse, archivage
- Processus incidents : détection, qualification, notification, preuves
- Clauses contractuelles et due diligence sous-traitants
- Tableau de bord de pilotage : risques, actions, échéances, KPI

Livrables format court (diagnostic / cadrage)

- Diagnostic de maturité et feuille de route priorisée
- Registre des traitements structuré + modèles de politiques
- DPIA ciblées sur les traitements à risque avec recommandations actionnables
- Plan incidents et accompagnement à la mise en œuvre
- Cartographie des écarts et plan de remédiation

CHAPITRE 2

NIS2 & DORA

Gouvernance cybersécurité et résilience opérationnelle

NIS2 & DORA

NIS2 & DORA — Aligner gouvernance, technique et capacité de réaction

Les directives NIS2 et le règlement DORA imposent aux organisations essentielles, importantes et au secteur financier un niveau d'exigence sans précédent en matière de cybersécurité et de résilience opérationnelle. L'enjeu ne se limite pas à la mise en place de mesures techniques : il s'agit d'aligner la gouvernance, les contrôles, la gestion des incidents et la surveillance des tiers — avec des preuves auditables à chaque étape.

Luxgap propose un **mandat de CISO externe** ou une **assistance CISO** adaptée au périmètre de chaque organisation, couvrant la conformité initiale, les contrôles récurrents et le reporting aux autorités.

CISO externe

Stratégie et gouvernance sécurité, risk management et contrôles continus, animation des comités sécurité, définition des KPI et suivi des plans d'action. Le CISO externe agit comme un véritable directeur de la sécurité de l'information, intégré à votre gouvernance.

Programme NIS2

Scoping de l'entité et de ses activités essentielles/importantes, mise en place des mesures organisationnelles et techniques (Art. 21), plan de gestion des incidents avec reporting aux autorités (Art. 23), et gestion de la chaîne d'approvisionnement.

Programme DORA

ICT risk management (politiques, contrôles, documentation conforme au Ch. II), tests et exercices de résilience incluant TLPT selon le périmètre applicable (Ch. IV), et gestion du risque fournisseurs ICT avec registre des accords (Ch. V).

En option : cartographie des risques, SOC/monitoring, gestion des vulnérabilités, campagnes de sensibilisation, et préparation aux audits clients et autorités compétentes.

CHAPITRE 3

Business Continuity

Programme ISO 22301 mensualisé : analyse d'impact, stratégies de continuité, plans, exercices et amélioration continue

BCP

Business Continuity — Programme ISO 22301 mensualisé et clé en main

Luxgap propose un programme complet de continuité d'activité (BCP) aligné sur la norme ISO 22301. Déployé de manière progressive et facturé mensuellement, ce programme couvre l'ensemble du cycle de continuité d'activité : analyse d'impact, définition des stratégies, élaboration des plans, exercices pratiques et amélioration continue.

Analyse d'impact métier (BIA)

Identification des processus critiques, des objectifs de temps et de point de reprise (RTO/RPO), des dépendances et des scénarios de perturbation potentiels.

Stratégies de continuité

Définition des stratégies de reprise, des solutions alternatives et de l'allocation des ressources critiques pour maintenir les fonctions essentielles de l'entreprise.

Plans de continuité & gestion de crise

Rédaction des plans BCP/DRP détaillés, procédures de crise, chaînes d'escalade et communication pour une réponse coordonnée en cas d'incident.

Exercices & tests

Programme annuel d'exercices (tabletop, simulation, test réel), mesure de l'efficacité des plans et recueil des retours d'expérience pour ajustement.

Amélioration continue & audit

Revues périodiques, suivi des indicateurs de performance et préparation aux audits de certification ISO 22301 pour une résilience durable.

Un budget prévisible, un programme structuré : notre approche mensualisée permet de déployer progressivement la conformité ISO 22301 sans mobiliser un budget projet massif, tout en garantissant des livrables concrets à chaque étape.

CHAPITRE 4

Lanceur d'alerte

Portail sécurisé, confidentialité, traçabilité et gestion du dispositif

LANCEUR D'ALERTE

Lanceur d'alerte — Canal interne sécurisé et gestion complète du dispositif

La directive européenne (EU) 2019/1937 impose aux organisations de mettre en place un canal de signalement interne sécurisé, garantissant la confidentialité du lanceur d'alerte, la traçabilité des échanges et le suivi des actions correctives. Luxgap fournit un portail en ligne clé en main, associé à un accompagnement méthodologique pour garantir la conformité opérationnelle du dispositif.

Portail lanceur d'alerte (online)

- Canal de signalement interne (web) avec accusé de réception automatique dans les délais légaux
- Confidentialité renforcée et séparation stricte des rôles (instructeur, décisionnaire, DPO)
- Workflow complet : triage, échanges sécurisés avec le lanceur d'alerte, actions correctives, clôture
- Traçabilité intégrale : journal d'événements, preuves horodatées, respect des délais réglementaires
- Reporting anonymisé pour la gouvernance et les instances de contrôle

Mode d'engagement

01

Diagnostic rapide

Périmètre, obligations applicables, niveau de maturité actuel

02

Cadrage

Rôles, planning, indicateurs de suivi, preuves attendues

03

Mise en place

Politiques, processus, outillage technique, formations

04

Run

Surveillance, contrôles, gestion des incidents, audits

Option : externalisation du traitement des signalements (garantie d'indépendance) et articulation avec RGPD / sécurité pour une gestion cohérente des données sensibles.

CHAPITRE 5

AI Act

Conformité au règlement européen sur l'intelligence artificielle : classification, gouvernance, documentation et transparence

AI ACT

AI Act — Accompagnement structuré à la conformité du règlement (UE) 2024/1689

Le règlement européen sur l'intelligence artificielle (AI Act) est entré en vigueur le 2 août 2024 avec une application progressive jusqu'en août 2027. Il impose aux fournisseurs et déployeurs de systèmes d'IA une approche par les risques : pratiques interdites, systèmes à haut risque soumis à des obligations renforcées, et obligations de transparence pour tous. Luxgap accompagne les organisations dans la mise en conformité opérationnelle de leurs systèmes d'IA, de l'inventaire initial à la gouvernance continue.

Inventaire & classification des systèmes IA

Cartographie exhaustive des systèmes d'IA utilisés ou développés, classification selon les niveaux de risque (inacceptable, haut, limité, minimal), identification des obligations applicables par système.

Documentation technique & conformité

Rédaction de la documentation technique (Art. 11), évaluations de conformité, analyses d'impact sur les droits fondamentaux (Art. 27), articulation avec les DPIA RGPD existantes.

Gouvernance IA & organisation

Mise en place du cadre de gouvernance interne : rôles et responsabilités, politiques d'utilisation de l'IA, processus de validation avant déploiement, supervision humaine (Art. 14).

Transparence & information

Obligations d'information des utilisateurs (Art. 13, 50), marquage des contenus générés par IA (deepfakes, textes), registre des systèmes à haut risque, traçabilité des décisions automatisées.

Surveillance post-marché & amélioration continue

Monitoring continu des performances et des risques, gestion des incidents graves (Art. 62), mise à jour de la documentation, préparation aux audits et contrôles des autorités nationales.

Mode d'engagement

01

Diagnostic IA

Inventaire des systèmes, classification des risques, gap analysis

02

Cadrage

Plan de conformité, priorisation, gouvernance cible

03

Mise en œuvre

Documentation, processus, formation, outillage

ÇÇ

Run

Surveillance continue, incidents, audits, amélioration

Articulation RGPD / AI Act : lorsque des systèmes d'IA traitent des données personnelles, nous assurons la cohérence entre les obligations du règlement IA (documentation, transparence, supervision humaine) et celles du RGPD (DPIA, base légale, droits des personnes) — un accompagnement intégré pour éviter les doublons et les angles morts.

CHAPITRE 5

Plateforme SIRH

E-Learning, IA intégrée et écosystème sécurisé — notre logiciel orienté salarié ultra sécurisé

SIRH

Architecture globale : un SIRH sécurisé et modulaire

La plateforme ne constitue pas un simple outil de formation. Elle s'inscrit dans une architecture complète de type **SIRH** (Système d'Information des Ressources Humaines), intégrant gestion administrative, conformité réglementaire et intelligence artificielle dans un environnement hautement sécurisé. Cette approche unifiée transforme la plateforme en outil de **gouvernance transverse**, liant RH, conformité et sécurité opérationnelle.

Gestion RH complète

- Fiches de salaires et gestion administrative du personnel
- Gestion des congés, absences et planification
- Suivi contractuel et documentaire centralisé
- Portail collaborateur pour l'autonomie des salariés

Gestion de flotte automobile

- Attribution des véhicules et suivi des utilisateurs
- Suivi des contrats, assurances et échéances
- Documentation liée aux responsabilités employeur
- Alertes automatiques sur les renouvellements

Gestion documentaire de conformité

- Centralisation des politiques internes et procédures
- Registre des traitements et AIPD intégrés
- Gestion des sous-traitants et plans d'actions correctrices
- Suivi des audits avec piste d'audit complète

E-LEARNING IA

E-Learning intégré et Intelligence Artificielle

Module E-Learning

Le module de formation est intégré nativement à l'écosystème SIRH, permettant une gestion fluide des parcours de sensibilisation et de certification.

- **Capsules vidéo courtes** adaptées aux contraintes opérationnelles des collaborateurs
- **Questionnaires de validation** avec scoring et seuils de réussite configurables
- **Certification de suivi** avec attestations téléchargeables
- **Traçabilité probatoire** des parcours : données exportables pour les audits
- Invitations automatiques : l'employeur sélectionne les modules et transmet les emails

Intelligence Artificielle intégrée

L'IA agit comme un **assistant interne permanent**, intégré au cœur du SIRH pour renforcer la diffusion réglementaire et réduire les risques d'erreurs internes.

- **Réponses automatisées** aux questions des salariés sur les politiques internes et obligations réglementaires
- **Adaptation dynamique** aux évolutions légales et organisationnelles en temps réel
- **Support pédagogique interactif** intégré aux parcours de formation
- Diffusion homogène de l'interprétation réglementaire à travers toute l'organisation

SÉCURITÉ

Sécurité, conformité et audit indépendant ISAE 3000 Type 2

La plateforme a fait l'objet d'un **audit indépendant ISAE 3000 Type 2**, attestant de la conformité des contrôles de sécurité et de protection des données sur la durée. Cet audit constitue un gage de confiance pour les organisations soumises à des obligations strictes de due diligence sur leurs sous-traitants.

Information des personnes

Transparence complète sur les traitements réalisés

Sécurité des données

Mesures techniques et organisationnelles auditées

Minimisation

Collecte limitée au strict nécessaire

Gestion des droits

Processus d'exercice des droits opérationnels

Suppression des données

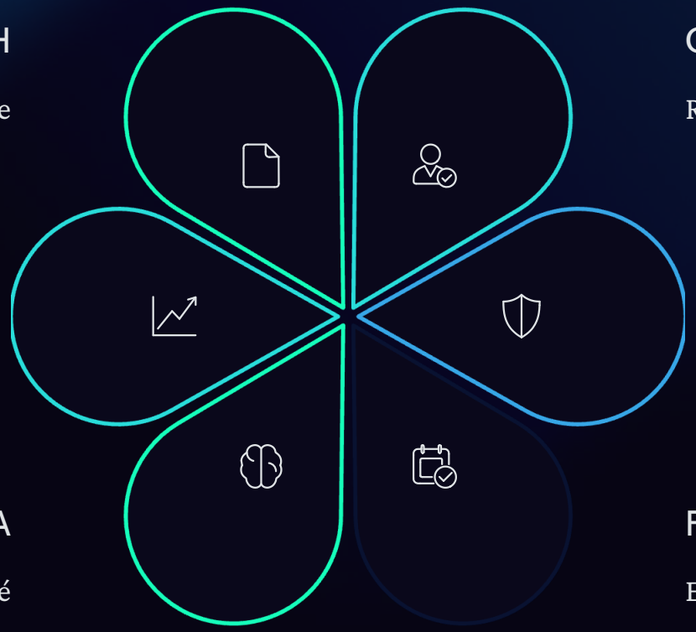
Purge automatisée selon les durées définies

Le traitement est encadré par un **registre spécifique** distinguant la fourniture du service et l'amélioration de la sécurité. L'environnement est conçu pour répondre aux exigences du **RGPD (Art. 5, 24, 25, 32)**, ainsi qu'aux obligations organisationnelles issues de **NIS2** et **DORA** lorsqu'applicables.

INTÉGRATION

Intégration complète et positionnement stratégique

La plateforme intègre l'ensemble des briques applicatives LuxApps pour constituer une **infrastructure numérique unifiée** combinant RH, conformité, sécurité, formation et intelligence artificielle. Elle offre à la direction une vision consolidée et sécurisée de l'ensemble des obligations organisationnelles.



RH

Gestion administrative complète

Conformité

Registre, AIPD, sous-traitants

Reporting

Pilotage exécutif en temps réel

Sécurité

Scanner vulnérabilités, contrôles

IA

Assistant réglementaire intégré

Formation

E-Learning et certification

Centralisation

Données RH et conformité unifiées

Risque réduit

Réduction du risque juridique

Traçabilité

Preuves probatoires des actions

Automatisation

Réponses réglementaires internes

NOTRE APPROCHE

Un mode d'engagement simple et éprouvé

Quel que soit le périmètre réglementaire — RGPD, NIS2, DORA ou lanceur d'alerte — notre méthodologie suit un cycle structuré en quatre phases. Ce cadre garantit une montée en conformité progressive, documentée et mesurable, adaptée à la maturité et aux ressources de chaque organisation.

1. Diagnostic

Évaluation rapide du périmètre, des obligations applicables et du niveau de maturité actuel. Identification des écarts critiques et des quick wins.

2. Cadrage

Définition des rôles, du planning, des indicateurs de suivi et des preuves attendues. Feuille de route priorisée et validée par la direction.

3. Mise en place

Déploiement des politiques, processus, outillage technique et formations. Production des premiers livrables auditables.

4. Run

Surveillance continue, contrôles récurrents, gestion des incidents, audits et amélioration continue du dispositif.

Formats courts disponibles (diagnostic / cadrage) — formats longs sur demande (programme complet par réglementation et par secteur).

Prochaines étapes — Contactez-nous

Vous souhaitez la version détaillée ? Nous disposons de formats longs — playbooks, modèles, preuves, programmes complets — par réglementation et par secteur.

Julien Winkin

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

Luxgap SARL

2 rue de l'école

L-8376 Kahler, Luxembourg

Conformité • Cybersécurité • Résilience — Nous traduisons les exigences réglementaires en dispositifs opérationnels.