GUIDE DE CONFORMITÉ · PME

Checklist de Conformité

Dix étapes concrètes pour aligner vos pratiques informatiques et de protection des données sur le RGPD et le nLPD suisse.

RGPD · Règlement UE 2016/679 nLPD suisse

AVENUE DE LA GARE 46B – 1920 MARTIGNY
AVENUE LOUIS-CASAÏ 71 – 1216 COINTRIN
MAIL@AWSMTECH.CH – WWW.AWSMTECH.CH – +41 (0)22 552 60 70

Pourquoi cette checklist

Voici une checklist des étapes et pratiques clés pour garantir la conformité au RGPD et au nLPD. Les PME peuvent l'utiliser comme référence pour évaluer leur niveau de préparation en matière informatique et de protection des données.

Chaque étape correspond à un aspect essentiel de la conformité RGPD / nLPD. En suivant cette checklist dans l'ordre, votre organisation peut traiter méthodiquement ses obligations, de la gouvernance de base jusqu'à l'amélioration continue.

01 – 03	**FONDATIONS**	Les fondations : responsabilité, sensibilisation, transparence.
04 – 05	**SÉCURITÉ & DONNÉES**	Sécurité et gestion des données au sein des opérations informatiques.
06	**TIERS**	La conformité des prestataires — un point souvent négligé.
07	**GESTION DES INCIDENTS**	La préparation au pire scénario : une violation de données.
08	**DROITS DES PERSONNES**	S'assurer que les droits des personnes sont respectés en pratique.
09 – 10	**HUMAIN & CONTINUITÉ**	Le facteur humain et le caractère continu de la conformité.

COMMENT UTILISER CE GUIDE

Parcourez les dix étapes avec votre responsable informatique et votre direction. Chaque fiche des pages suivantes précise l'action à mener et ce à quoi ressemble sa mise en œuvre concrète — utilisez-la pour évaluer où vous en êtes aujourd'hui.

Étapes 01–06

01 FONDATIONS

Désigner un responsable

Désigner une personne ou une équipe responsable de la conformité — un délégué à la protection des données (DPO) ou un coordinateur. S'assurer que la direction soutient cette démarche et comprend sa responsabilité.

02 FONDATIONS

Cartographier vos données

Établir une cartographie détaillée des données personnelles au sein de vos systèmes informatiques. Identifier les données détenues, leur lieu de stockage, leur circulation et les personnes y ayant accès. Consigner la finalité et la base légale de chaque traitement.

03 FONDATIONS

Mettre à jour les mentions d'information

Maintenir des mentions d'information claires et à jour informant clients et employés sur la collecte, l'utilisation, la conservation des données et leurs droits. Les rendre facilement accessibles — sur votre site web, par exemple.

04 SÉCURITÉ & DONNÉES

Mettre en œuvre des mesures de sécurité

Appliquer des contrôles de sécurité informatique adaptés : restrictions d'accès, authentification forte, chiffrement des données au repos et en transit, et sécurité réseau (pare-feux, antivirus). Mettre en place des sauvegardes sécurisées et un plan de reprise après sinistre.

05 SÉCURITÉ & DONNÉES

Définir des règles de conservation

Définir et documenter les durées de conservation pour chaque type de donnée. Configurer les systèmes pour supprimer ou archiver les données à l'expiration de ces durées, avec un effacement sécurisé. Ne jamais conserver de données personnelles au-delà du nécessaire.

06 TIERS

Gérer les risques liés aux tiers

Passer en revue chaque prestataire et partenaire traitant des données personnelles. Signer des contrats de sous-traitance incluant des clauses RGPD / nLPD, utiliser des clauses contractuelles types pour les transferts internationaux, et vérifier que les sous-traitants appliquent de bonnes pratiques de sécurité.

Étapes 07–10

07 GESTION DES INCIDENTS

Se préparer aux violations de données

Élaborer un plan de réponse aux incidents définissant les étapes à suivre en cas de violation — confinement, investigation, escalade interne — avec des modèles prêts à l'emploi pour notifier la CNIL et les personnes concernées. Viser une notification sous 72 heures.

08 DROITS DES PERSONNES

Garantir les droits des personnes

Mettre en place des procédures pour enregistrer et répondre aux demandes des personnes — accès, rectification, effacement ou opposition — dans le délai légal, généralement 30 jours sous le RGPD. S'assurer que les équipes IT peuvent retrouver ou supprimer les données sur demande, dans tous les systèmes.

09 HUMAIN & CONTINUITÉ

Former les collaborateurs

Organiser des formations régulières sur les fondamentaux de la protection des données et vos politiques internes. Apprendre aux équipes à sécuriser les données — repérer les emails de phishing, par exemple — et à traiter correctement les demandes liées à la vie privée.

10 HUMAIN & CONTINUITÉ

Surveiller et améliorer en continu

Auditer régulièrement votre conformité. Maintenir à jour le registre des traitements, suivre des indicateurs comme le nombre d'incidents et les délais de réponse, et rester informé des évolutions réglementaires. Considérer la protection des données comme un processus continu, non un projet ponctuel.

Pour aller plus loin

POUR ALLER PLUS LOIN

Référez-vous toujours aux textes faisant autorité. Les textes officiels — le RGPD (Règlement UE 2016/679) et le nLPD suisse — restent les références principales ; le site du PFPDT propose des synthèses détaillées des dispositions de la nouvelle loi suisse. Des autorités telles que la CNIL, le Comité européen de la protection des données (CEPD) ou le PFPDT publient également des guides et des FAQ utiles aux PME.

En restant informés grâce à ces sources et en suivant cette checklist, les responsables informatiques et les dirigeants de PME peuvent conduire leur organisation vers une conformité complète au RGPD et au nLPD — protégeant ainsi les données de leurs clients et leur activité.

L’infogérance IT de confiance
pour les métiers sensibles.

AVENUE DE LA GARE 46B – 1920 MARTIGNY
AVENUE LOUIS-CASAÏ 71 – 1216 COINTRIN
MAIL@AWSMTECH.CH – WWW.AWSMTECH.CH – +41 (0)22 552 60 70