Luxgap
DATA PRIVACY PARTNER

EMPOWERING TRUST!

Conformité & Cybersécurité

Maîtrisez vos obligations, sécurisez votre croissance.

LuxGap est le partenaire privilégié des entreprises exigeantes en matière de conformité réglementaire et de cybersécurité. Grâce à une expertise et une approche globale et humaine, LuxGap simplifie la gouvernance des données tout en renforçant la sécurité informatique.

2025

Luxgap
DATA PRIVACY PARTNER

Contact:

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

contact@luxgap.com

Visitez notre site web
pour plus d'informations :
www.luxgap.com

Domaines d'expertise

Sommaire

Nos services opérationnels

LuxGap propose une gamme complète de services, regroupés en quatre grandes familles opérationnelles afin de répondre précisément à vos enjeux de conformité réglementaire et de sécurité numérique.

Gouvernance et conformité réglementaire

- Rédaction de politiques internes
- Réalisation d'audits RGPD, NIS2, AI Act, etc.
- Assistance aux contrôles/audits par les autorités compétentes

Mise en Conformité sur mesure

- Fonction externalisée de CISO (Chief Information Security Officer)
- Surveillance proactive des cybermenaces
- Mise en place et suivi des plans de résilience opérationnelle (DORA, CRA)

Protection des données et gestion des flux internationaux

- Cartographie des flux de données
- Gestion sécurisée des transferts internationaux de données
- Réalisation d'Analyses d'Impact sur la Protection des Données (PIA)

Formations et sensibilisation des collaborateurs

- Formations générales ou spécifiques par métier
- Modules courts en e-learning
- Sensibilisation à la gestion des incidents et à la protection des lanceurs d'alerte

CISO EXTERNE

Sécurisez vos systèmes d'information avec un Chief Information Security Officer (CISO) externalisé.

- ✓ Mise en œuvre d'une stratégie "cybersécurité efficace"
- ✓ Identifier et gérer les risques liés aux cyberattaques
- ✓ Assurer la conformité aux normes (ISO 27001, NIS2...)
- ✓ Sensibiliser et former vos collaborateurs

DPO EXTERNE

Assurez votre conformité RGPD avec un Data Protection Officer (DPO) externalisé.

- ✓ Auditer et mettre en conformité votre entreprise
- ✓ Gérer les risques liés aux données personnelles
- ✓ Assurer l'encadrement avec vos sous-traitants
- ✓ Former et sensibiliser vos équipes à la protection des données

CAIO EXTERNE

Intégrez l'IA dans votre stratégie avec un Chief Artificial Intelligence Officer (CAIO) externalisé.

- ✓ Élaborer une stratégie IA
- ✓ Identifier les cas d'usage pertinents de l'intelligence artificielle
- ✓ Superviser l'éthique, la gouvernance et la conformité des projets IA
- ✓ Accompagner vos équipes dans la montée en compétence sur l'IA
- ✓ Évaluer les risques liés à l'automatisation

Anticiper.
Accompagner.
Sécuriser.

Notre vision

Chaque année, de nouvelles régulations voient le jour, de nouvelles menaces émergent, et les entreprises doivent composer avec une complexité croissante. Nous avons fondé LuxGap pour répondre à ce défi : proposer une approche globale, haut de gamme et résolument proactive, qui ne se contente pas de réagir, mais qui anticipe.

Notre force réside dans notre capacité à conjuguer expertise juridique, vision stratégique et maîtrise technologique. En tant que partenaires de confiance, nous avons à cœur de transformer ce qui est souvent perçu comme une contrainte — la conformité réglementaire — en un réel avantage compétitif pour nos clients.

Nous croyons en une conformité élégante, qui s'intègre naturellement à la stratégie d'entreprise, sans l'entraver. Nous croyons aussi à l'importance d'une cybersécurité humaine, accessible et compréhensible par tous, au service de la performance.

Je suis fier du chemin parcouru par LuxGap, et surtout de la confiance que nous accordent nos clients à travers l'Europe. Ensemble, continuons à bâtir un monde numérique plus sûr, plus transparent, et plus responsable.

"Nous avons accompagné de nombreuses entreprises à transformer leur conformité RGPD en avantage commercial mesurable"

RGPD Règlement Général sur la Protection des Données

Le RGPD constitue la base légale pour la protection des données personnelles au sein de l'Union européenne, garantissant les droits fondamentaux des citoyens. Il définit les principes, les obligations et les droits en matière de traitement des données personnelles.

Les étapes clés pour une mise en conformité RGPD :

1. Formation et sensibilisation :

- → Organiser des sessions de formation générale pour les collaborateurs.
- → Proposer des formations ciblées par métier pour sensibiliser aux nouvelles politiques et pratiques de gestion des données.
- → Mettre à disposition des micro-formations de 3 à 5 minutes via une plateforme e-learning.

2. Analyse des données :

- → Identifier les données personnelles traitées dans chaque département/service.
- → Établir un registre des traitements avec une politique de conservation des données adaptée.
- → Réaliser une évaluation de l'intérêt légitime pour les traitements concernés.

3. Transparence et information :

- → Rédiger une politique générale de protection des données personnelles.
- → Informer les collaborateurs, clients, prospects et autres parties prenantes sur le traitement de leurs données et leurs droits, par le biais de notices spécifiques (site internet, recrutement, employés, etc.).

4. Sécurité des données personnelles :

- → Évaluer les risques existants et tester les mesures de sécurité en place.
- → Proposer et mettre en œuvre des mesures organisationnelles et techniques basées sur les risques identifiés.
- → Documenter et expliquer les mesures via un plan d'assurance qualité, incluant les TOMs (Technical and Organizational Measures).

5. Droits des personnes :

- → Savoir identifier et répondre aux demandes d'exercice des droits (accès, rectification, suppression...).
- → Mettre en place une procédure claire pour la gestion des demandes.
- → Documenter et suivre les demandes reçues pour assurer leur traitement dans les délais légaux.

6. Analyse d'impact relative à la protection des données (AIPD) :

- → Identifier les traitements nécessitant une AIPD en fonction des critères légaux.
- → Documenter la décision de réaliser ou non une AIPD pour chaque traitement concerné.
- → Réaliser l'analyse à l'aide d'outils sur mesure développés pour évaluer les risques sur les droits et libertés des personnes.

Secteurs concernés

Toutes organisations opérant dans l'UE

Entreprises manipulant des données personnelles (UE)

7. Gestion des violations de données :

- → Mettre en place une procédure de gestion des violations de données, incluant la documentation des incidents.
- → Préparer un plan de continuité d'activité pour réagir efficacement en cas de crise.
- → Former les équipes à réagir rapidement en cas de fuite de données.

8. Transferts internationaux de données :

- → Identifier les transferts de données personnelles hors UE/EEE.
- → Rédiger et mettre en place des procédures pour encadrer ces transferts conformément aux exigences réglementaires.

NOS SERVICES

1. **Création de cartographies des flux de données et audits détaillés.**
2. **Réalisation de PIA adaptées à vos activités.**
3. **Développement de politiques RGPD spécifiques, incluant la gestion des droits des individus.**
4. **Assistance lors des contrôles ou audits par les autorités compétentes.**
5. **Formation pratique pour vos équipes sur les obligations RGPD et la gestion quotidienne des données.**
6. **Outils sur mesure pour gérer les analyses d'impact et les transferts internationaux de données.**

BÉNÉFICES

1. **Réduction des risques financiers et réputationnels liés aux non-conformités.**
2. **Valorisation de votre entreprise auprès de vos clients et partenaires grâce à une gestion éthique des données.**
3. **Amélioration de la résilience face aux nouvelles obligations réglementaires.**
4. **Mise en place d'une gouvernance des données pérenne et adaptable.**

NIS2 Network and Information Security Directive 2

La directive NIS2 (Network and Information Security) vise à améliorer la résilience et la cybersécurité des réseaux et des systèmes d'information dans l'Union européenne. Elle remplace la directive NIS précédente et introduit des exigences plus rigoureuses et harmonisées pour les organisations concernées.

Que faut-il faire pour se conformer à NIS2?

1. Gouvernance et gestion des risques :

- → Définir des politiques de cybersécurité claires.
- → Identifier les rôles et responsabilités internes et externes (y compris pour les sous-traitants).

2. Mesures techniques et organisationnelles :

- → Mettre en œuvre des contrôles de sécurité adaptés (ex. : gestion des accès, protection des données, détection des incidents).
- → Assurer la résilience des infrastructures critiques via des systèmes redondants.

3. Notification des incidents :

- → Signaler tout incident majeur à l'autorité compétente dans un délai de 24 heures.

4. Audit et conformité :

- → Effectuer régulièrement des audits internes et externes pour garantir la conformité aux normes applicables.

5. Formation et sensibilisation :

- → Former les employés et intégrer les partenaires tiers dans la stratégie de cybersécurité.

NOS SERVICES

1. Analyse et évaluation initiale :

- → Identification des entités essentielles ou importantes grâce à des outils d'évaluation spécifiques comme les matrices et tableaux fournis.
- → Évaluation des risques et des niveaux d'impact (haut, moyen, faible).

2. Mise en conformité :

- → Rédaction de politiques internes alignées sur NIS2.
- → Implémentation des mesures techniques adaptées (multi-factor authentication, détection des vulnérabilités).

3. Services externalisés :

- → Fonction de CISO as a Service pour une gouvernance continue.
- → Gestion des audits de conformité et préparation des rapports pour les autorités compétentes.

Infrastructures critiques | Énergie | Transport | Santé | Finances | Eau

Services numériques | infrastructure cloud | Centres de données & hébergement | Plateformes en ligne

Industries spécifiques | Agroalimentaire | Produits chimiques | Gestion des déchets

Autres secteurs critiques | Services postaux et Fournisseurs de messagerie | Services publics

communications électroniques | Fabricants de technologies critiques

Critères de taille pour les entités concernées | 50 employés ou +* | C.A ou Bilan : > 10M. €

* Ces entités sont systématiquement concernées, à condition d'opérer dans un secteur couvert par la directive.

Niveaux d'application

Les obligations imposées par NIS2 sont définies en fonction de la taille, de l'impact potentiel et de l'importance stratégique de l'entité concernée. Voici les quatre niveaux :

1. Micro-Entités :

- → Comprend les organisations de très petite taille (moins de 10 employés ou chiffre d'affaires annuel inférieur à 2 millions d'euros).
- → Applicabilité limitée, sauf dans des secteurs à haut risque ou en cas d'implication critique.

2. Entités Importantes :

- → Moyennes et grandes organisations jouant un rôle clé dans des secteurs critiques.
- → Obligations de gouvernance et de sécurité renforcées pour atténuer les incidents significatifs.

3. Entités Essentielles :

- → Grandes organisations ayant un impact critique sur la société, l'économie ou la sécurité nationale.
- → Régulation plus stricte, incluant des audits fréquents et des mesures de résilience renforcées.

4. Entités à Très Haut Impact :

- → Opérateurs d'infrastructures ou services stratégiques à l'échelle nationale ou européenne.
- → Soumis à des exigences de gouvernance et de sécurité les plus élevées, en raison d'un impact disproportionné en cas de défaillance.

4. Formation et sensibilisation :

- → Formation e-learning sur les exigences de NIS2 et leur application pratique.
- → Sensibilisation des équipes internes et des fournisseurs aux nouvelles obligations.

5. Gestion des incidents :

- → Mise en place d'un plan de réponse aux incidents conforme à NIS2.
- → Accompagnement dans la notification des incidents et la communication avec les parties prenante.

BÉNÉFICES

LuxGap combine son expertise en gouvernance et sécurité IT pour accompagner les entreprises à chaque étape de leur mise en conformité, en réduisant les risques tout en optimisant leurs ressources. Nous offrons également des outils automatisés et personnalisés pour un suivi simplifié de vos obligations.

Loi sur les Lanceurs d'alerte
(Directive (UE) 2019/1937)

La loi sur les lanceurs d'alerte vise à protéger toute personne signalant des violations du droit de l'Union ou des lois nationales, dans un contexte professionnel. Amécanismes de signalement sûrs et confidentiels, tout en prévenant les représailles à l'encontre des lanceurs d'alerte.

Quelles sont les obligations clés?

1. Mise en place de canaux de signalement internes

→ Création de procédures internes pour recueillir et traiter les alertes de manière confidentielle.
→ Désignation d'un responsable ou d'une équipe chargée de gérer ces signalements.

2. Protection contre les représailles

→ Interdiction formelle des mesures discriminatoires ou disciplinaires à l'encontre des lanceurs d'alerte (licenciement abusif, rétrogradation, intimidation, etc.).
→ Mise en œuvre de mécanismes de réparation en cas de préjudice subi par le lanceur d'alerte.

3. Canaux de signalement externes

→ Possibilité pour le lanceur d'alerte de s'adresser à des autorités ou organismes compétents lorsqu'il n'est pas en mesure d'utiliser les canaux internes ou lorsque ceux-ci se révèlent inefficaces.

4. Information et formation

→ Sensibilisation des collaborateurs et mise à disposition de procédures claires.
→ Formation des équipes dirigeantes et RH sur la gestion des alertes et la protection légale des lanceurs d'alerte.

l'intégration d'une politique efficace de protection des lanceurs d'alerte est aujourd'hui un impératif réglementaire et éthique. LuxGap vous accompagne à chaque étape — de l'évaluation de votre dispositif actuel à la formation de vos équipes — pour garantir une mise en conformité complète et une culture d'entreprise exemplaire en matière de transparence et de responsabilité.

* les obligations sont toutefois modulées selon le nombre d'employés)

NOS SERVICES

1. Audit et mise en conformité

→ Évaluation des procédures internes et des politiques RH pour vérifier leur adéquation avec la législation en vigueur.
→ Élaboration de canaux de signalement sécurisés et respectueux de la confidentialité.

2. Rédaction de politiques internes

→ Conception ou révision de politiques internes de « whistleblowing » alignées sur la Directive (UE) 2019/1937 et la législation nationale.
→ Intégration de chartes éthiques et de codes de conduite adaptés.

3. Formation et sensibilisation

→ Sessions de formation sur la protection des lanceurs d'alerte pour l'ensemble du personnel, y compris la direction, les managers et les équipes RH.
→ Mise à disposition de supports e-learning pour expliquer les bonnes pratiques et les obligations légales.

4. Gestion des signalements

→ Mise en place de dispositifs d'écoute et d'accompagnement pour les lanceurs d'alerte.
→ Externalisation partielle ou complète de la fonction « canal de signalement » pour garantir neutralité et confidentialité.

BÉNÉFICES

1. Réduction des risques juridiques et réputationnels

→ Limitation des contentieux et des sanctions liées à une absence ou à une mauvaise gestion des canaux de signalement.

2. Renforcement de la confiance interne

→ Promotion d'une culture d'intégrité et de transparence, valorisant la contribution de chacun à la conformité et à l'éthique de l'entreprise.

3. Amélioration de la gouvernance d'entreprise

→ Mise en place de mécanismes de contrôle interne plus efficaces pour détecter rapidement les infractions potentielles.

4. Alignement avec les bonnes pratiques européennes

→ Réassurance pour les partenaires, investisseurs et régulateurs, démontrant une volonté claire de se conformer aux standards les plus exigeants en matière de gouvernance et de protection des lanceurs d'alerte.

AI Act

Chez Luxgap, nous adoptons une approche en deux temps pour accompagner votre entreprise dans l'intégration de l'intelligence artificielle.

D'abord, nous recensons et sélectionnons, parmi plus d'une centaine de technologies éprouvées, celles qui répondent le mieux à vos enjeux métiers.

Ensuite, nous déployons ces solutions de manière fluide et structurée, en veillant à leur conformité avec les exigences légales, notamment le RGPD et l'AI Act (Règlement sur l'IA).

Principales étapes de conformité :

1. Identification des systèmes d'IA à haut risque (selon les critères de l'AI Act).
2. Évaluation technique pour détecter biais et vulnérabilités.
3. Documentation approfondie (algorithmes, données, processus).
4. Mise en œuvre de procédures internes garantissant la surveillance continue et la mitigation des risques.

Le futur Règlement sur l'IA (AI Act) vise à encadrer les systèmes d'intelligence artificielle afin de garantir le respect de normes éthiques et juridiques strictes. Il s'applique à toute organisation développant ou utilisant des systèmes d'IA au sein de l'UE, particulièrement lorsqu'ils sont considérés « à haut risque ».

NOS SERVICES

1. Audit complet des systèmes d'IA pour valider leur conformité (AI Act, RGPD).
2. Analyse avancée des biais algorithmiques et des enjeux éthiques.
3. Accompagnement dans la documentation et la rédaction des rapports de conformité.
4. Conseil stratégique pour atténuer les risques juridiques et réputationnels.

BÉNÉFICES

1. Maîtrise du risque réglementaire et réduction des sanctions potentielles.
2. Intégration responsable de l'IA au sein de vos processus, renforçant l'éthique et la transparence.
3. Amélioration de l'image de marque et de la confiance auprès de vos clients et partenaires.

En synthèse, Luxgap vous accompagne de la sélection des technologies IA les plus pertinentes jusqu'à leur mise en œuvre en toute conformité. Vous bénéficiez ainsi d'une expertise globale, conjuguant innovation et rigueur juridique, pour faire de l'IA un atout durable au service de votre compétitivité.

DORA Digital Operational Resilience Act

Le règlement DORA, adopté au niveau européen, vise à garantir une résilience opérationnelle numérique robuste dans le secteur financier. Il impose des exigences standardisées et harmonisées aux institutions financières et aux parties prenantes critiques pour réduire les interruptions et renforcer la sécurité des opérations numériques face aux cybermenaces et aux perturbations technologiques.

Quelles sont les obligations principales sous DORA?

1. Cartographie et gestion des dépendances technologiques :

→ Identifier tous les services, infrastructures et fournisseurs critiques.
→ Documenter les interdépendances entre les opérations financières et les systèmes technologiques.

2. Mise en place de tests avancés de résilience opérationnelle :

→ Effectuer des tests réguliers, comme des simulations de cyberattaques, pour évaluer la robustesse des systèmes.
→ Impliquer les tiers critiques (fournisseurs) dans ces tests.

3. Plans de continuité des activités et de reprise après incident :

→ Élaborer des plans pour assurer la continuité des opérations numériques en cas de perturbation.
→ Ces plans doivent couvrir la gestion des cyberincidents, les attaques physiques, les pannes techniques, et les crises systémiques.

4. Surveillance et reporting continus :

→ Mettre en place des systèmes de surveillance proactifs pour détecter les failles technologiques.
→ Rapporter les incidents majeurs aux régulateurs nationaux dans des délais stricts.

5. Gestion des risques liés aux tiers :

→ Garantir que les fournisseurs critiques se conforment aux exigences de sécurité et de résilience.
→ Élaborer des accords contractuels détaillés pour définir les responsabilités en matière de cybersécurité.

Institutions financières
Banques
Assurances
Sociétés de gestion d'actifs
Fonds d'investissement
Prestataires de services de paiement
Infrastructures de marché
Chambres de compensation
Dépositaires centraux de titres
plateformes de négociation
Infrastructures de paiement
Fournisseurs de services technologiques critiques
Services informatiques
Infrastructure cloud
Cybersécurité aux institutions financières

! Ces secteurs sont désormais soumis à des contrôles accrus, y compris des audits.

NOS SERVICES

LuxGap accompagne votre organisation à chaque étape de la conformité avec DORA grâce à des solutions adaptées et personnalisées :

1. **Évaluation et diagnostic :**

→ Identification des systèmes critiques et des vulnérabilités dans vos infrastructures technologiques.
→ Évaluation de la conformité initiale avec DORA.

2. **Stratégies de mise en conformité :**

→ Élaboration et mise en œuvre de politiques et procédures conformes aux exigences DORA.
→ Assistance dans la mise en place de tests de résilience avancés et de plans de continuité.

3. **Simulations et tests pratiques :**

→ Réalisation de simulations d'incidents (ex. : attaques cybernétiques) pour tester la robustesse de vos systèmes.
→ Validation de vos capacités de réponse et de reprise après incident.

4. **Documentation et suivi réglementaire :**

→ Production de rapports clairs et complets pour répondre aux exigences des régulateurs compétents.
→ Mise à jour continue des dossiers de conformité pour maintenir un haut niveau de résilience.

BÉNÉFICES

1. **Réduction des interruptions opérationnelles :**

→ Limitation des impacts des pannes technologiques et des cyberincidents.
→ Maintien de la continuité des services financiers critiques.

2. **Conformité aux normes européennes :**

→ Alignement avec les exigences harmonisées de l'Union européenne, renforçant votre position auprès des régulateurs.

3. **Renforcement de la confiance des partenaires :**

→ Assurance d'une résilience technologique solide, augmentant la confiance des investisseurs, clients, et partenaires financiers.

4. **Préparation aux cyberrisques :**

→ Meilleure anticipation et réponse aux menaces émergentes, garantissant une position proactive sur les risques technologiques.

CRA Cyber Resilience Act

Secteurs concernés produits numériques

Importateurs | Fabricants | Distributeurs

Les étapes clés pour se conformer au CRA:

1. Évaluation des risques des produits numériques commercialisés.
2. Mise en œuvre de mesures de sécurité dès la phase de conception.
3. Documentation des tests de sécurité et des garanties mises en place.
4. Surveillance continue des vulnérabilités et mises à jour de sécurité.

Le Cyber Resilience Act établit des exigences de sécurité pour les produits numériques afin d'assurer leur robustesse face aux cyberattaques.

NOS SERVICES

1. **Audit des produits numériques pour identifier les vulnérabilités.**
2. **Assistance pour la mise en conformité avec le CRA.**
3. **Conseils sur les meilleures pratiques en matière de sécurité produit.**

BÉNÉFICES

1. **Sécurité accrue des produits numériques.**
2. **Réduction des risques de failles et d'exploitation.**
3. **Confiance renforcée des utilisateurs et partenaires.**

DSA Digital Services Act

Secteurs concernés | Prestataires de services | Plateformes en ligne | Moteurs de recherche

Le Digital Services Act vise à encadrer les plateformes numériques pour assurer un environnement en ligne sécurisé et transparent.

Les étapes clés pour se conformer au DSA :

1. Mise en œuvre de mécanismes de modération des contenus.
2. Transparence sur les algorithmes de recommandation utilisés.
3. Gestion des notifications et signalements de contenus illicites.
4. Publication de rapports réguliers sur les pratiques de modération.

NOS SERVICES

1. Accompagnement dans la mise en conformité avec le DSA.
2. Développement de mécanismes de modération des contenus.
3. Formation des équipes sur les obligations réglementaires.
4. Reporting et documentation pour les autorités compétentes.

BÉNÉFICES

1. Sécurité accrue des produits numériques.
2. Réduction des risques de failles et d'exploitation.
3. Confiance renforcée des utilisateurs et partenaires.

Data Act

Le Data Act, adopté par l'Union européenne, vise à instaurer un cadre juridique pour réguler l'accès, le partage et l'exploitation des données non personnelles entre entreprises, consommateurs et entités publiques. L'objectif principal est de favoriser une économie des données équitable, transparente et compétitive tout en respectant les droits des acteurs impliqués.

OBJECTIFS

1. **Favoriser le partage équitable des données :**

→ Éviter les abus de position dominante par des acteurs détenant un volume massif de données.
→ Garantir un accès équitable aux données pour les PME et les startups.

2. **Encourager l'innovation intersectorielle :**

→ Permettre l'utilisation des données au-delà des frontières industrielles et organisationnelles, créant ainsi de nouvelles opportunités économiques.

3. **Assurer la transparence et la protection des droits :**

→ Définir des règles claires sur l'accès, la portabilité et la sécurité des données partagées.

Quelles sont les obligations clés sous le Data Act?

1. Identification et classification des données :

→ Inventorier les données non personnelles utilisées, partagées ou échangées, en distinguant les données commerciales sensibles des autres types de données.

2. Élaboration de contrats de partage de données :

→ Rédiger des contrats clairs et conformes, précisant les droits d'accès, les responsabilités, et les conditions d'utilisation des données.
→ Garantir des clauses de protection contre les usages abusifs ou la réutilisation non autorisée.

3. Mise en place de standards techniques et d'interopérabilité :

→ Adapter les systèmes et outils numériques pour assurer l'échange fluide et sécurisé des données entre différents acteurs.
→ Appliquer des standards reconnus pour faciliter l'interopérabilité technique.

4. Documentation et gouvernance des données :

→ Maintenir un registre des pratiques de partage, des partenaires impliqués, et des contrats établis.
→ Mettre en place une gouvernance interne pour surveiller les pratiques de partage et garantir leur conformité.

5. Mécanismes d'accès pour le secteur public :

→ Prévoir des procédures spécifiques pour répondre aux demandes légitimes des autorités publiques, notamment en cas de force majeure ou d'intérêt public.

Entreprises privées

Toute entité qui collecte, génère, utilise, partage ou monétise des données non personnelles, y compris les données issues de l'Internet des Objets (IoT), de la production industrielle ou des services numériques.

Exemples : fabricants de machines intelligentes, plateformes numériques, opérateurs logistiques.

Secteur public

Organismes publics demandant un accès aux données privées pour des besoins spécifiques.

Exemples : la recherche, la santé publique ou les situations d'urgence.

Fournisseurs de services de données

Plateformes d'intermédiation de données, prestataires d'analyse de données ou tout acteur offrant des services basés sur l'exploitation des données non personnelles.

NOS SERVICES

LuxGap accompagne les entreprises et les institutions publiques à chaque étape de leur mise en conformité avec le Data Act grâce à des solutions sur mesure :

1. **Conseil stratégique et évaluation initiale :**

→ Identification des données concernées et évaluation des pratiques actuelles de partage.
→ Analyse des risques juridiques et techniques associés à l'échange de données.

2. **Développement de contrats et politiques conformes :**

→ Rédaction de contrats de partage de données respectant les exigences du Data Act.
→ Assistance pour la création de politiques internes de gouvernance des données.

3. **Implémentation technique et juridique :**

→ Mise en œuvre de standards techniques pour l'interopérabilité et la sécurité des données.
→ Assistance pour gérer les demandes d'accès du secteur public ou des tiers.

4. **Simulations et audits :**

→ Réalisation d'audits pour évaluer la conformité et la robustesse des systèmes de gestion des données.
→ Simulations de scénarios pour tester les procédures de partage et de réponse.

BÉNÉFICES

1. **Exploitation optimale et sécurisée des données :**

→ Maximisation de la valeur économique des données tout en respectant les cadres réglementaires.

2. **Amélioration de la coopération intersectorielle :**

→ Établissement de relations solides avec des partenaires commerciaux grâce à des pratiques de partage claires et sécurisées.

3. **Réduction des risques juridiques et réputationnels :**

→ Mise en conformité avec la législation européenne, réduisant ainsi les risques de litiges ou de sanctions.

4. **Positionnement compétitif :**

→ Accès facilité à des opportunités d'innovation grâce à un partage de données fluide et conforme.

DGA Data Governance Act

Le Data Governance Act (DGA), adopté au niveau européen, vise à instaurer un cadre juridique facilitant le partage sécurisé, transparent et responsable des données. Il établit des mécanismes et des normes clairs pour encourager l'innovation basée sur les données tout en respectant les droits des parties prenantes.

OBJECTIFS

1. **Favoriser la réutilisation des données publiques et privées :**

→ Permettre aux entreprises et aux organismes publics de mettre à disposition leurs données dans un cadre sécurisé et légal.

2. **Créer des mécanismes de gouvernance standardisés :**

→ Faciliter les collaborations entre acteurs publics et privés grâce à des processus harmonisés.

3. **Promouvoir la transparence et la sécurité :**

→ Renforcer la confiance dans le partage de données via des règles claires sur l'accès, l'autorisation et la gestion des données.

Quels sont les Objectifs principaux du DGA?

1. Structuration de la gouvernance interne des données :

→ Mettre en place des politiques et des processus clairs pour gérer, classifier et structurer les données à partager ou réutiliser.
→ Nommer un responsable ou une équipe dédiée à la gouvernance des données.

2. Conformité avec les mécanismes d'autorisation :

→ Adopter des processus d'autorisation pour garantir que les données sont partagées dans le respect des droits des parties prenantes.
→ S'assurer que les données sensibles ou confidentielles sont protégées contre tout usage non autorisé.

3. Documentation des processus de partage et de réutilisation :

→ Maintenir une traçabilité complète des données échangées, des partenaires impliqués, et des conditions de partage.
→ Utiliser des contrats clairs et conformes aux exigences du DGA.

4. Collaboration avec des partenaires publics et privés :

→ Établir des partenariats stratégiques pour maximiser la valeur des données tout en respectant les obligations réglementaires.
→ Intégrer des standards techniques pour l'interopérabilité et la sécurité des échanges.

5. Implémentation de mécanismes pour l'altruisme des données :

→ Fournir des données pour des projets d'intérêt général dans un cadre encadré par le DGA.

Entreprises privées

Organisations ayant des données à forte valeur ajoutée, telles que les données industrielles, environnementales ou de santé, et souhaitant les partager ou monétiser sous un cadre sécurisé.

Exemples : fabricants, entreprises technologiques, prestataires de services numériques.

Organismes publics

Institutions détentrices de données non personnelles pouvant être réutilisées pour le développement de services innovants ou de projets de recherche.

Exemples:donnéesgéospatiales, environnementales, statistiques ou issues de la recherche publique.

Prestataires de services d'intermédiation de données

Plateformes facilitant l'échange ou la monétisation des données entre les parties dans un cadre sécurisé et neutre.

Organismes d'Altruisme des données

Acteurs partageant des données à des fins d'intérêt général, tels que la recherche médicale ou les projets environnementaux.

NOS SERVICES

LuxGap offre un accompagnement complet pour assurer la conformité avec le DGA et optimiser les opportunités de partage de données :

1. **Structuration de la gouvernance des données :**

→ Assistance dans la création de politiques internes de gouvernance des données.
→ Organisation des processus pour garantir une gestion efficace et conforme.

2. **Mise en conformité avec les mécanismes d'autorisation :**

→ Élaboration de mécanismes robustes pour protéger les données sensibles.
→ Rédaction de contrats de partage et d'autorisation conformes aux normes du DGA.

3. **Assistance dans la collaboration public-privé** :

→ Mise en place de partenariats stratégiques en respectant les règles de transparence et de sécurité.
→ Intégration des standards techniques nécessaires pour des échanges fluides et sécurisés.

4. **Gestion de l'altruisme des données :**

→ Aide à structurer des initiatives de partage de données à des fins d'intérêt général.

BÉNÉFICES

1. **Amélioration de la transparence et de la gouvernance des données :**

→ Renforcement de la confiance des partenaires et des parties prenantes dans la gestion des données.

2. **Maximisation des opportunités commerciales :**

→ Exploitation des données dans un cadre sécurisé pour générer de nouvelles opportunités économiques.

3. **Réduction des risques juridiques et réputationnels :**

→ Garantie de conformité aux exigences européennes, minimisant les risques de sanctions.

4. **Stimulation de l'innovation et de l'intérêt général :**

→ Participation à des projets collaboratifs pour des applications innovantes ou des objectifs sociétaux.

DMA Digital Markets Act

Le Digital Markets Act (DMA) vise à limiter les pratiques anticoncurrentielles sur les marchés numériques en imposant des règles strictes aux plateformes numériques qui occupent une position de “gatekeeper” (gardien d’accès). Son objectif est de promouvoir une concurrence équitable, d’encourager l’innovation et de protéger les droits des entreprises et des consommateurs.

Quelles sont les obligations clés sous DMA?

1. Identification des obligations spécifiques

- → Respect des obligations positives telles que la transparence des publicités numériques et la portabilité des données.
- → Interdiction des pratiques abusives comme :
  - Le favoritisme de leurs propres services.
  - L’empêchement des entreprises clientes de proposer des prix ou conditions différents sur d’autres plateformes.
  - L’imposition de l’utilisation de certains services connexes (ex. : systèmes de paiement internes).

2. Mise en conformité des pratiques commerciales :

- → Révision des contrats et des conditions d’utilisation pour éliminer les clauses anticoncurrentielles.
- → Modification des pratiques commerciales pour respecter les nouvelles règles.

3. Documentation et transparence :

- → Mise en place de mécanismes internes pour surveiller la conformité.
- → Partage d’informations pertinentes avec les régulateurs et les parties prenantes.

4. Collaboration avec les autorités de régulation :

- → Coopération lors des audits et enquêtes.
- → Notification proactive des changements pouvant affecter la conformité avec le DMA.

LES “GATEKEEPERS” SONT VISÉS PAR LE DMA, REMPLISSANT CES CRITÈRES

1. **Taille significative sur le marché intérieur :**

→ Chiffre d'affaires annuel dans l'UE supérieur à 7,5 milliards d'euros ou une valorisation boursière de plus de 75 milliards d'euros.
→ Exploitation d'un service de plateforme avec au moins 45 millions d'utilisateurs finaux actifs mensuels et 10 000 utilisateurs professionnels actifs annuels.

2. **Contrôle sur l'accès au marché :**

→ Les plateformes qualifiées comme "gatekeepers" sont celles qui servent d'intermédiaires incontournables entre les entreprises et les consommateurs.

3. **Position durable sur le marché :**

→ Maintien des seuils ci-dessus pendant au moins trois années consécutives.
→ Exemples de services couverts : moteurs de recherche, places de marché en ligne, réseaux sociaux, systèmes d'exploitation, services cloud, publicité en ligne.

NOS SERVICES

LuxGap fournit un accompagnement spécialisé pour aider les plateformes numériques à se conformer efficacement aux obligations du DMA :

1. **Audit de conformité :**

→ Évaluation des pratiques commerciales actuelles pour identifier les écarts avec les obligations du DMA.
→ Analyse des contrats et conditions d'utilisation des plateformes.

2. **Assistance dans la mise en œuvre des obligations :**

→ Accompagnement dans l'adaptation des pratiques commerciales.
→ Développement de mécanismes internes pour garantir la transparence et la conformité.

3. **Gestion des relations avec les autorités régulatrices :**

→ Assistance dans la préparation des réponses aux audits et des rapports de conformité.
→ Représentation auprès des régulateurs pour minimiser les risques de sanctions.

BÉNÉFICES

1. **Réduction des risques liés aux sanctions**

→ Évitement des amendes pouvant atteindre 10 % du chiffre d'affaires mondial annuel en cas de non-conformité.

2. **Conformité avec les attentes du marché**

→ Positionnement compétitif grâce à une conformité proactive.

3. **Renforcement de la réputation**

→ Amélioration de la confiance des utilisateurs, des entreprises partenaires et des régulateurs.

Règlement sur le libre flux des données non personnelle

Le règlement sur le libre flux des données non personnelles vise à garantir la libre circulation des données au sein de l'Union européenne tout en renforçant la sécurité et l'interopérabilité. Il permet de supprimer les restrictions de localisation injustifiées et d'optimiser les opérations numériques transfrontalières.

Quelles sont les obligations sous le règlement?

1. Identification des données non personnelles concernées :

→ Classification des données non personnelles utilisées ou stockées (ex. : données machine, analyses statistiques, données commerciales).

2. Élaboration de politiques internes :

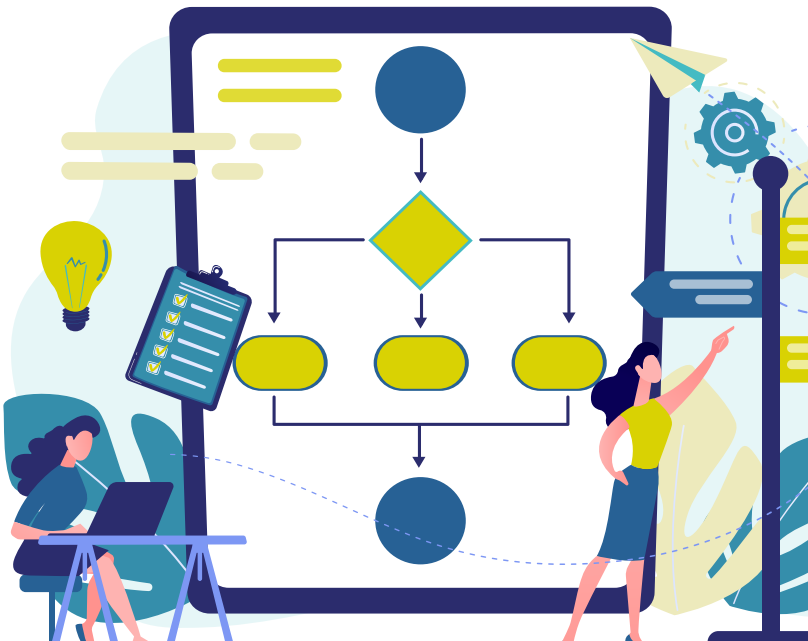
→ Création de politiques sur le traitement et la sécurité des données, incluant les plans de continuité en cas d'incident.

3. Mécanismes pour la portabilité des données :

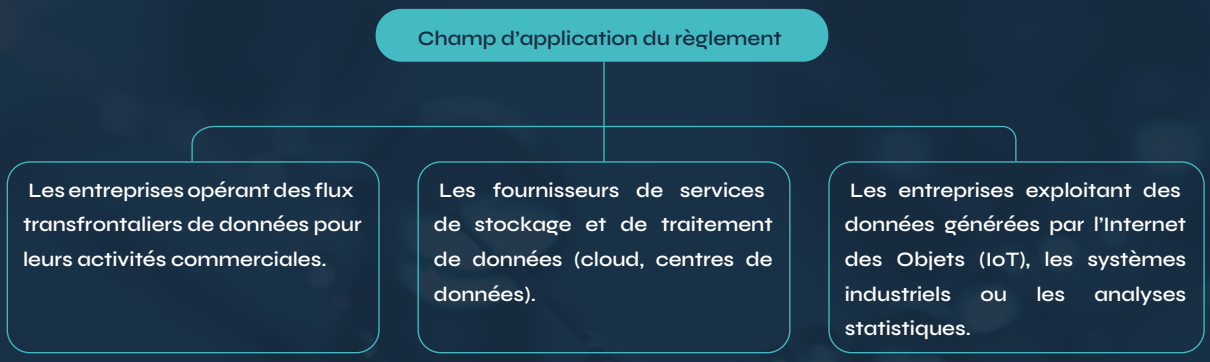
→ Mise en place d'outils permettant le transfert fluide des données entre fournisseurs de services et pays membres de l'UE.

4. Documentation des flux transfrontaliers :

→ Traçabilité complète des flux de données entre pays pour assurer leur conformité avec les exigences de localisation et de sécurité.



LE RÈGLEMENT S'APPLIQUE À TOUTE ORGANISATION TRAITANT OU STOCKANT DES DONNÉES NON PERSONNELLES DANS L'UE...



NOS SERVICES

LuxGap accompagne les organisations dans la gestion et la conformité liées au libre flux des données non personnelles :

1. **Conseil stratégique :**

→ Analyse des flux de données transfrontaliers et des restrictions locales potentielles.
→ Optimisation des politiques internes de gestion des données.

2. **Mise en conformité technique et juridique :**

→ Développement de mécanismes pour garantir la sécurité et l'interopérabilité des données.
→ Assistance dans la mise en place de contrats de traitement et d'hébergement conformes.

3. **Assistance opérationnelle :**

→ Aide à l'optimisation des flux de données pour réduire les coûts et augmenter l'efficacité opérationnelle.

BÉNÉFICES

1. **Simplification des processus opérationnels :**

→ Accès sans restriction aux services cloud et aux solutions de traitement de données au sein de l'UE.

2. **Réduction des contraintes techniques et juridiques :**

→ Suppression des obstacles liés à la localisation des données.

3. **Optimisation des coûts :**

→ Réduction des dépenses liées à la gestion et au stockage des données grâce à des pratiques unifiées

Le règlement eIDAS établit un cadre juridique pour l'identification électronique et les services de confiance dans l'Union européenne. Son objectif est de garantir des interactions numériques sécurisées et fiables entre citoyens, entreprises et autorités publiques.

eIDAS Electronic Identification and Trust Services Regulation

Quelles sont les obligations clés sous le règlement eIDAS?

1. Évaluation des besoins en identification électronique et services de confiance :

→ Identifier les cas d'usage des solutions eIDAS dans leurs interactions numériques (transactions en ligne, signatures électroniques).

2. Mise en œuvre de solutions conformes :

→ Intégrer des solutions techniques répondant aux standards eIDAS, telles que les signatures électroniques qualifiées ou les sceaux électroniques.

→ Garantir l'interopérabilité des systèmes d'identification avec ceux des autres États membres de l'UE.

3. Formation des utilisateurs finaux :

→ Former les employés et utilisateurs pour assurer une adoption efficace des solutions déployées.

4. Documentation et audits :

→ Documenter les processus et les politiques liés aux services de confiance pour répondre aux régulateurs en cas d'inspection

Fournisseurs de services de confiance qualifiés | Signature électronique | Horodatage

Cachet électronique | Certificats de validation de site web

Organisations utilisant des systèmes d'identification électronique | Entreprises | Institutions publiques

Autorités de certification | Entités délivrant des certificats électroniques garantissant l'identité des signataires

NOS SERVICES

1. **Audit et mise en conformité des solutions eIDAS :**

→ Évaluation des pratiques actuelles pour identifier les écarts par rapport aux exigences eIDAS.
→ Proposition de recommandations adaptées pour atteindre la conformité.

2. **Assistance dans l'intégration de services de confiance :**

→ Aide à l'implémentation de services tels que les signatures électroniques qualifiées et les certificats de validation de site web.

3. **Formation des équipes :**

→ Sessions de formation pour assurer une utilisation efficace et conforme des outils eIDAS.

BÉNÉFICES

1. **Renforcement de la sécurité :**

→ Protection accrue des transactions numériques et limitation des risques de fraude.

2. **Réduction des risques juridiques :**

→ Conformité avec un cadre réglementaire clair et uniformisé dans toute l'UE.

3. **Gain de confiance des utilisateurs finaux :**

→ Amélioration de la fiabilité perçue par les partenaires, clients et régulateurs.

ePrivacy Règlement sur la confidentialité électronique

Le règlement ePrivacy complète le RGPD en encadrant spécifiquement la confidentialité des communications électroniques et le traitement des données associées. Il vise à protéger les droits des utilisateurs tout en favorisant des pratiques commerciales transparentes et éthiques.

Quelles sont les obligations clés sous le règlement ePrivacy?

1. Mise en conformité des pratiques de collecte des données :

→ Adapter les pratiques de collecte de données liées aux communications électroniques pour respecter les exigences de confidentialité.

2. Élaboration de politiques sur les cookies et consentements :

→ Mettre en œuvre des bannières et des politiques de cookies conformes, avec une gestion claire des consentements.

3. Formation des équipes :

→ Sensibiliser les équipes marketing et IT sur les règles spécifiques au traitement des données électroniques.

4. Documentation et démonstration de la conformité :

→ Maintenir des registres des pratiques de traitement des données pour prouver la conformité lors d'audits.

5. Implémentation de mécanismes pour l'altruisme des données :

→ Fournir des données pour des projets d'intérêt général dans un cadre encadré par le DGA.

NOS SERVICES

1. Mise en conformité des pratiques de marketing numérique :

→ Audit des pratiques de collecte et d'utilisation des données.
→ Mise en œuvre de solutions conformes pour la gestion des cookies et consentements.

2. Assistance sur la gestion des cookies et consentements :

→ Aide technique et juridique pour développer des outils conformes de gestion des traceurs.

3. Formation des équipes :

→ Sessions sur les bonnes pratiques en matière de confidentialité et de traitement des données.

Fournisseurs de services de communication électronique

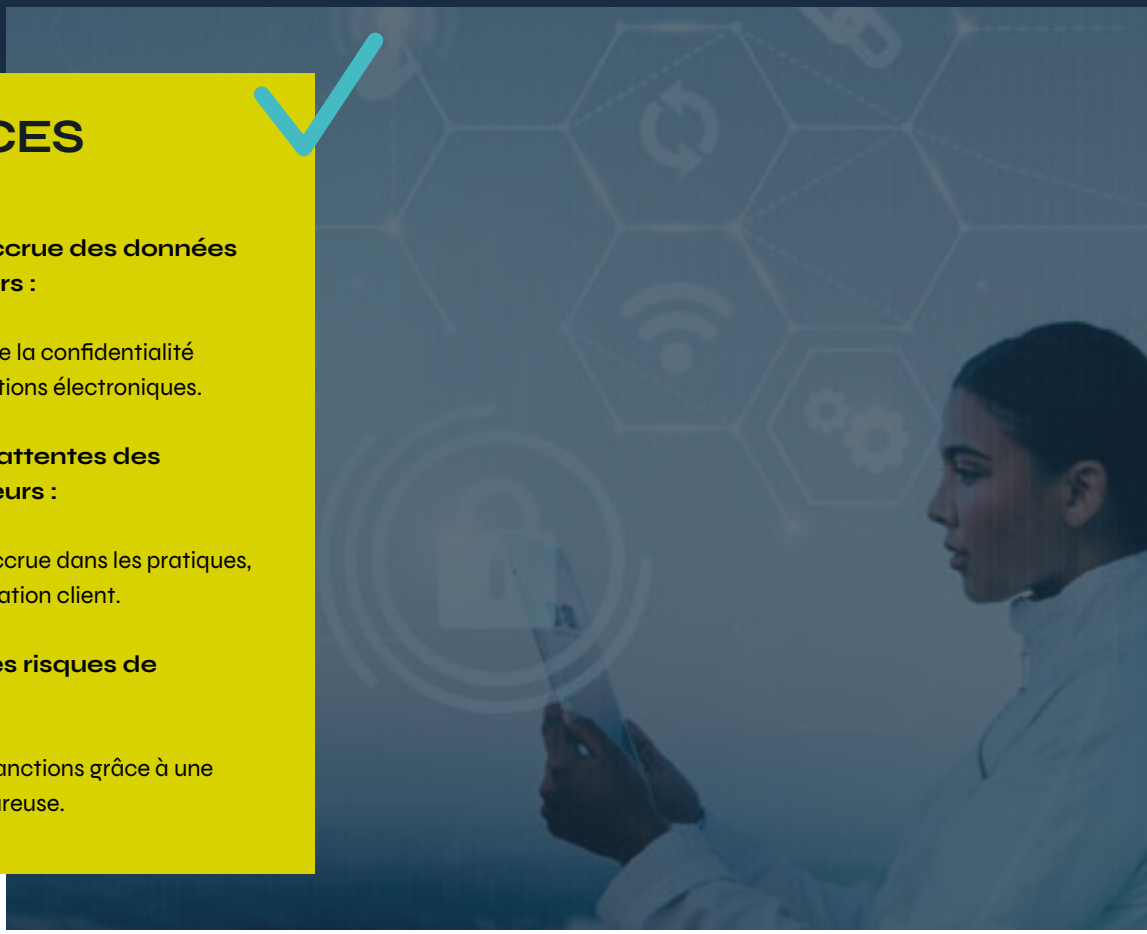
Opérateurs télécoms, plate-formes de messagerie en ligne, et services de VoIP.

Organisations traitant des métadonnées

Entreprises exploitant les données liées aux communications électroniques pour l'analyse ou le marketing.

Sites web et applications

Acteurs utilisant des cookies, traceurs ou autres technologies similaires pour collecter des informations utilisateur.



BÉNÉFICES

1. **Protection accrue des données des utilisateurs :**

→ Renforcement de la confidentialité des communications électroniques.

2. **Respect des attentes des consommateurs :**

→ Transparence accrue dans les pratiques, améliorant la relation client.

3. **Réduction des risques de violations :**

→ Évitement des sanctions grâce à une conformité rigoureuse.

Luxgap
DATA PRIVACY PARTNER

MAINTENANT QUE VOUS SAVEZ TOUT...
ET SI LA CONFORMITÉ DEVENAIT VOTRE ATOUT STRATÉGIQUE ?

Chez LuxGap, nous ne vous aidons pas simplement à cocher des cases réglementaires. Nous vous accompagnons pour gagner en sérénité, renforcer votre crédibilité et préparer l'avenir avec confiance.

- ☑ Une gouvernance des données solide
- ☑ Une cybersécurité proactive
- ☑ Une expertise internationale au service de votre conformité
- ☑ Un partenaire de confiance, engagé à vos côtés
- ☑ Prêt à passer à l'action ?

Discutons de vos enjeux. Construisons ensemble une stratégie de conformité efficace, claire et durable.

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

EMPOWERING TRUST!

CRÉDITS

TEXTE : LUXGAP

MISE EN PAGE: PARASOL STUDIO

ILLUSTRATIONS ET IMAGES: FREEPIK, ADOBE STOCK

Luxgap
DATA PRIVACY PARTNER

Contact:

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

contact@luxgap.com

Visitez notre site web
pour plus d'informations :
www.luxgap.com