Luxgap
DATA PRIVACY PARTNER

Le métier de Délégué à la Protection des Données (DPO)

Cadre juridique, missions, livrables et pilotage continu de la conformité

Version 27/02/2026 — Document de référence opérationnel à destination des dirigeants, directions métiers, IT & sécurité.

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

NAVIGATION

Sommaire

Ce document complète et structure la feuille de route de mise en conformité RGPD (9 axes) présentée dans notre approche proposée.

CHAPITRE 1

Le DPO en pratique

Le DPO (Data Protection Officer / Délégué à la protection des données) est l'organe interne ou externe chargé d'**orchestrer la conformité au RGPD**, de conseiller et de contrôler le dispositif, sans se substituer au responsable du traitement (principe d'accountability — art. 5(2) et 24 RGPD).

Point clé : le DPO n'est pas le « responsable » juridique de la conformité. Il conseille, alerte, documente, contrôle et facilite la prise de décision. La décision (finalités, moyens, arbitrages) reste portée par la direction et les métiers.

Ce que le DPO apporte concrètement

Cartographie des traitements

Une cartographie fiable des traitements et des flux de données, alignée sur les finalités et bases légales (art. 6, 9, 10 et 30). Le DPO identifie chaque traitement, ses destinataires, ses flux et ses fondements juridiques pour offrir une vision complète du patrimoine de données.

Règles & preuves documentées

Des règles opérationnelles et des preuves documentées (politiques, procédures, registres) pour démontrer la conformité (art. 5(2) et 24). Ce corpus documentaire constitue le socle de l'accountability exigée par le RGPD.

Gestion du risque privacy

Un mécanisme de gestion du risque « privacy » centré sur les personnes (AIPD — art. 35) et sur la sécurité (mesures techniques et organisationnelles — art. 32). L'approche par les risques permet de prioriser les efforts là où l'impact est le plus élevé.

Pilotage continu

Revues, audits, indicateurs, gestion du changement (privacy by design — art. 25) et coordination en cas d'incident (art. 33-34). Le DPO assure un suivi permanent et adapte le dispositif aux évolutions de l'organisation.

Point de contact unique

Un point de contact unique et compétent pour l'autorité de contrôle et les personnes concernées (art. 38(4) et 39(1)(d)-(e)). Le DPO centralise les échanges et garantit la réactivité de l'organisation.

DPO interne vs DPO externe

Le choix entre un DPO interne et un DPO externe dépend de la taille de l'organisation, de sa maturité et de ses ressources. Chaque option présente des avantages et des contraintes spécifiques.

1

🏢 DPO interne

Avantages : connaissance fine de l'organisation, proximité avec les métiers, disponibilité immédiate.

Contraintes : nécessite une indépendance effective, des ressources dédiées et l'absence de conflit d'intérêts (art. 38). Le DPO interne ne peut pas occuper une fonction qui détermine les finalités et moyens des traitements.

2

🌐 DPO externe

Avantages : mutualisation d'expertise (juridique, sécurité, métiers), montée en maturité plus rapide, capacité d'intervention et d'audit, regard extérieur objectif.

Contraintes : nécessite une gouvernance claire et un accès aux informations (art. 38(2)). Le contrat doit définir précisément le périmètre, les modalités de reporting et les règles d'escalade.

CHAPITRE 2

Quand et comment désigner un DPO

La désignation d'un DPO est **obligatoire** dans les cas listés à l'article 37(1) RGPD :

Autorités publiques

Autorités ou organismes publics (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle)

Suivi à grande échelle

Activités de base impliquant un suivi régulier et systématique des personnes à grande échelle

Données sensibles

Activités de base impliquant un traitement à grande échelle de données sensibles (art. 9) ou relatives aux condamnations et infractions (art. 10)

Grille de décision pratique

Pour déterminer si la désignation d'un DPO est obligatoire, quatre critères doivent être analysés au cas par cas :

1

Activités de base

Le traitement est-il indissociable de la mission principale ? Exemples : plateforme en ligne, RH centralisé, santé, assurance, fintech, télématique, marketing data-driven. Si le traitement est accessoire, le critère n'est pas rempli.

2

Suivi régulier et systématique

Profilage, scoring, géolocalisation, traçage, surveillance (en ligne/hors ligne), monitoring continu (ex. IoT, apps, CCTV intelligente). Le caractère « régulier » implique une récurrence ; « systématique » implique un système organisé.

3

Grande échelle

Volume de personnes, volume de données, durée, étendue géographique. L'appréciation se fait au cas par cas en combinant ces facteurs. Un médecin isolé ne traite pas à grande échelle ; un réseau hospitalier, oui.

4

Données sensibles / pénales

Catégories particulières (santé, biométrie, opinions politiques, orientation sexuelle, etc.) ou données pénales traitées dans l'activité de base. La combinaison avec le critère de grande échelle déclenche l'obligation.

Même hors obligation stricte, désigner un DPO (ou une fonction équivalente) est une **bonne pratique de gouvernance** et facilite la démonstration de conformité, notamment pour les organisations exposées (clients B2B, appels d'offres, audits, cybersécurité).

Formalités et livrables de désignation

La désignation du DPO doit être formalisée et communiquée. Trois livrables essentiels structurent cette étape :

📋 Acte de désignation

Lettre ou mandat précisant le périmètre d'intervention, le rattachement hiérarchique, les ressources allouées et les règles d'escalade (art. 37(5) et 38(2)). Ce document formalise l'engagement de l'organisation et les moyens mis à disposition du DPO.

📢 Publication des coordonnées

Les coordonnées du DPO doivent être publiées (site web, notices d'information, signature e-mail, etc.) et communiquées à l'autorité de contrôle (art. 37(7)). Cette publicité garantit l'accessibilité du DPO pour les personnes concernées et l'autorité.

📄 Charte DPO (recommandé)

Document définissant les règles d'indépendance, l'accès aux informations, la gestion des conflits d'intérêts, la confidentialité et les modalités de reporting (art. 38). La charte constitue le cadre de référence de la fonction DPO au sein de l'organisation.

CHAPITRE 3

Garanties d'indépendance et gouvernance

L'efficacité du DPO repose sur des **garanties formelles** : absence d'instructions sur l'exercice des missions, absence de sanction liée à ces missions, accès direct au plus haut niveau, ressources suffisantes, et prévention des conflits d'intérêts (art. 38 RGPD).

Exigences non négociables (art. 38)

Indépendance

Le DPO informe et conseille, mais ne reçoit pas d'instruction sur la manière d'exécuter ses missions (art. 38(3))

Rattachement

Le DPO rend compte directement à la direction (art. 38(3))

Ressources

Temps, budget, outils, accès aux systèmes et aux parties prenantes (art. 38(2))

Participation précoce

Implication dès la conception des projets/traitements (privacy by design — art. 25 et art. 38(1))

Confidentialité

Secret ou confidentialité sur l'exercice des missions selon le droit de l'UE/droit national (art. 38(5))

Gestion des conflits d'intérêts

Le DPO **ne peut pas** être placé dans une fonction qui détermine les finalités et moyens des traitements. Les fonctions suivantes sont incompatibles avec le rôle de DPO :

- Direction générale
- Direction IT
- Direction RH
- Direction marketing/ventes
- Direction sécurité (si elle arbitre les finalités/moyens)

Une **analyse de conflit d'intérêts documentée** est recommandée, notamment en cas de cumul de fonctions.

Livrable recommandé : matrice des rôles incompatibles + procédure de traitement des conflits (déclaration, arbitrage, mesures compensatoires).

Gouvernance type

Comité Privacy

Mensuel ou trimestriel : arbitrages, priorités, validation des politiques, suivi des incidents et des risques.

Réseau de « privacy champions »

Par département : collecte des informations pour le registre, relai de formation, détection des projets.

Processus de changement

Tout nouveau traitement/projet (outil, prestataire, campagne marketing, IA, CCTV) déclenche une analyse privacy (art. 25 et 35).

CHAPITRE 4

Missions légales et livrables attendus (art. 39)

L'article 39 RGPD définit les missions minimales du DPO. En pratique, ces missions se traduisent par des **livrables et des routines de pilotage mesurables**. Le DPO doit disposer d'un accès effectif aux informations (registre, contrats, incidents, projets) pour pouvoir produire ces preuves de manière robuste (art. 38(2)).

Informer, conseiller & surveiller

Mission (art. 39)	Traduction opérationnelle	Preuves / livrables
Informer & conseiller (art. 39(1)(a))	Assistance métiers/direction : bases légales, clauses, cookies, transferts, IA, RH.	Avis DPO datés, notes de position, fiches de traitement, décisions documentées
Surveiller la conformité (art. 39(1)(b))	Programme de conformité : politiques, contrôles, audits, indicateurs, plan d'actions.	Plan annuel, tableau de bord KPI, rapports d'audit, registre des actions
Sensibiliser & former (art. 39(1)(b))	Formation initiale + recyclage + sensibilisation ciblée par métier.	Plan de formation, contenus, taux de complétion, quiz/attestations

Conseiller, coopérer & coordonner

Mission (art. 39)	Traduction opérationnelle	Preuves / livrables
Conseiller sur les AIPD (art. 39(1)(c))	Méthode d'analyse de risque sur les personnes ; suivi des mesures.	Registre AIPD, screening, rapports AIPD, revues périodiques
Coopérer avec l'autorité (art. 39(1)(d))	Gestion des échanges : demandes, contrôles, notifications, consultations.	Journal des échanges, dossiers contrôle, décisions/mesures
Point de contact (art. 39(1)(e))	Canal personnes/autorité ; triage des demandes ; coordination interne.	Canal DPO, procédure d'escalade, registre des demandes

CHAPITRE 5

Cycle de conformité : mise en place, suivi, amélioration

Une conformité durable ne se limite pas à produire des documents. Elle repose sur un **cycle de vie documenté**, des revues régulières et une gestion structurée du changement. Le cycle se décompose en trois phases complémentaires.

Les trois phases du cycle de conformité

1. Mettre en place

Phase initiale :

- Gouvernance DPO (mandat, comité, RACI)
- Cartographie & registre (art. 30)
- Bases légales & tests (LIA, consentement)
- Notices & cookies (art. 12-14)
- Politiques & procédures
- Contrats (art. 28/26)
- Screening AIPD (art. 35)
- Plan de formation

2. Opérer au quotidien

Phase « run » :

- Triage des projets (privacy by design — art. 25)
- Gestion des droits (art. 15-22)
- Suivi des tiers & sécurité
- Incidents & violations (art. 33-34)
- Mises à jour notices/registre
- Support métiers (avis)
- Reporting direction

3. Améliorer & prouver

Phase assurance :

- Revues trimestrielles KPI
- Audits ciblés et correctifs
- Tests (phishing, vulnérabilités)
- Revue annuelle registre & politiques
- Revue des transferts (art. 44+)
- Rapport DPO & plan d'actions N+1

Déclencheurs imposant une revue

Certains événements imposent une revue immédiate du dispositif de conformité, indépendamment du calendrier de revue périodique :

1

Nouveaux traitements

Nouvel outil/logiciel, nouvelle collecte, nouveau canal marketing, nouveau traitement RH ou vidéosurveillance. Chaque nouveau traitement doit être intégré au registre et faire l'objet d'un screening AIPD.

2

Nouveaux tiers

Nouveau prestataire ou transfert hors UE/EEE, changement d'hébergeur, sous-traitance en cascade. La due diligence et la mise à jour contractuelle sont requises avant toute mise en production.

3

IA & profilage

Nouveau projet IA/profilage/scoring, décision automatisée (art. 22) ou évolution substantielle d'un traitement. Ces projets nécessitent systématiquement une AIPD approfondie.

4

Incidents

Incident de sécurité, suspicion de fuite, anomalie récurrente, audit client ou contrôle de l'autorité. La réactivité et la documentation sont essentielles pour démontrer la conformité.

CHAPITRE 6

Axes opérationnels de conformité

Les sections suivantes détaillent les **9 axes opérationnels** du dispositif de conformité RGPD, chacun avec ses actions de mise en place, ses revues périodiques et ses déclencheurs de suivi.

AXE 6.0

Gouvernance et accountability (socle DPO)

Cadre juridique : Principes art. 5 ; accountability art. 5(2) et 24 ; privacy by design art. 25 ; obligations DPO art. 37-39 RGPD.
Objectif : Mettre en place un dispositif de conformité pilotable, proportionné aux risques, et démontrable à tout moment.

Mise en place

- Mandat/charte DPO : périmètre, rattachement, ressources, accès, escalade
- Cartographie parties prenantes + RACI
- Comité Privacy + réseau de relais
- Référentiel documentaire : politiques, procédures, modèles
- Plan de conformité priorisé + registre des actions
- Mécanisme de validation des décisions privacy

Suivi & déclencheurs

- Escalade direction si risque résiduel élevé
- Suivi nouveaux projets via « privacy intake »
- Traçabilité : décisions, arbitrages, exceptions

1 2 3

Revues périodiques

- Revue annuelle de la gouvernance (mandat, ressources, conflits)
- Revue trimestrielle du plan d'actions et des risques
- Revue annuelle du corpus de politiques/procédures

Preuves à conserver : Lettre de désignation / contrat DPO externe + charte signée ; PV de comité et décisions d'arbitrage ; tableau de bord (KPI, risques, incidents) + rapport DPO annuel ; référentiel documentaire avec gestion de versions.

AXE 6.1

Formation et sensibilisation

Cadre juridique : Art. 39(1)(b) RGPD (sensibilisation/formation) ; art. 24 RGPD (mesures appropriées).

Objectif : Créer une culture de protection des données : réduire les erreurs humaines, rendre les politiques applicables et mesurables.

Mise en place

- Analyse des besoins par métier (RH, IT, support, marketing, sales, finance, direction)
- Formation générale RGPD (socle) + modules ciblés (recrutement, prospection, CCTV, support IT)
- Parcours d'onboarding privacy pour les nouveaux arrivants
- Micro-formations courtes (3-5 min) lors de nouvelles politiques ou incidents récurrents
- Procédure de preuve : participation, quiz, attestations et archivage

Revues & suivi

- Recyclage annuel (ou biannuel selon risque) + mise à jour lors de changement de process/outil
- Revue trimestrielle des taux de complétion et des populations non formées
- Revue annuelle de la bibliothèque de contenus
- Suivi mensuel des complétions (KPI) et relances automatiques
- Campagnes ponctuelles : phishing simulation, focus mots de passe, partage de fichiers
- Analyse des incidents/DSAR pour identifier les sujets à (re)former

Preuves : Plan de formation et calendrier ; contenus versionnés ; liste des participants, attestations, scores/quiz ; rapports de campagnes et actions correctives.

AXE 6.2

Analyse des données : cartographie, registre et conservation

Cadre juridique : Art. 30 RGPD (registre) ; art. 5(1) (minimisation, finalités, conservation) ; art. 6, 9, 10 (bases légales) ; art. 25 (privacy by design).
Objectif : Connaître, justifier et maîtriser les traitements : finalités, bases légales, données, destinataires, durées, transferts, risques.

Mise en place

- Inventaire des traitements par département/service (registre structuré)
- Validation des bases légales et conditions art. 9/10
- Évaluation de l'intérêt légitime (LIA) pour les traitements concernés
- Politique de conservation : durées + règles d'archivage/suppression
- Cartographie des flux (systèmes, accès, destinataires internes/externes)

Revues périodiques

- Revue au minimum annuelle du registre et des durées ; mise à jour à chaque changement substantiel
- Revue trimestrielle des nouveaux traitements/projets et intégration au registre
- Contrôle semestriel de la suppression/archivage sur systèmes critiques

Suivi & déclencheurs

- Nouveau traitement, nouvelle finalité, nouveau système, fusion/acquisition, nouveau prestataire
- Suivi des écarts : traitements non enregistrés, bases légales discutables, durées non appliquées
- Corrélation avec AIPD : détection précoce des traitements à risque élevé (art. 35)

Preuves : Registre des traitements (art. 30) à jour ; dictionnaire de données et schémas de flux ; LIA documentées ; preuves de consentement ; politique de conservation + preuves d'exécution (logs de purge, tickets, paramétrages).

AXE 6.3

Transparence et information (notices, cookies)

Cadre juridique : Art. 12 à 14 RGPD ; art. 5(1)(a) ; art. 7 et 21 ; règles cookies/ePrivacy selon les États.

Objectif : Informer clairement les personnes (clients, prospects, candidats, employés, visiteurs) et maîtriser les cookies/traceurs.

Mise en place

Politique générale + notices par population : site web, clients/prospects, employés, candidats, CCTV. Registre des notices (versioning). Cadre cookies/traceurs : inventaire, catégorisation, bandeau/consentement, preuve des choix. Modèles d'information pour collecte indirecte (art. 14). Canal DPO visible et opérationnel (art. 37(7) et 38(4)).

Revues périodiques

Revue annuelle des notices et immédiate en cas de changement de traitement. Revue trimestrielle des cookies/traceurs (scan technique, vérification scripts). Contrôle de cohérence : registre (art. 30) vs notices (art. 13-14) vs contrats (art. 28/26).

Suivi & déclencheurs

Nouvelle campagne marketing, nouveau tracker, nouveau SaaS analytics/CRM, nouveau formulaire. Suivi du retrait du consentement et des oppositions marketing (art. 7(3) et 21). Suivi des plaintes/questions reçues via le canal DPO.

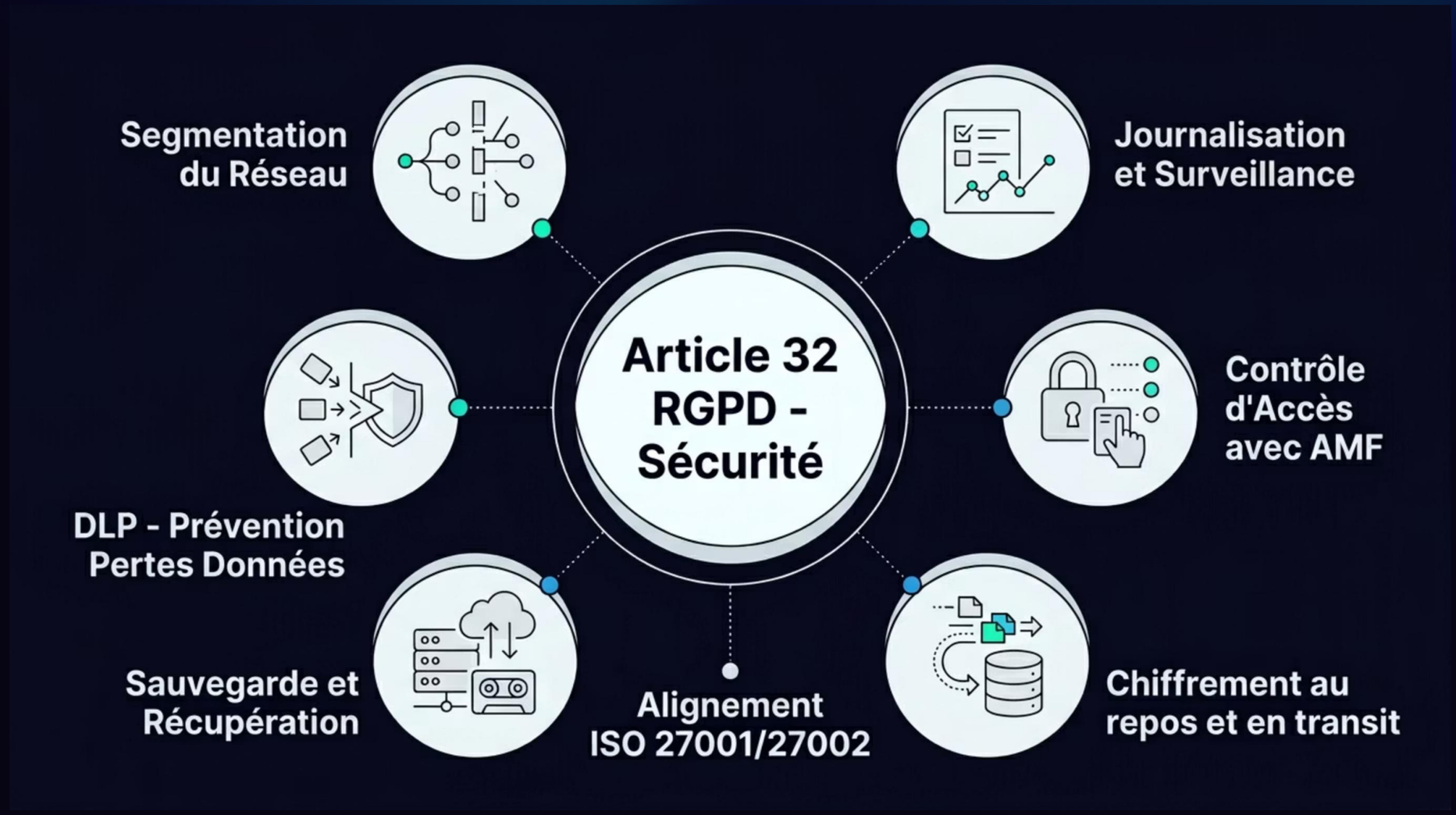
Preuves : Notices datées et versionnées ; captures bandeau cookies ; rapports de scan de traceurs ; registre des consentements + preuve de retrait ; journal des oppositions marketing ; preuves de diffusion.

AXE 6.4

Sécurité des données personnelles (TOMs, risques, maturité)

Cadre juridique : Art. 32 RGPD ; art. 5(1)(f) ; art. 25 ; art. 24 (mesures appropriées).

Objectif : Réduire le risque d'atteinte aux droits et libertés via une sécurité proportionnée aux risques, testée et documentée.



Sécurité : actions et suivi opérationnel

Mise en place

- Revue des mesures existantes et analyse de risques (menaces, vulnérabilités, impacts)
- Définition d'une liste de TOMs : accès, MFA, chiffrement, sauvegardes, logs, segmentation, DLP
- Politiques IT : gestion des accès, postes, mobiles, mots de passe, sauvegardes, télétravail, BYOD
- Alignement avec ISO 27001/27002 pour piloter la montée en maturité
- Plan de tests : scans vulnérabilités, correctifs, revues d'accès, exercices

Revues périodiques

- Revue annuelle de l'analyse de risques et des TOMs ; ajustement en cas d'évolution majeure
- Scans de vulnérabilité hebdomadaires (ou selon criticité) + suivi de remédiation
- Revue trimestrielle des habilitations sur systèmes sensibles

Suivi & déclencheurs

- Suivi des vulnérabilités : SLA de correction, exceptions documentées, risques résiduels acceptés
- Déclencheur : incident sécurité, nouveau cloud, intégration API, accès fournisseur
- Suivi des campagnes de sensibilisation sécurité (phishing) et des écarts récurrents

Preuves : Registre TOMs ; politiques IT ; preuves d'implémentation (tickets, logs, paramétrages) ; rapports scan/pentest ; plans de remédiation ; comptes rendus de revues d'accès ; analyse de risques ; décisions d'acceptation de risque ; PCA/PRA si applicables.

AXE 6.5

Acteurs du traitement : responsables, sous-traitants et partenaires

Cadre juridique : Art. 28 (sous-traitants) ; art. 26 (responsables conjoints) ; art. 29 ; art. 32 ; art. 44+.
Objectif : Maîtriser la chaîne de traitement : qui fait quoi, sur quelle base, avec quelles garanties, et avec quel niveau de risque.

Registre des tiers

Inventaire de tous les fournisseurs, partenaires et clients manipulant des données personnelles

Qualification juridique

Responsable, sous-traitant, responsable conjoint ou destinataire — chaque tiers doit être qualifié

Mise à niveau contrats

Clauses art. 28, sécurité, assistance droits/AIPD, audit, sous-traitance en cascade

Due diligence

Privacy & security basée sur le risque : questionnaire, preuves, analyse technique si nécessaire

Onboarding fournisseur

Validation DPO + IT/Sécurité + Achats avant signature de tout nouveau contrat

Revues : Revue annuelle des fournisseurs à risque et avant renouvellement contractuel. Revue périodique des sous-traitants ultérieurs (liste, changements, notifications). Contrôles ponctuels : audits, revues de preuve, vérification des mesures annoncées.

Preuves : Registre des tiers + fiches de qualification ; DPAs/accords art. 26 signés ; rapports de due diligence, scoring de risque ; traçabilité des validations et des sous-traitants ultérieurs approuvés.

AXE 6.6

Droits des personnes (DSAR) : organisation, délais, preuves

Cadre juridique : Art. 12 ; art. 15-22 ; art. 7(3) ; art. 19 ; art. 21(2) RGPD.

Objectif : Répondre de manière sécurisée, complète et dans les délais à toute demande d'exercice de droits (clients, prospects, employés).

Mise en place

- Procédure DSAR : canaux, triage, vérification d'identité, rôles, escalade, délais, exemptions
- Modèles de réponses + registre des demandes
- Mécanisme de recherche/extraction : cartographie des systèmes, responsables de collecte, extraction sécurisée
- Procédure marketing : désinscription, opposition, listes d'exclusion
- Formation des équipes front-office/RH pour reconnaître une demande (même implicite)

Délais & suivi

Réponse sous 1 mois (prolongeable de 2 mois) — art. 12(3)

- Revue mensuelle/trimestrielle : délais, qualité, incidents (KPI)
- Test annuel bout-en-bout DSAR
- Mise à jour des modèles/registre en cas d'évolution
- Suspicion d'usurpation, demande répétitive, conflit avec obligation légale de conservation
- Suivi de l'effacement et preuves ; notification aux destinataires si requis (art. 19)

Preuves : Registre DSAR : dates, identité vérifiée, droit invoqué, décision, date réponse, pièces transmises. Copies des réponses ; logs extraction/effacement ; listes d'opposition marketing. Compte-rendu de tests DSAR et actions d'amélioration.

AXE 6.7

Privacy by design & AIPD (DPIA)

Cadre juridique : Art. 25 ; art. 35 ; art. 36 ; art. 22 ; art. 9-10 RGPD.

Objectif : Détecter les traitements à risque élevé, analyser les impacts sur les personnes, définir et suivre des mesures de réduction du risque.

1

Screening AIPD

Processus intégré à la gestion de projet (questionnaire court, traçable) avec critères d'alerte basés sur les lignes directrices EDPB (9 critères)

2

Modèle AIPD

Description, nécessité/proportionnalité, risques, mesures, risque résiduel, décision. Validation métiers, IT/sécurité, DPO

3

Registre & décisions

Registre AIPD + registre des décisions (AIPD réalisée / non nécessaire). Consultation préalable si risque résiduel élevé (art. 36)

4

Revues périodiques

Revue en cas de changement substantiel. Revue périodique (1 à 3 ans) des AIPD sur traitements critiques. Revue de l'efficacité des mesures

Déclencheurs : IA/profilage, biométrie, géolocalisation, CCTV, surveillance employés, mutualisation de bases. Suivi du plan d'action AIPD : mesures, jalons, preuves. Traçabilité des avis DPO et des décisions finales de la direction.

Preuves : Questionnaires screening ; rapports AIPD signés ; décisions de consultation préalable ; plans d'action et preuves d'implémentation ; avis DPO datés, arbitrages et acceptations de risque résiduel.

AXE 6.8

Violations de données : préparation, réaction, documentation

Cadre juridique : Art. 33 (notification sous 72h) ; art. 34 ; art. 32 ; art. 33(5) RGPD.
Objectif : Être prêt à détecter, qualifier et gérer une violation, limiter l'impact, notifier si nécessaire et prouver la conformité.

La procédure doit définir les rôles et la contact list (DPO, IT/Sécurité, Direction, Communication, Juridique), les modèles de notification et critères de décision (autorité / personnes), ainsi que le registre des incidents/violations (documentation systématique, même sans notification). Un exercice annuel « 72h » (table-top) et une revue post-incident systématique sont essentiels.

Preuves : Registre violations : chronologie, données, volume, causes, mesures, décision de notifier ou non (art. 33(5)). Notifications/échanges ; preuves de communication aux personnes. Rapports d'exercices et preuves de remédiation.

AXE 6.9

Transferts internationaux (hors UE/EEE)

Cadre juridique : Art. 44-49 RGPD ; art. 45 (adéquation) ; art. 46 (garanties, ex. SCC) ; art. 49 (dérogations).
Objectif : Identifier et encadrer tout transfert ou accès depuis un pays tiers (y compris accès distant, support, sous-traitance).

Mise en place

- Cartographie des transferts : prestataires, filiales, support, sauvegardes, outils non-européens
- Qualification : pays adéquat vs garanties vs dérogation
- Clauses contractuelles appropriées (SCC) ou autres mécanismes + gestion sous-traitants ultérieurs
- Processus TIA et mesures supplémentaires (chiffrement, pseudonymisation, contrôle d'accès)
- Mise à jour notices et contrats clients si nécessaire

Revues périodiques

- Revue annuelle du registre des transferts et des TIAs ; requalification si changement prestataire
- Veille sur les changements impactant les transferts (versions SCC, localisation, sous-traitance)
- Revue périodique des mesures supplémentaires (efficacité, logs, clés, accès)

Suivi & déclencheurs

- Nouveau SaaS, changement région cloud, support hors UE, accès admin tiers
- Suivi des demandes d'accès autorités étrangères (si applicable) et procédure interne
- Suivi des audits clients portant sur localisation des données

Preuves : Registre transferts + schémas de flux ; SCC/clauses signées ; TIAs ; preuves mesures supplémentaires (chiffrement, gestion des clés, logs) ; versions des notices et communications clients.

AXE 6.10

Contrôle, audit et amélioration continue

Cadre juridique : Art. 5(2) et 24 (accountability) ; art. 32 ; art. 39(1)(b) ; art. 30 et 33(5).

Objectif : Transformer la conformité en système de management : indicateurs, contrôles, revues, audits, actions correctives.

Tableau de bord

Registre, formation, DSAR, AIPD, fournisseurs évalués, incidents, vulnérabilités, audits

Audits clients/tiers

Réponses standardisées, pack sécurité & privacy

Audit interne

Plan annuel ciblé sur risques et traitements critiques

Evidence pack

Localisation des documents et preuves d'effectivité

Non-conformités

Détection, analyse, action corrective, validation, clôture

Cadence : Revue mensuelle/trimestrielle KPI en comité ; revue annuelle de direction (bilan, maturité, incidents, plan N+1) ; audit annuel ou biannuel (registre, contrats, droits, incidents, transferts). Suivi des actions : délais, responsables, preuves, risques résiduels. Amélioration continue via retours d'expérience et mises à jour des politiques.

CHAPITRE 7

Pilotage : cadence de revue recommandée

La fréquence exacte dépend du risque, du volume de traitements et du niveau de maturité. Le tableau ci-dessous propose une **cadence opérationnelle généralement adaptée aux PME et aux groupes**.

Revues hebdomadaires et mensuelles

Fréquence	Revue / activité	Indicateurs / livrables
Hebdomadaire	Scans de vulnérabilité / suivi patch ; triage nouveaux projets et demandes ; suivi incidents en cours	Rapport de scan & backlog ; journal privacy intake ; ticketing incident
Mensuelle	Suivi des demandes de droits (DSAR) ; suivi fournisseurs en onboarding ; reporting opérationnel DPO	KPI délais DSAR ; % fournisseurs évalués ; avis/notes DPO

Revues trimestrielles et semestrielles

Fréquence	Revue / activité	Indicateurs / livrables
Trimestrielle	Comité Privacy (direction) ; revue des risques & actions ; revue cookies/traceurs ; revue habilitations critiques	PV comité + décisions ; risk register ; rapport cookie scan ; access review log
Semestrielle	Test DSAR bout-en-bout ; exercice incident (partiel) ; contrôle conservation (échantillon)	Rapport test DSAR ; compte-rendu exercice ; preuves de purge/archivage

Revue annuelle

Registre & notices

Revue du registre (art. 30) et des notices d'information — versionnage et mise à jour

AIPD critiques

Revue des AIPD sur les traitements les plus sensibles — registre AIPD & revues périodiques

Audit interne ciblé

Audit focalisé sur les risques et traitements critiques — rapports d'audit et plans d'actions

Plan de formation N+1

Élaboration du plan de formation pour l'année suivante — contenus, populations, calendrier

Rapport annuel DPO

Bilan complet de l'année : maturité, incidents, KPI, recommandations et plan d'actions N+1

Checklist de conformité documentaire

Cette annexe rapide récapitule l'ensemble des documents et preuves à maintenir pour démontrer la conformité à tout moment :

- Registre des traitements (art. 30)

  À jour + politique de conservation associée

- Notices (art. 12-14)

  + politique cookies/traceurs et preuves de consentement si applicable

- Registre des tiers + DPAs (art. 28)

  Accords art. 26 + preuves de due diligence

- Procédure DSAR + registre

  Preuves de réponse dans les délais (art. 12, 15-22)

- Registre AIPD + screening + rapports (art. 35)

  Décisions (consultation art. 36 si nécessaire)

- Procédure incidents/violations + registre (art. 33(5))

  Preuves d'exercices de simulation

- Registre transferts + SCC/TIA (art. 44-49)

  Mesures supplémentaires documentées

- Politiques IT/TOMs + preuves de tests (art. 32)

  Scans, pentests, revues d'accès

- Programme de formation + taux de complétion (art. 39)

  Attestations et scores

- Tableau de bord et rapports DPO

  Accountability art. 5(2)/24 — preuves de pilotage continu

Références juridiques principales

Règlement (UE) 2016/679 (RGPD) — articles les plus mobilisés dans un dispositif DPO :

Principes & accountability

Art. 5 (principes) et 5(2) (accountability). Art. 24-25 (responsabilité et privacy by design). Art. 28-29 (sous-traitance et personnes autorisées).

Bases légales & données sensibles

Art. 6, 7 (bases légales et consentement). Art. 9-10 (données sensibles/pénales).

Transparence & droits

Art. 12-14 (transparence). Art. 15-22 (droits des personnes concernées).

Registre & sécurité

Art. 30 (registre des traitements). Art. 32-34 (sécurité et violations).

AIPD & DPO

Art. 35-36 (AIPD et consultation préalable). Art. 37-39 (désignation, positionnement, missions du DPO).

Transferts internationaux

Art. 44-49 (transferts internationaux de données personnelles).

Pour une implémentation robuste, il est recommandé de s'appuyer sur les **lignes directrices du Comité européen de la protection des données (EDPB)** relatives au DPO, aux AIPD et aux transferts, ainsi que sur des référentiels de sécurité (**ISO 27001/27002**) lorsque pertinent.

En résumé : les clés du succès

Gouvernance claire

Un mandat formalisé, un comité privacy actif et un réseau de relais par département constituent le socle indispensable du dispositif DPO.

Cycle continu

La conformité n'est pas un projet ponctuel mais un cycle permanent : mise en place, opération quotidienne, amélioration et preuve.

Preuves documentées

L'accountability exige de pouvoir démontrer la conformité à tout moment : registres, avis, rapports, tests et tableaux de bord versionnés.

Culture privacy

La formation, la sensibilisation et l'implication de tous les métiers transforment la conformité en réflexe organisationnel durable.

Note : ce document est une brochure opérationnelle. Il doit être adapté au contexte sectoriel, au droit national applicable et aux exigences contractuelles de chaque organisation.

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