GUIDE DE CONFORMITÉ

RGPD & nLPD

pour les infrastructures IT des PME suisses

ÉDITION 2026

GUIDE DE CONFORMITÉ

SOMMAIRE

CONTACT

Pour toute question concernant ce guide, veuillez contacter votre représentant conformité AWSMTECH.

PREMIÈRE PARTIE

L’ESSENTIEL

Tout ce qu’il faut savoir, en une page.

01 — POURQUOI C'EST IMPORTANT

Ce que la loi exige de vous

Les PME suisses doivent se conformer à la fois au **RGPD** européen et à la **Loi fédérale sur la protection des données** suisse (nLPD). Ces lois s'appliquent à toutes les organisations qui traitent des données personnelles, quelle que soit leur taille.

Le non-respect de ces obligations expose à des amendes pouvant atteindre **20 millions d'euros** au titre du RGPD et **CHF 250'000** au titre de la nLPD, ainsi qu'à un risque important pour la réputation.

02 — PRINCIPES JURIDIQUES CLÉS

Les quatre piliers de la conformité

PRINCIPE	DESCRIPTION
Licéité et transparence	Informer clairement les personnes concernées sur l'utilisation des données et obtenir un consentement valable. Informer clairement les utilisateurs sur l'utilisation des données et obtenir un consentement valable.
Minimisation des données	Ne collecter que les données strictement nécessaires.
Sécurité et confidentialité	Protéger les données grâce au chiffrement, au contrôle des accès et à des plans de réponse aux incidents.
Responsabilité	Tenir des registres, attribuer les responsabilités et former les collaborateurs.

03 — CHECKLIST DE CONFORMITÉ IT

Dix étapes pour sécuriser votre infrastructure

ÉTAPE	ACTION	RESPONSABLE
Attribuer les responsabilités	Désigner un responsable protection des données ou un délégué à la protection des données (DPO). Désigner un responsable protection des données ou un DPO.	Direction
Cartographier les données et les risques	Auditer les flux de données et évaluer les écarts.	IT + Protection des données
Base légale et consentement	Justifier chaque utilisation des données (consentement, contrat, etc.).	Juridique + IT
Mettre à jour les politiques	Publier la déclaration de confidentialité et les directives internes.	Juridique

ÉTAPE	ACTION	RESPONSABLE
Mettre en place les mesures de sécurité	Chiffrer les données, imposer l'authentification multifacteur (MFA), surveiller les systèmes. Chiffrer les données, imposer la MFA, surveiller les systèmes.	Sécurité IT
Conservation et minimisation	Supprimer les données inutiles et définir des règles de conservation.	IT + Juridique
Gérer les prestataires	Signer des accords de traitement des données (DPA).	Achats
Permettre les demandes liées aux droits	Permettre aux personnes concernées d'accéder à leurs données, de les corriger ou de les supprimer. Permettre aux utilisateurs d'accéder à leurs données, de les corriger ou de les supprimer.	IT + Support
Former les collaborateurs	Sensibiliser les collaborateurs à la protection des données et à la sécurité.	RH + IT
Plan de réponse aux violations	Préparer et tester les procédures de réponse aux incidents.	IT + Protection des données

04 — INDISPENSABLES TECHNIQUES

Ce que votre infrastructure doit garantir

CHIFFREMENT **au repos et en transit**	**CONTRÔLE DES ACCÈS** **rôles et MFA**	**CONSERVATION** **suppression automatisée**	**SURVEILLANCE** **détection des incidents**

05 — SUISSE VS UE

Différences clés à connaître

— Le droit suisse protège **uniquement les personnes physiques**, et non les entreprises.

— La notification d'une violation doit être faite **dans les meilleurs délais**, et non dans un délai fixe de 72 heures.

— Les amendes visent principalement les **personnes responsables**, et pas uniquement les entreprises.

— La base légale est plus flexible, mais ne doit **jamais porter atteinte à la sphère privée**.

DEUXIÈME PARTIE

LE GUIDE

Comprendre, mettre en œuvre, comparer.

06 — VUE D'ENSEMBLE

RGPD et nLPD suisse en bref

RGPD (Règlement général sur la protection des données)

Règlement européen sur la protection des données en vigueur depuis 2018, il fixe des règles strictes sur la manière dont les organisations traitent les données personnelles. Le RGPD a une **portée extraterritoriale** : il s'applique aux entreprises situées hors de l'UE — y compris les PME suisses — si elles proposent des biens ou services à des résidents de l'UE ou surveillent leur comportement en ligne.

Il impose des principes tels que la licéité, la transparence, la minimisation des données, la limitation des finalités, l'exactitude, la limitation de la conservation, l'intégrité/confidentialité et la responsabilité (article 5 RGPD). Il introduit la **protection des données dès la conception et par défaut**, la notification obligatoire des violations dans les 72 heures et des amendes importantes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial.

nLPD suisse (nouvelle Loi fédérale sur la protection des données, 2023)

La loi suisse révisée sur la protection des données, en vigueur depuis le 1er septembre 2023, s'aligne étroitement sur les principes du RGPD afin de maintenir l'adéquation avec l'UE. Elle renforce les droits des personnes et introduit la **protection des données dès la conception et par défaut** dans le droit suisse.

Point clé : elle **s'applique uniquement aux données personnelles des personnes physiques** — contrairement à l'ancienne loi, elle ne protège plus les données des personnes morales. Les PME suisses doivent s'y conformer même si elles ne relèvent pas du champ d'application du RGPD. La nLPD exige la tenue d'un registre des activités de traitement, avec certaines exemptions pour les PME à faible risque, ainsi qu'une notification « rapide » des violations à l'autorité compétente.

Points communs et importance

Le RGPD et la nLPD visent tous deux à protéger les données personnelles et à donner aux personnes le contrôle sur leurs informations. Pour l'équipe IT d'une PME suisse, cela signifie **concevoir une infrastructure IT conforme aux deux cadres à la fois**. Une entreprise conforme au RGPD respecte déjà la plupart des obligations de la nLPD, cette dernière ayant été conçue pour être compatible.

07 — EXIGENCES DE CONFORMITÉ

Exigences clés de conformité IT pour les PME

1. Traitement licite et transparent des données

Toute activité de traitement de données personnelles doit reposer sur une base légale et être transparente pour la personne concernée. Le RGPD définit six bases légales (consentement, contrat, obligation légale, intérêts vitaux, mission d'intérêt public, intérêts légitimes — article 6). La nLPD suisse exige également une justification du traitement des données.

Action recommandée : documenter toutes les catégories de données personnelles collectées et traitées par vos systèmes IT (données clients, données collaborateurs, etc.) et indiquer la base légale de chacune. Fournir des déclarations de confidentialité claires aux personnes concernées. Éviter de collecter des données inutiles et ne les utiliser que pour les finalités annoncées. Vos systèmes IT doivent être prêts à **répondre aux demandes des personnes concernées** (accès, correction, suppression, portabilité).

2. Stockage et conservation des données

Les données personnelles doivent être stockées de manière sécurisée et ne pas être conservées plus longtemps que nécessaire. Selon le principe de « limitation de la conservation » du RGPD, les données doivent être supprimées ou anonymisées lorsqu'elles ne sont plus nécessaires. La nLPD suisse attend le même comportement.

Action recommandée : mettre en place des politiques de conservation — supprimer ou archiver automatiquement les données après une période définie. S'assurer que les sauvegardes et archives sont également couvertes par ces limites. Si vous utilisez des services cloud à l'étranger, confirmer que les transferts internationaux respectent les règles RGPD/nLPD (décision d'adéquation ou clauses contractuelles types). Documenter la durée de conservation de chaque catégorie de données dans votre registre de traitement.

3. Contrôle des accès et sécurité des données

Le RGPD et la nLPD imposent tous deux de protéger les données personnelles contre les accès non autorisés, la perte ou les violations — principe d'« intégrité et confidentialité » (article 5(1)(f) et article 32 RGPD), qui exige des **mesures techniques et organisationnelles appropriées**.

Action recommandée : limiter les accès selon le principe du besoin d'en connaître (contrôle d'accès basé sur les rôles), imposer une authentification forte, notamment l'authentification multifacteur (MFA), et maintenir les systèmes à jour. Le **chiffrement** des données au repos et en transit est explicitement recommandé par l'article 32 RGPD : bases de données chiffrées, HTTPS pour toutes les transmissions. La nLPD suisse impose des standards de sécurité minimaux similaires. Il convient également de maintenir une protection anti-malware et un plan de reprise après sinistre.

4. Notification et réponse aux violations

Malgré les meilleures précautions, des violations de données peuvent survenir. **Selon le RGPD**, toute violation susceptible de présenter un risque pour les droits des personnes doit être signalée à l'autorité de contrôle **dans les 72 heures** suivant sa découverte. **Selon la nLPD suisse**, les violations doivent être annoncées au Préposé fédéral à la protection des données et à la transparence (PFPDT) **« dans les meilleurs délais »** lorsqu'il existe un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées — sans délai horaire fixe, mais sans retard injustifié.

Action recommandée : mettre en place un **plan de réponse aux incidents** — procédures d'identification et d'analyse des violations, chaîne de remontée interne claire et modèle de notification à l'autorité. Former les collaborateurs à reconnaître les incidents. Si le délai de 72 heures prévu par le RGPD est dépassé, le retard doit être justifié ; les personnes concernées peuvent également devoir être informées si la violation est grave.

5. Responsabilité et documentation

La conformité n'est pas une action ponctuelle : le RGPD et la nLPD exigent une **responsabilité continue**. Vous devez donc pouvoir démontrer votre conformité à tout moment. L'article 30 du RGPD impose aux responsables du traitement de tenir un **registre des activités de traitement**, avec une exemption possible pour les entreprises de moins de 250 collaborateurs dont les traitements sont occasionnels ou à faible risque. La nouvelle loi suisse impose également un registre de traitement, avec une exemption comparable.

Action recommandée : constituer un inventaire des traitements de données — finalité, types de données, catégories de personnes concernées, destinataires externes, durée de conservation et mesures de sécurité appliquées. Définir des politiques internes (sécurité IT, protection des données) et former les collaborateurs. Attribuer clairement la responsabilité de la conformité : la nLPD n'impose pas de DPO, mais la pratique est recommandée. Auditer et mettre à jour régulièrement votre documentation.

08 — STRATÉGIES PRATIQUES

Stratégies pratiques pour les équipes IT

Mettre en œuvre le RGPD et la nLPD peut sembler complexe, mais quelques stratégies concrètes permettent de transformer les obligations légales en pratiques IT quotidiennes.

Cartographie et classification des données

Commencez par une **cartographie des données** : identifiez tous les emplacements où l'infrastructure IT de votre PME stocke ou transmet des données personnelles (bases de données, serveurs de fichiers, ordinateurs portables, services cloud, messagerie). Classez les données selon leur sensibilité. Cette cartographie soutient toutes les autres étapes et met en évidence les flux transfrontaliers pertinents au regard du RGPD ou de la nLPD.

Appliquer la protection des données dès la conception

Intégrez la protection des données et la sécurité dans les projets IT dès le départ : contrôle d'accès granulaire, chiffrement, possibilité de supprimer ou d'exporter les données. Les paramètres par défaut doivent être favorables à la confidentialité. Réalisez une **analyse d'impact relative à la protection des données (AIPD)** pour tout traitement à risque élevé, comme l'exige le RGPD.

Chiffrement renforcé partout

Le chiffrement rend les données illisibles sans la clé : c'est une protection essentielle contre les violations. Chiffrez les données **au repos** (disques, bases de données, sauvegardes) et **en transit** (TLS/SSL, VPN, e-mails sensibles). Gérez les clés séparément des données. Les autorités considèrent souvent le chiffrement comme un facteur atténuant lors d'une enquête.

Sauvegardes et restauration sécurisées

Maintenez des **sauvegardes régulières**, chiffrées et protégées par des contrôles d'accès. Testez-les périodiquement afin de confirmer que les données peuvent effectivement être restaurées. Un système de sauvegarde robuste permet de rétablir rapidement les données personnelles après un incident, comme l'attendent le RGPD et la nLPD.

Gestion des accès et surveillance

Mettez en place un processus de gestion des identités et des accès (IAM) pour l'attribution et le retrait des droits, activez la journalisation sur les systèmes contenant des données sensibles et revoyez régulièrement les privilèges selon le principe du moindre privilège. **Chiffrement + contrôle des accès + surveillance** forment le socle de la sécurité des données.

Gestion des prestataires et partenaires

Tout sous-traitant traitant des données pour votre compte doit être couvert par un **accord de traitement des données (DPA)** conforme à l'article 28 du RGPD. Utilisez des clauses contractuelles types pour les transferts hors d'une juridiction adéquate, évaluez la sécurité des prestataires (ISO 27001, questionnaires) et limitez les données partagées au strict nécessaire.

Formation et politiques internes

La technologie seule ne suffit pas : formez les collaborateurs aux bonnes pratiques de protection des données, au traitement des demandes de suppression et au signalement des incidents. Une équipe informée renforce les mesures IT et réduit le risque d'erreur humaine.

En appliquant ces stratégies, les équipes IT des PME créent un environnement où la conformité fait partie des opérations quotidiennes — et non d'une correction de dernière minute.

09 — COMPARAISON

RGPD vs nLPD : différences et points communs

Bien que le RGPD et la nLPD suisse partagent le même esprit et la plupart de leurs exigences, quelques différences importantes méritent d'être connues, en particulier pour les équipes IT et conformité.

Champ d'application

Les deux lois protègent les données des **personnes physiques**. Le RGPD s'applique à toute organisation qui traite des données de résidents de l'UE, quel que soit son lieu d'établissement. La nLPD s'applique principalement aux traitements effectués en Suisse ou ayant un effet sur des personnes en Suisse. Nouveauté de la nLPD : elle ne protège plus les données des **personnes morales**, contrairement à l'ancienne loi suisse.

Autorité de contrôle et amendes

Le RGPD prévoit des amendes administratives pouvant atteindre **20 millions d'euros ou 4 % du chiffre d'affaires mondial**, prononcées par les autorités de chaque pays de l'UE. La nLPD plafonne les amendes à **CHF 250'000**, généralement dirigées contre les **personnes responsables** plutôt que contre l'entreprise elle-même ; le PFPDT ne prononce pas directement d'amendes, les cas graves pouvant être transmis aux autorités pénales.

Délai de notification des violations

Le RGPD fixe un délai clair de **72 heures** après la découverte d'une violation. La nLPD exige une notification **« dans les meilleurs délais »** lorsqu'il existe un risque élevé — une norme plus flexible, mais tout aussi urgente en pratique. Il est conseillé de viser une fenêtre similaire de 72 heures dans les deux cas.

Délégué à la protection des données (DPO)

Le RGPD **impose un DPO** à certaines organisations (autorités publiques, surveillance à grande échelle, traitements de données sensibles — article 37). La nLPD **n'impose pas de DPO**, mais permet la désignation volontaire d'un conseiller à la protection des données, ce qui reste une bonne pratique.

Registres de traitement et PME

Les deux lois exigent un registre des activités de traitement, avec des exemptions comparables pour les petites organisations à faible risque. En pratique, la conformité au RGPD sur ce point couvre la plupart des obligations de la nLPD.

Droits des personnes et consentement

Les droits accordés aux personnes (accès, rectification, suppression, opposition, portabilité) sont **très similaires** entre le RGPD et la nLPD, cette dernière ayant aligné ses standards sur le RGPD. Certaines nuances existent concernant le consentement pour le profilage à risque élevé.

Transferts internationaux de données

Le RGPD limite les transferts hors de l'UE/EEE, sauf en présence d'une protection adéquate ou de garanties appropriées (clauses contractuelles types, règles d'entreprise contraignantes). La nLPD applique une logique comparable, avec une liste de pays adéquats largement alignée sur celle de l'UE. L'UE et la Suisse se reconnaissent mutuellement comme offrant une protection adéquate.

En résumé, le RGPD et la nLPD ont plus de points communs que de différences. Les principes fondamentaux — licéité, transparence, sécurité, droits des personnes — et les tâches opérationnelles sont, dans les faits, très similaires. Il est judicieux de s'aligner sur l'exigence la plus stricte de chaque cadre : viser une notification dans un délai comparable à 72

heures lorsque la situation l'exige, et garder à l'esprit le plafond de 4 % du chiffre d'affaires comme niveau de risque maximal.