

Sécurité juridique et financière de la donnée



MODE D'EMPLOI POUR ÊTRE EN SÉCURITÉ

*Ce que tout dirigeant doit savoir avant qu'un régulateur, un juge
ou un concurrent ne le lui apprenne*

France · Suisse · Canada

Avertissement aux dirigeants	3
L'état du risque — chiffres 2025-2026	4
Suisse : quand la sanction cesse d'être celle de l'entreprise	5
Canada : l'un des régimes les plus stricts au monde	6
Le risque RH — un terrain particulièrement sanctionné	7
En Suisse, trois textes se combinent et surprennent souvent les directions RH habituées au seul RGPD :	8
Qui peut vous contrôler, et avec quels pouvoirs	9
Mode d'emploi : comment éviter cette situation	10
En France	10
En Suisse	10
Au Canada	11
Pourquoi nous vous offrons de livre ?	12
Questions fréquentes	14
En savoir plus	16



Avertissement aux dirigeants

Ce document n'est pas un argumentaire commercial.

C'est une mise en garde, construite à partir de faits vérifiables, de montants de sanctions réels et de textes de loi en vigueur en France, en Suisse et au Canada.

Selon notre enquête,

la majorité des dirigeants n'ont qu'une idée approximative de leur exposition réelle aux risques, qu'ils soient juridiques, réglementaires et financiers, liée à la gouvernance de leurs données.

Ils le découvrent le jour où il est trop tard pour l'éviter, et juste à temps pour le payer à titre personnelle selon les pays et parfois très chers.

Pendant des décennies, une non-conformité de données est restée, pour l'essentiel, un problème de l'entreprise : image écornée, amende, procès désagréable porté par la structure.

Ce n'est plus vrai aujourd'hui.

En Suisse depuis 2023, au Québec depuis 2022, la loi vise désormais nommément le dirigeant, le DRH, le responsable de traitement.

Une équipe technique qui affirme que « tout va bien » ne vous protège pas :

le jour du contrôle, c'est vous qui répondez, et c'est parfois votre nom, et non celui de l'entreprise, qui figure sur le jugement.

Le présent document se lit comme un mode d'emploi.

Il expose :

- L'état du risque,
- Qui peut vous contrôler
- Et avec quels pouvoirs,
- Ce que cela coûte concrètement,
- Et surtout, comment s'en prémunir avant l'incident plutôt qu'après.

L'état du risque — chiffres 2025-2026

En 2025, les autorités européennes ont infligé environ 1,15 milliard d'euros d'amendes RGPD, tous secteurs confondus, pour plus de 330 sanctions.

En France, la CNIL a prononcé 486,8 millions d'euros d'amendes (83 sanctions), contre 55,2 millions en 2024. Une hausse d'un facteur 9. Début 2026, Free a été sanctionné à 42 M€ et France Travail à 5 M€, notamment pour absence d'authentification multifacteur.

Contrairement à une idée reçue, ce ne sont pas seulement les géants du numérique qui trinquent :

32 % des entreprises sanctionnées par la CNIL en 2025 étaient des PME ou des TPE, souvent via sa procédure simplifiée, conçue spécifiquement pour les structures plus petites.

Et 29 % des sanctions prononcées portent sur de simples manquements techniques, données mal sécurisées, non traçables, dispersées entre plusieurs systèmes sans gouvernance claire, pas sur une intention malveillante, mais sur un défaut de maîtrise.

Le rapport LUCY 2026 de l'AMRAE le confirme du côté assurantiel : les sinistres cyber indemnisés en France ont atteint 83,2 millions d'euros en 2025, en hausse de 53 % sur un an, une sinistralité qui touche désormais massivement les entreprises de taille intermédiaire.

Réglementation	Portée	Sanction maximale
RGPD	Données personnelles (UE)	20 M€ ou 4 % du CA mondial
NIS2	Cybersécurité — entités essentielles	10 M€ ou 2 % du CA mondial
DORA	Résilience numérique — secteur	10 M€ ou 5 % du CA
AI Act	Systèmes d'IA à haut risque	35 M€ ou 7 % du CA mondial
nLPD (Suisse)	Responsabilité pénale personnelle du	250 000 CHF, à titre individuel
Loi 25 (Québec)	Sanctions administratives et pénales	25 M CAD ou 4 % du CA mondial

L'entrée en force de NIS2 démarre en octobre 2026.

Pour les prestataires TIC critiques sous DORA, l'astreinte peut atteindre 1 % du chiffre d'affaires mondial par jour de retard.

Suisse : quand la sanction cesse d'être celle de l'entreprise



Depuis le 1er septembre 2023, la nouvelle Loi fédérale sur la protection des données (nLPD) rompt avec la logique du RGPD sur un point essentiel : la sanction ne vise pas l'entreprise, mais la personne physique responsable, le dirigeant, le DRH, le responsable de traitement.

Une amende pénale jusqu'à 250 000 CHF peut être prononcée à titre personnel contre un dirigeant, sans possibilité pour l'entreprise de la prendre en charge.

Les millions partent en fumée pour l'organisation ; les 250 000 francs, eux, partent du compte du dirigeant.

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) instruit et recommande la procédure.

C'est le juge pénal, sur dénonciation du préposé, qui prononce la sanction nommément, sur un jugement, contre une personne qui n'a peut-être fait que laisser filer une situation qu'une équipe technique lui assurait maîtrisée.

Le PFPDT a par ailleurs confirmé publiquement en 2025 que la nLPD s'applique pleinement aux traitements reposant sur l'intelligence artificielle générative, sans attendre de réglementation spécifique.

Une entreprise suisse traitant des données de clients ou de collaborateurs résidant en France ou ailleurs dans l'UE reste en plus soumise au RGPD, du fait de sa portée extraterritoriale. Un même incident de données mal gouvernées peut donc déclencher simultanément une amende RGPD au niveau de l'entreprise et une sanction pénale nLPD au niveau individuel.

Canada : l'un des régimes les plus stricts au monde



Avec la Loi 25 au Québec, renforcée en 2026,

le Canada s'est doté d'un cadre de protection des données qui dépasse sur certains points le RGPD.

Le plafond des sanctions administratives a été relevé à 4 % du chiffre d'affaires mondial ou 25 M CAD (le montant le plus élevé étant retenu), avec des sanctions individuelles pouvant atteindre 100 000 CAD par dirigeant ayant autorisé, ordonné ou consenti à l'infraction.

LE RISQUE CACHÉ : LA QUALITÉ DES DONNÉES

Un second risque, moins visible mais tout aussi coûteux, existe indépendamment de toute sanction.

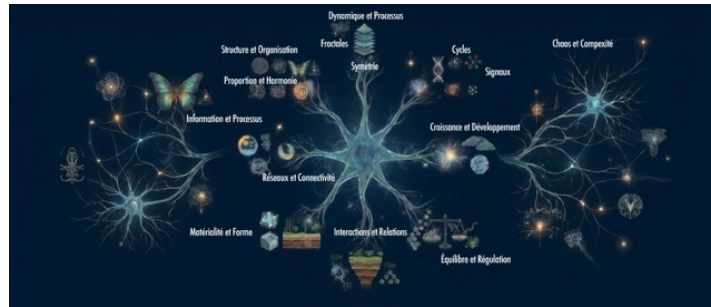
Selon Gartner, la mauvaise qualité des données coûte en moyenne 12,9 à 15 millions de dollars par an à une organisation, entre pertes de revenus, inefficacités opérationnelles et non-conformité réglementaire.

Une étude du MIT Sloan Management Review, menée avec la Cork University Business School, estime que les entreprises perdent 15 à 25 % de leur chiffre d'affaires annuel à cause de données de mauvaise qualité.

Un chiffre plus ancien mais toujours cité, publié par IBM en 2016 dans la Harvard Business Review, évaluait ce coût à 3 100 milliards de dollars par an pour la seule économie américaine.

Concrètement, ce coût se cache dans des rapports produits en plusieurs jours au lieu de quelques minutes, des décisions prises sur des données incomplètes ou dupliquées, et des risques juridiques, financiers et humains qui restent invisibles avec des technologies non appropriées.

Le risque RH — un terrain particulièrement sanctionné

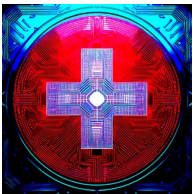


La fonction RH n'est pas un angle mort marginal de la conformité des données : c'est l'un des terrains les plus sanctionnés, en France comme en Suisse, pour trois raisons structurelles.

- Le consentement y est quasi inopérant : le lien de subordination rend juridiquement fragile le consentement d'un salarié à voir ses données traitées.
- Les dossiers RH concentrent des données particulièrement sensibles : santé, éléments fiscaux et bancaires, parfois opinions ou appartenance syndicale.
- La surveillance (badges, vidéosurveillance, suivi d'activité) y est omniprésente et rarement documentée dans les règles. La CNIL rappelle que les journaux de badgeage doivent en principe être conservés trois mois maximum, sauf justification spécifique.

Les sanctions récentes le confirment : Spartoo (250 000 €), Cdiscount (230 000 €), JobTeaser (200 000 €) et pap.fr (30 000 €, 2024).

Voici des montants qui touchent des entreprises de tailles très différentes, pas seulement les grands groupes.



En Suisse, trois textes se combinent et surprennent souvent les directions RH habituées au seul RGPD :

1. l'article 328b du Code des obligations limite le traitement des données d'un collaborateur à ce qui concerne son aptitude au poste ou l'exécution du contrat ;
2. l'article 26 de l'Ordonnance 3 relative à la loi sur le travail interdit catégoriquement les systèmes de surveillance comportementale continue, ce qui est une interdiction de principe plus stricte que le RGPD ;
3. l'article 8 de la nLPD impose une obligation positive de former les collaborateurs au traitement des données, de façon effective et démontrable.

Qui peut vous contrôler, et avec quels pouvoirs



Dans les trois pays, le schéma est le même : des autorités administratives aux pouvoirs d'enquête de plus en plus étendus, qui peuvent transmettre le dossier à la police judiciaire et au parquet lorsque les faits relèvent aussi du pénal,

La perquisition au sens strict et l'arrestation restent l'apanage du pouvoir judiciaire.

- **France** : la CNIL peut contrôler sur place (art. 19 de la loi Informatique et Libertés), copier tout document et saisir sa formation restreinte pour sanctionner ; l'ANSSI (NIS2) mène audits et inspections ; l'AMF dispose d'un vrai pouvoir de perquisition et de saisie, avec le concours possible d'officiers de police judiciaire.
- **Suisse** : le PFPDT enquête, demande l'accès aux systèmes et peut ordonner une mise en conformité, mais ne peut ni perquisitionner sans mandat, ni sanctionner financièrement seul le juge pénal cantonal le peut, sur dénonciation.
- **Canada** : la Commission d'accès à l'information (CAI) dispose d'un pouvoir de demande péremptoire, opposable à toute personne, assujettie ou non à la loi, sous peine d'amende en cas de refus ; les sanctions pénales relèvent des tribunaux.

Mode d'emploi : comment éviter cette situation

La conformité doit être intégrée nativement dans les pipelines de données, dès la conception, pas ajoutée après coup ni patchée au gré des besoins.

En France

- Cartographier l'ensemble des traitements de données et tenir le registre RGPD à jour en continu. L'absence de cartographie est la cause la plus fréquente des sanctions récentes.
- Désigner formellement un DPO et documenter ses décisions.
- Anticiper l'entrée en force de NIS2 (octobre 2026) : audits, SOC, preuves de conformité prêtes avant tout contrôle de l'ANSSI.
- Pour les entités financières, se mettre en ordre de marche DORA avant les premiers cycles d'inspection de l'ACPR et de l'AMF.
- Exiger de tout fournisseur technologique une preuve contractuelle de conformité opérable.
- Mettre en place un plan de réponse aux incidents testé, avec notification à la CNIL et à l'ANSSI dans les délais impartis.

En Suisse

- Chaque dirigeant, DRH ou responsable de traitement doit savoir précisément ce qui relève de sa responsabilité individuelle, avec une trace écrite de sa diligence.
- Coopérer de façon proactive avec le PFPDT réduit fortement le risque d'une dénonciation transmise au juge pénal.
- Réaliser les analyses d'impact et les mesures de sécurité exigées par la nLPD avant tout traitement à risque, plutôt qu'en réaction à une enquête.
- Former les dirigeants et responsables de traitement à leur exposition pénale personnelle — un point que beaucoup sous-estiment encore.

Au Canada

- Désigner sans délai un responsable de la protection des renseignements personnels, obligatoire sous la Loi 25.
- Réaliser une analyse d'impact avant tout traitement de données sensibles.
- Mettre en place la notification obligatoire des incidents et un registre systématique des violations.
- Documenter la diligence de chaque dirigeant ayant autorité sur les traitements.

Ce qui protège une organisation n'est pas l'absence d'incident, mais la preuve d'une diligence raisonnable continue : gouvernance documentée, contrats fournisseurs exigeants, formation des équipes, journaux d'audit disponibles à tout moment.



Pourquoi nous vous offrons de livre ?

Pour expliquer le niveau de sécurité juridique et financière qu'il vous est indispensable, si ce n'est obligatoire d'obtenir 24h sur 24 pour être en conformité et en sécurité.

De plus ce livre blanc sur les risques n'a de valeur que si la réponse qu'il propose est elle-même vérifiable, mesurable, certifiante et conforme.

Voici donc, ce qui, dans Symbiocratie / DEMS-Nixus, peut être contrôlé indépendamment, par vous même, plutôt que pris sur parole.

UN FINANCEMENT PUBLIC VÉRIFIABLE, PAS UNE PROMESSE COMMERCIALE

Le projet DEMS-Nixus, a été sélectionné et financé par la Commission européenne dans le cadre du programme Horizon 2020, Instrument PME phase 2, sous la convention de subvention n°871647.

Le projet s'est déroulé de septembre 2019 à février 2021, pour un coût total de 2 863 500 € et une contribution de l'Union européenne de 2 004 450 €. Ces informations sont publiques et vérifiables sur le portail officiel CORDIS de la Commission européenne (cordis.europa.eu/project/id/871647).

Ce financement n'est ni une allégation, ni un argument marketing : c'est un fait administratif public, consultable par n'importe quel dirigeant, DPO ou juriste avant toute décision d'achat.

UNE GOUVERNANCE QUI NE DÉPLACE JAMAIS LA DONNÉE

Le principe de Data Sovereignty signifie que Symbiocratie / DEMS-Nixus se connecte aux systèmes existants sans migrer les données.

Cela réduit mécaniquement la surface d'attaque et la nouvelle exposition juridique que créerait, par nature, tout déplacement ou toute duplication de données sensibles vers un tiers.

DES RÉSULTATS MESURÉS, PAS DÉCLARÉS

Cas client bancaire : la cartographie sémantique a révélé que 89 % des données ne participaient pas au calcul de la valeur nette d'actifs de l'établissement, et a permis d'identifier 80 000 comptes représentant plusieurs milliards de dollars de risque de non-conformité KYC.

Délai de création de valeur réduit de 3-6 mois à 3 jours, selon les objectifs mêmes du projet déposés auprès de la Commission européenne.

Coûts de transformation digitale réduits de 30 à 80 % selon les cas d'usage.

Taux de conformité maintenu à 100 % en continu, avec détection des écarts avant qu'ils ne deviennent des incidents, Ceci est plus sécuritaire qu'un audit annuel qui laisse le risque s'accumuler silencieusement entre deux contrôles.

CE QUI RESTE À VOTRE CHARGE DE VÉRIFIER

Par souci de rigueur, ce document ne reprend pas certaines mentions de reconnaissance (analystes, distinctions d'accélérateurs) car nous recommandons à tout dirigeant d'exiger ce même niveau de preuve de la part de tout fournisseur technologique.



Questions fréquentes

Quelle est la différence entre le RGPD et la nLPD ?

Le RGPD sanctionne l'entreprise elle-même, jusqu'à 4 % du chiffre d'affaires mondial. La nLPD suisse sanctionne pénalement la personne physique responsable, jusqu'à 250 000 CHF.

Une entreprise suisse doit-elle appliquer le RGPD ?

Oui, dès lors qu'elle traite des données de résidents de l'Union européenne, indépendamment de son siège social.

Combien coûte la mauvaise qualité des données à une entreprise ?

Entre 12,9 et 15 millions de dollars par an en moyenne selon Gartner, soit 15 à 25 % du chiffre d'affaires selon le MIT Sloan Management Review.

Un outil de tri de CV par intelligence artificielle est-il concerné par l'AI Act ?

En France, oui : depuis août 2025, la CNIL contrôle le respect de l'AI Act pour les systèmes d'IA à haut risque utilisés en recrutement, qui doivent démontrer une supervision humaine effective.

EN RÉSUMÉ

La non-conformité réglementaire, la mauvaise qualité des données et le risque RH ne sont pas trois problèmes distincts : ce sont trois symptômes d'une même cause.

- Des données dispersées dans des systèmes qui ne se parlent pas,
- Pas de gouvernance claire
- Pas de preuve de diligence continue.

Dans les trois juridictions étudiées, la tendance est identique :

les montants augmentent, les contrôles se multiplient, et la responsabilité individuelle des dirigeants devient la norme plutôt que l'exception.

La différence entre le dirigeant qui subit et celui qui anticipe se joue toujours avant l'incident, jamais après.



En savoir plus

Pour un audit de conformité légale, en respect total de la Data Excellence Science, en maximum 3 jours sans rien toucher de vos données :

didier@la-machina.xyz

Sources

RGPD 2025 : 1,15 Md€ d'Amendes – Bilan et Perspectives 2026 — rgpdkit.fr

Sanctions CNIL : la liste des amendes RGPD (mise à jour juillet 2026) — dpliance.com

Étude LUCY 2026 — AMRAE (Lumière sur la Cyberassurance)

Les dispositions pénales de la nLPD — Graduate Institute

Sanctions et amendes de la Loi 25 — loi25simple.ca

Quebec Law 25 in 2026: What the Recent Amendments Mean — Sherlock Forensics

Data Excellence Management System / DEMS-Nexus — Grant Agreement n°871647, CORDIS, Commission européenne (cordis.europa.eu/project/id/871647)

Guide RGPD du recrutement — CNIL

Article 328b du Code des obligations ; Ordonnance 3 relative à la loi sur le travail (OLT 3), art. 26 ; art. 8 nLPD — droit suisse