LA PROTECTION DES DONNÉES EN SUISSE

Guide pratique pour indépendants et micro-entreprises

Edition 2026

Collection SimplE-IAdmin – Guides pour indépendants et micro-entreprises

Dans la même collection :

Guide 1
Devenir indépendant en Suisse

Guide 2
La protection des données pour indépendants et micro-entreprises

À QUI S’ADRESSE CE GUIDE ?

Ce guide s’adresse aux :

— indépendants,
— artisans,
— professions libérales,
— micro-entreprises,
— petites PME suisses,
qui traitent des données personnelles dans le cadre de leur activité.
Il est particulièrement adapté aux structures de 1 à 5 personnes, et reste pertinent jusqu’à 10 collaborateurs.

Ce guide est fait pour toi si :

— tu factures des clients,
— tu conserves des coordonnées,
— tu utilises un logiciel de gestion,
— tu envoies des devis par email,
— tu stockes des données sur ton ordinateur ou dans un cloud.
Autrement dit : si tu exerces une activité professionnelle, tu es concerné.

Ce guide n’est pas :

— un traité juridique universitaire,
— un manuel technique informatique avancé,
— une formation destinée aux grandes multinationales,
Il ne remplace pas un conseil juridique personnalisé dans des situations complexes.

Ce guide a été conçu pour :

— expliquer la LPD sans jargon inutile,
— donner un ordre logique d’action,
— proposer des modèles concrets,
— permettre une mise en conformité proportionnée.

PRÉAMBULE

Pourquoi la protection des données concerne aussi les petites entreprises

Lorsque l’on parle de protection des données, beaucoup pensent immédiatement aux grandes entreprises ou aux plateformes numériques.

Pourtant, une coiffeuse, un peintre indépendant ou un thérapeute traite également des données personnelles :
— coordonnées clients,
— informations de facturation,
— historiques de prestations,
— parfois données sensibles.

La Loi fédérale sur la protection des données (LPD) ne distingue pas selon la taille de l’entreprise.
Elle exige une chose simple : des mesures proportionnées.
Ce guide ne vise pas la perfection technique.

Il vise :
— la compréhension,
— l’organisation,
— la cohérence,
— la démonstration d’une démarche sérieuse.

La conformité s’inscrit dans une logique progressive et évolutive.
Elle repose sur une méthode structurée.

SOMMAIRE
À qui s’adresse ce guide

PARTIE I – COMPRENDRE LE CADRE LÉGAL

Introduction

Avant de sécuriser, il faut comprendre.
La protection des données repose sur des principes simples.
Cette partie clarifie :

— ce qu'est une donnée personnelle,
— ce que signifie " traiter " une donnée,
— quels sont les droits des personnes,
— dans quels cas le RGPD européen peut s'appliquer.

Chapitre 1 – Les bases de la LPD expliquées simplement

La LPD repose sur quatre principes fondamentaux :

1. Qu'est-ce qu'une donnée personnelle ?

Toute information permettant d'identifier une personne.
Exemples :

— nom,
— adresse,
— email,
— numéro de téléphone,
— données de facturation.

Même une simple adresse email est une donnée personnelle.

2. Qu’est-ce qu’un traitement ?

Un traitement est toute action effectuée sur une donnée :

— collecte,
— enregistrement,
— stockage,
— modification,
— transmission,
— suppression.

Envoyer une facture par email = traitement.
Archiver un devis = traitement.

3. Les principes fondamentaux

Transparence

La personne doit savoir que ses données sont collectées.

Finalité

Les données ne doivent être utilisées que pour un objectif précis.

Proportionnalité

Ne collecter que ce qui est nécessaire.

Sécurité

Mettre en place des mesures adaptées.

Chapitre 2 – Les droits des personnes

Toute personne peut demander :

— l’accès à ses données,
— leur rectification,
— leur suppression (dans certains cas),
— des informations sur leur utilisation.

Le droit d’accès

Une personne peut, par exemple, écrire :
“ Quelles données avez-vous sur moi ? ”

Tu dois répondre dans un délai de 30 jours.
La réponse doit être claire et compréhensible.

Peut-on refuser ?

Dans certains cas :

— si cela concerne des tiers,
— si la loi impose une conservation,
— si la demande est abusive.

Mais un refus doit être justifié.

Chapitre 3 – LPD suisse et RGPD européen

Beaucoup confondent les deux.
La LPD est la loi suisse.
Le RGPD est la loi européenne.

Quand la LPD suffit-elle ?

Si ton activité est :

— en Suisse,
— avec des clients suisses,
— sans ciblage de résidents européens.

La LPD est ton cadre principal.

Quand le RGPD peut-il s’appliquer ?

Si tu :

— vends activement à des clients dans l’UE,
— livres en France ou en Allemagne,
— cibles des résidents européens.

Différence notable

Le RGPD prévoit des amendes administratives très élevées.
La LPD prévoit des sanctions pénales ciblées, principalement en cas de violation intentionnelle.

PARTIE II – IDENTIFIER ET ORGANISER

Introduction

Comprendre la loi ne suffit pas.

Il faut savoir :

— quelles données tu traites,
— où elles se trouvent,
— qui y a accès.

L’organisation est souvent la clé.

Chapitre 4 – Identifier les données dans ton entreprise

La première étape est la cartographie.

Pose-toi ces questions :

— quelles sont les données que je collecte ?
— où sont-elles stockées ?
— quelles personnes y ont accès ?
— combien de temps sont-elles conservées ?

Renvoi : Annexe 1 – Inventaire des données (page 77)

Chapitre 5 – Organiser ses outils numériques

Une micro-entreprise structurée doit distinguer :

— email professionnel,
— cloud organisé,
— comptes individuels,
— sauvegarde.

Email professionnel

Éviter les adresses personnelles.

Préférer :

prenom@entreprise.ch

Cloud

Un cloud est un espace de stockage en ligne.
Il permet :

— accès multi-appareils,
— partage structuré,
— gestion des accès.

Organisation des dossiers

Structure simple :

— clients,
— comptabilité,
— RH,
— fournisseurs.

Accès limités selon le rôle de chacun.

Schéma organisationnel

Entreprise

Une organisation simple peut être représentée ainsi :

→ Email
→ Cloud
→ Sécurité (mot de passe + 2FA)
→ Sauvegarde

PARTIE III – SÉCURISER PROPORTIONNELLEMENT

Introduction

La LPD n’exige pas une infrastructure complexe.
Elle exige des mesures adaptées :

— à la taille de l’entreprise,
— au volume de données,
— à leur sensibilité.

Une micro-entreprise ne doit pas appliquer les mêmes mesures qu’un hôpital.
Mais elle ne peut pas non plus ignorer les bases.

Chapitre 6 – Sécurité de base (1 à 3 personnes)

La LPD impose des mesures techniques et organisationnelles appropriées.
Pour une micro-entreprise, cela ne signifie pas :
— infrastructure informatique complexe,
— pare-feu professionnel dédié,
— serveur interne sécurisé.

Cela signifie :

Mettre en place des protections simples, cohérentes et adaptées à la taille de l’activité.

1. Antivirus : première ligne de défense

Un antivirus est un logiciel qui :

— détecte les programmes malveillants,
— bloque les virus,
— empêche certaines intrusions.

Ce qui est important :

— qu'il soit actif,
— qu'il soit régulièrement mis à jour,
— que les analyses automatiques soient activées.

Un antivirus installé mais ignoré n'est pas une protection.

2. Mises à jour automatiques

Les mises à jour corrigent des failles de sécurité.
Sans mise à jour :

— ton système peut devenir vulnérable,
— ton navigateur peut être exploité,
— ton logiciel de facturation peut contenir des failles.

À vérifier :

— système d'exploitation,
— navigateur,
— logiciels professionnels,
— téléphone.

3. Pare-feu activé : protection intégrée

Un pare-feu filtre les connexions entre ton appareil et Internet.

Bonne nouvelle :

Les systèmes actuels (Windows, macOS) disposent déjà d'un pare-feu intégré.

Pour une micro-entreprise :

— vérifier qu'il est activé,
— éviter les WiFi publics non sécurisés,
— protéger l'accès à son réseau domestique.

4. Double authentification (2FA)

La double authentification demande :

— un mot de passe,
— un code temporaire envoyé sur ton téléphone.

À activer prioritairement sur :

— email,
— cloud,
— banque,
— logiciel de facturation,
— réseaux sociaux professionnels.

C'est aujourd'hui l'une des mesures les plus efficaces contre le piratage.

5. Gestion des mots de passe

La majorité des intrusions commencent par un mot de passe faible ou réutilisé.

Erreurs fréquentes :

❌ utiliser le même mot de passe partout
❌ utiliser des mots prévisibles (ex: prenom2024)
❌ les noter dans un fichier texte
❌ les envoyer par email

Bonne pratique proportionnée

— utiliser un gestionnaire de mots de passe sécurisé,
— créer un mot de passe maître long et unique,
— activer la double authentification du gestionnaire,
— générer des mots de passe aléatoires pour chaque service.

🔎 Encadré pédagogique – Pourquoi la longueur du mot de passe est déterminante

Le temps nécessaire pour casser un mot de passe dépend principalement de :
— sa longueur,
— sa complexité,
— sa prévisibilité.

Un mot de passe court et simple peut être découvert en quelques secondes par des outils automatisés.

Exemples :

Mot court et courant
→ cassé quasi instantanément

Mot basé sur un mot réel avec une année
→ minutes ou heures

Mot de passe long et aléatoire (12 à 16 caractères, lettres, chiffres, symboles)
→ peut nécessiter des années, voire bien davantage selon les méthodes d'attaque

Il ne s'agit pas d'un doublement progressif.
Chaque caractère ajouté multiplie exponentiellement la difficulté.

🔎 Encadré pédagogique – Pourquoi la longueur du mot de passe est déterminante (suite)

La règle simple :
Plus c’est long et imprévisible, plus c’est résistant.
Un mot de passe long et généré automatiquement est souvent plus sûr qu’un mot “intelligent” mais court.

Récapitulatif

🔐 Temps estimatif pour casser un mot de passe

— 4 caractères simples → Instantané,
— 6 caractères simples → Minutes,
— 8 caractères simples → Semaines,
— 10 caractères simples → Années,
— 12+ caractères aléatoires → extrêmement difficile en attaque par force brute.

6. Sauvegarde : protection contre la perte

Une sauvegarde protège contre :

— vol d'ordinateur,
— panne,
— ransomware (logiciel de rançon),
— erreur humaine.

Ransomware – définition simple

Un ransomware est un programme malveillant qui :

— bloque l'accès à tes fichiers,
— exige un paiement pour les débloquer.

Sans sauvegarde, l'activité peut être paralysée.

Bonne pratique proportionnée

Pour une micro-entreprise :

✓ cloud actif,
✓ sauvegarde externe périodique,
✓ vérification annuelle de la restauration.

7. Téléphone professionnel

Le téléphone contient souvent :

— contacts clients,
— emails,
— accès cloud.

À vérifier :

✓ code de verrouillage,
✓ mises à jour activées,
✓ possibilité d'effacement à distance.

8. Réseau WiFi

Si tu travailles à domicile :

✓ mot de passe WiFi fort,
✓ mot de passe différent de celui d'origine,
✓ mise à jour du routeur.

9. Ce que la LPD attend réellement

La loi ne demande pas la perfection.

Elle demande que tu puisses démontrer :

— une réflexion,
— une organisation,
— des mesures adaptées,
— une réduction raisonnable des risques.

Une micro-entreprise qui :

— protège ses accès,
— active la double authentification,
— sauvegarde ses données,
— utilise un gestionnaire de mots de passe.

est déjà dans une démarche sérieuse.

À retenir

La sécurité de base repose davantage sur :

— des habitudes cohérentes,
— une organisation claire,
— une vigilance constante,

que sur des outils complexes.

Chapitre 7 – Sécurité renforcée (4 à 10 employés)

Lorsque l'entreprise grandit, le risque évolue.

Ce n'est plus uniquement :

— une question d'antivirus,
— une question de mot de passe.

C'est une question :

— d'accès,
— de responsabilités,
— de circulation de l'information.

À partir de 4 collaborateurs, la sécurité doit devenir structurée.

1. Comptes individuels obligatoires

Chaque collaborateur doit disposer :
— de son propre compte utilisateur,
— de son propre accès email,
— de son propre mot de passe,
Les comptes partagés sont à éviter.

Pourquoi ?

Un compte partagé signifie :
— absence de traçabilité,
— impossibilité d'identifier l'origine d'une modification,
— difficulté en cas de départ.

Exemple concret :

Entreprise de 6 personnes utilisant :
info@entreprise.ch
mot de passe partagé

Problème :
si une personne quitte l'entreprise, le mot de passe doit être modifié partout.
Impossible de savoir qui a envoyé quoi.

Bonne pratique :
✓ Adresse personnelle professionnelle pour chaque collaborateur.
✓ Adresse générique redirigée si nécessaire.

2. Principe du moindre privilège

Chaque collaborateur doit avoir accès uniquement aux données nécessaires à sa fonction.

Exemples :
— un employé administratif n'a pas besoin d'accéder aux dossiers RH détaillés,
— un collaborateur terrain n'a pas besoin d'accéder à la comptabilité complète.

Limiter les accès réduit le risque.

3. Gestion des départs (procédure essentielle)

Lorsqu'un collaborateur quitte l'entreprise :

✓ désactiver immédiatement son compte,
✓ supprimer les accès cloud,
✓ supprimer les accès aux logiciels,
✓ modifier les accès partagés si existants.

Ne pas attendre plusieurs jours.

4. Tableau de gestion des accès

À partir de 4 collaborateurs, il devient recommandé de documenter :

— qui a accès à quoi,
— quel type d'accès (lecture / modification / admin),
— date de création,
— date de suppression.

Renvoi : Annexe 2 Tableau de gestion des accès (page 78)

5. Gestionnaire de mots de passe équipe

Lorsque plusieurs collaborateurs doivent accéder aux mêmes comptes (réseaux sociaux, logiciels, outils administratifs), un gestionnaire de mots de passe en version équipe devient nécessaire.

— un cloud (kDrive, OneDrive, etc.) sert à stocker des fichiers.
— un gestionnaire de mots de passe sert à sécuriser et organiser les accès.

Ce sont deux fonctions distinctes.

Pourquoi éviter les solutions “artisanales” ?

À éviter :

— fichier Excel partagé,
— document stocké dans un dossier cloud,
— transmission d’identifiants par email ou messagerie,
— mot de passe identique pour plusieurs services.

Ces pratiques ne permettent :

— ni traçabilité,
— ni retrait rapide des accès,
— ni contrôle en cas de départ.

Exemples de solutions disponibles

Il existe plusieurs gestionnaires proposant une version “ équipe ” ou “ business ”.

Exemples non exhaustifs :

— bitwarden,
— 1Password,
— nordPass Business,
— keeper,
— dashlane Business.

Ces solutions proposent généralement :

— chiffrement des données,
— comptes individuels,
— coffres ou dossiers partagés,
— gestion des droits,
— retrait immédiat des accès.

Le choix dépendra :
— du budget,
— du niveau de confort technique,
— des besoins spécifiques de l’entreprise.

Mise en place simplifiée

1. Désigner un administrateur
En principe le dirigeant ou une personne de confiance.

2. Créer un compte par collaborateur
Chaque collaborateur dispose :
— d’un compte personnel,
— d’un mot de passe maître,
— de la double authentification activée.

3. Créer des coffres partagés
Exemples :
— réseaux sociaux,
— comptabilité,
— marketing,
— outils internes.

4. Attribuer les droits
Selon les besoins :
— lecture seule,
— utilisation sans afficher le mot de passe,
— modification,
— administration.

5. Supprimer les anciennes pratiques

Une fois le système en place :

— supprimer les fichiers contenant les mots de passe,
— ne plus transmettre d'identifiants par email,
— ne plus conserver de carnets non sécurisés.

Procédure en cas de départ

Le jour du départ d'un collaborateur :

— désactiver immédiatement son compte,
— retirer les accès aux coffres partagés,
— modifier les mots de passe sensibles si nécessaire.

Cette opération prend généralement quelques minutes.

6. Sensibilisation minimale

La sécurité ne repose pas uniquement sur les outils. Chaque collaborateur doit comprendre les règles de base :

— ne pas transmettre de mot de passe,
— ne pas cliquer sur des liens suspects,
— verrouiller son poste de travail en cas d'absence,
— signaler immédiatement un incident.

Une courte sensibilisation annuelle peut suffire dans une petite structure.

7. Séparation des environnements

Si l’entreprise reçoit des clients ou du public :
— mettre en place un WiFi invité séparé,
— protéger le réseau interne,
— éviter que des visiteurs puissent accéder aux postes de travail.

Cela réduit le risque d’accès non autorisé.

8. Sauvegarde et responsabilités

Lorsque l’entreprise compte plusieurs collaborateurs, il devient important de clarifier :
— qui vérifie les sauvegardes,
— qui gère les accès,
— qui tient à jour le tableau des droits,
— qui documente les incidents.

Même si le dirigeant reste responsable, l’organisation doit être formalisée.

9. Ce que la LPD attend à ce niveau

À partir de plusieurs collaborateurs, l'autorité s'attend à :
— une organisation documentée,
— une limitation des accès,
— une gestion structurée des départs,
— une maîtrise des mots de passe,
Il ne s'agit pas d'exigences techniques lourdes, il s'agit d'exigences d'organisation.

À retenir

Entre 4 et 10 employés :
La sécurité devient principalement une question de gestion des accès et de responsabilités.

Les principaux risques sont :
— accès excessif,
— comptes partagés,
— départs mal gérés,
— erreurs humaines.

Une organisation claire réduit fortement ces risques.

Chapitre 8 – Gouvernance et organisation (+10 employés)

À partir d'une certaine taille, la sécurité ne peut plus reposer uniquement sur le dirigeant.
L'organisation devient une question de gouvernance.
Cela signifie :

— définir des responsabilités claires,
— documenter les processus,
— structurer la gestion des risques.

1. Désignation d'un responsable interne

Dans une entreprise de plus de 10 collaborateurs, il devient recommandé de désigner :

— un responsable de la protection des données,
— ou au minimum un référent interne.

Ce responsable :
— coordonne les mesures,
— tient à jour la documentation,
— supervise les incidents,
— centralise les demandes d'accès.

Il ne s'agit pas forcément d'un juriste, une personne organisée et formée peut effectuer ces tâches.

2. Formalisation des procédures

À ce stade, les pratiques doivent être formalisées.
Cela comprend :

— procédure de gestion des accès,
— procédure de gestion des incidents,
— procédure de départ des collaborateurs,
— politique interne documentée.

Ces documents existent déjà dans ton guide sous forme simplifiée.
Ils doivent obligatoirement être utilisés.

3. Journalisation et traçabilité

Lorsque plusieurs personnes manipulent des données sensibles, il devient pertinent de pouvoir :

— tracer les connexions,
— tracer les modifications,
— tracer les accès administrateurs.

Beaucoup de logiciels professionnels intègrent déjà ces fonctionnalités.

Il faut simplement :
— les activer,
— vérifier qu’elles fonctionnent.

4. Analyse des risques

Une entreprise plus grande doit réfléchir de manière plus structurée aux risques :

— quels types de données sensibles sont traitées ?
— quels seraient les impacts d'une fuite ?
— quels systèmes sont critiques pour l'activité ?

Il ne s'agit pas d'un audit complexe.
Il s'agit d'une réflexion documentée.

5. Gestion des sous-traitants

À ce stade, l'entreprise travaille souvent avec :

— un prestataire informatique,
— un hébergeur,
— une fiduciaire,
— un logiciel SaaS *(Software as a Service).*

Il devient important de vérifier :

— que ces partenaires respectent des standards de sécurité,
— qu'un contrat existe,
— que la protection des données est mentionnée.

6. Formation et sensibilisation régulière

Plus l'équipe grandit, plus le risque humain augmente.
Il est recommandé :

— de faire un rappel annuel,
— d'expliquer les bonnes pratiques,
— de rappeler la procédure en cas d'incident.

La majorité des incidents proviennent :

— d'une erreur humaine,
— d'un clic imprudent.
— d'un partage involontaire.

7. Plan de continuité minimal

À partir d'une certaine taille, l'entreprise doit réfléchir :

— que se passe-t-il si le serveur tombe ?
— si le cloud devient inaccessible ?
— si une attaque bloque les systèmes ?

Il peut être pertinent de :

— documenter les sauvegardes,
— identifier un prestataire IT,
— définir une procédure de reprise.

8. Ce que la LPD attend à ce niveau

L’autorité attend :

— une organisation documentée,
— une responsabilité clairement identifiée,
— une gestion structurée des risques,
— une capacité de réaction.

La complexité doit rester proportionnée à la taille et au risque.

À retenir

Lorsque l’entreprise dépasse 10 collaborateurs :
La protection des données devient un élément de gouvernance.

Elle ne repose plus uniquement sur :

— des outils,
— ou la vigilance individuelle.

Elle repose sur :

— des processus,
— des responsabilités,
— une organisation claire.

PARTIE IV – GÉRER LES SITUATIONS CONCRÈTES

Introduction

Même avec une bonne organisation, des situations surviennent :

— demande d’accès,
— incident de sécurité,
— erreur humaine.

L’important est la réaction.

Chapitre 9 – Répondre à une demande d’accès

Toute personne dont tu traites les données peut demander :

— quelles sont les données que tu détiens sur elle ?
— à quoi elles servent ?
— à qui elles sont transmises ?

C’est ce qu’on appelle le droit d’accès.

1. Qu’est-ce qu’une demande d’accès ?

Une demande d’accès peut arriver :

— par email,
— par courrier,
— parfois verbalement,

Exemple :

“Pouvez-vous me transmettre les données que vous avez sur moi ?”

Il n’est pas nécessaire que la personne cite la loi.

2. Qui peut faire une demande ?

Toute personne concernée :
— client actuel,
— ancien client,
— collaborateur,
— ancien collaborateur,
— fournisseur (si données personnelles traitées).

3. Délai de réponse

En principe, la réponse doit être donnée dans un délai raisonnable.
Il est recommandé de répondre dans les 30 jours.
Si la demande est complexe, il est possible d’indiquer que le traitement nécessite un délai supplémentaire.

4. Que faut-il fournir ?

La personne peut obtenir :
— les données personnelles la concernant,
— la finalité du traitement,
— la durée de conservation,
— les catégories de destinataires.

Il ne s’agit pas de transmettre l’intégralité de ton système informatique.
Il s’agit de transmettre les données relatives à la personne concernée.

5. Comment procéder concrètement ?

Étape 1 – Vérifier l’identité

Avant de transmettre des données :

— vérifier que la demande provient bien de la personne concernée,

— en cas de doute, demander une pièce justificative.

Étape 2 – Rechercher les données

Identifier où se trouvent les données :

— logiciel de facturation,

— cloud,

— emails,

— dossiers papier,

— archives.

C’est ici que l’organisation mise en place dans les chapitres précédents devient essentielle.

Étape 3 – Préparer la réponse

Rassembler :

— copie des données,

— explication claire et compréhensible,

— indication de la finalité.

La réponse doit être compréhensible.
Éviter le jargon.

Étape 4 – Transmettre de manière sécurisée

Ne pas envoyer des données sensibles par email non sécurisé.

Privilégier :
— envoi sécurisé,
— lien protégé,
— remise en main propre si nécessaire.

6. Peut-on refuser ?

Un refus est possible dans certains cas :

— demande manifestement abusive,
— atteinte aux droits de tiers,
— obligation légale empêchant la communication.

Un refus doit être motivé.

7. Exemple concret – Micro-entreprise

Une cliente demande :
“Quelles informations détenez-vous sur moi ?”

Tu vérifies :

— fiche client,
— devis,
— factures,
— échanges email.

Tu transmets :

— copie des documents,
— explication de l’usage (gestion contractuelle, facturation),
— durée de conservation (ex. obligations légales comptables),
— Procédure simple, structurée, proportionnée.

8. Pourquoi ce chapitre est stratégique

La demande d’accès est souvent :
— le premier point de contrôle,
— un déclencheur de plainte,
— un révélateur de désorganisation.
Une entreprise organisée peut répondre rapidement.
Une entreprise désorganisée entre en difficulté.

À retenir

La demande d’accès n’est pas une menace.
C’est un droit.
Une organisation claire permet d’y répondre sereinement.

🔎 Encadré pratique – Où chercher les données lors d’une demande d’accès ?

Lorsqu’une personne demande quelles données sont détenues sur elle, il est utile de suivre une méthode structurée.
Voici une grille simple à utiliser :

Logiciels professionnels
— logiciel de facturation,
— CRM (gestion client),
— outil de gestion RH,
— logiciel de réservation.

Cloud
— dossiers clients,
— contrats,
— devis,
— documents scannés.

Emails
— échanges contractuels,
— confirmations,
— pièces jointes.

🔎 Encadré pratique – Où chercher les données lors d’une demande d’accès ? (suite)

Dossiers papier

— contrats signés,
— fiches clients,
— archives.

Outils tiers

— plateforme de paiement,
— logiciel externe,
— outil marketing.

Méthode recommandée

✓ Faire une liste des sources
✓ Cocher celles vérifiées
✓ Documenter brièvement la recherche

Cela permet de démontrer une démarche sérieuse en cas de contestation.

Renvoi : Annexe 3 - Modèle de réponse à une demande d’accès (page 79)

Chapitre 10 – Gérer un incident de sécurité (Perte, fuite, piratage, ransomware)

Un incident de sécurité peut survenir même dans une petite structure.

Il peut s'agir :
— d'un ordinateur volé,
— d'un email envoyé au mauvais destinataire,
— d'un accès piraté,
— d'un ransomware,
— d'une clé USB perdue.

La LPD n'exige pas l'absence d'incident.
Elle exige une réaction adaptée.

1. Qu'est-ce qu'un incident de sécurité ?

Un incident de sécurité est un événement qui entraîne :
— perte de données,
— accès non autorisé,
— divulgation involontaire,
— destruction de données.

Exemples concrets

— mail contenant une facture envoyé au mauvais client,
— ordinateur portable volé dans une voiture,
— compte email piraté,
— fichiers chiffrés par un ransomware.

2. Première réaction : garder son calme

La première erreur est la panique.
La bonne approche :

— identifier l'incident,
— contenir l'incident,
— évaluer l'impact,
— documenter.

3. Étape 1 – Contenir l'incident

Exemples :

— déconnecter un ordinateur d'Internet,
— modifier immédiatement les mots de passe,
— désactiver un compte compromis,
— bloquer un accès.

L'objectif est d'éviter l'aggravation.

4. Étape 2 – Évaluer la gravité

Questions à se poser :

— quelles données sont concernées ?
— combien de personnes sont touchées ?
— s'agit-il de données sensibles ?
— les données sont-elles récupérables ?

Une erreur isolée et rapidement corrigée n'a pas le même impact qu'une fuite massive.

5. Étape 3 – Faut-il notifier l’autorité ?

En Suisse, une notification au Préposé fédéral à la protection des données et à la transparence (PFPDT) est requise si :

— l’incident présente un risque élevé pour les droits ou la personnalité des personnes concernées.

Exemples de risque élevé :

— données médicales exposées,
— données bancaires divulguées,
— fuite massive de données clients.

Toutes les erreurs ne nécessitent pas une notification.

6. Faut-il informer les personnes concernées ?

Si le risque est élevé, les personnes concernées doivent être informées.

L’objectif :

— leur permettre de prendre des mesures,
— éviter un dommage supplémentaire.

7. Exemple concret – Micro-entreprise

Un indépendant envoie par erreur un devis contenant des données personnelles au mauvais client.

Il doit :
— contacter immédiatement le destinataire,
— demander la suppression du document,
— documenter l’incident,
— vérifier que le fichier n’a pas été transmis plus loin.

Si les données ne sont pas sensibles et l’erreur est contenue rapidement, il n’est généralement pas nécessaire de notifier l’autorité.

8. Cas particulier – Ransomware

Un ransomware est un logiciel malveillant qui :
— bloque ou chiffre tes fichiers,
— empêche l'accès aux données,
— exige un paiement (souvent en cryptomonnaie).

Première réaction : isoler immédiatement

Dès suspicion :
— déconnecter l'ordinateur du réseau (WiFi et câble),
— éteindre la synchronisation cloud,
— déconnecter les disques externes.

Objectif : empêcher la propagation.
Ne pas redémarrer en boucle sans comprendre.

Ne pas payer immédiatement

Payer la rançon :
— ne garantit pas la récupération,
— encourage le modèle criminel,
— peut exposer à une nouvelle attaque,

La décision ne doit jamais être prise dans la panique.

Contacter un professionnel IT

Même une micro-entreprise devrait :
— contacter un prestataire informatique,
— évaluer la possibilité de restauration,
— vérifier si la sauvegarde est intacte.

Si une sauvegarde récente existe, la restauration est souvent possible.

Évaluer l’ampleur

Questions essentielles :
— les données ont-elles seulement été chiffrées ?
— où ont-elles été copiées (exfiltration) ?
— s’agit-il de données sensibles ?
— combien de personnes sont concernées ?
Aujourd’hui, certaines attaques combinent :
— chiffrement,
— menace de publication des données.

Déposer plainte

En Suisse, il est recommandé de :
— Déposer plainte auprès de la police cantonale.
Cela permet :
— d’officialiser l’incident,
— d’obtenir un procès-verbal,
— d’appuyer une éventuelle déclaration d’assurance.

Certaines assurances cyber exigent une plainte formelle.

Vérifier l'assurance

Si l'entreprise dispose :

— d'une assurance cyber,

— ou d'une assurance RC professionnelle élargie.

Il faut contacter immédiatement l'assureur.

Les contrats peuvent prévoir :

— assistance IT,

— prise en charge des frais,

— accompagnement juridique.

Notification au PFPDT ?

Si l'attaque présente un risque élevé pour les personnes concernées (ex. données médicales, données financières), une notification au Préposé fédéral à la protection des données et à la transparence peut être nécessaire.

La question clé est :

Y a-t-il un risque sérieux pour les personnes concernées ?

Informer les personnes concernées

Si les données ont été compromises :

— informer de manière claire,

— indiquer les risques,

— suggérer des mesures de précaution.

Exemple :

— surveillance des comptes bancaires,

— vigilance face aux tentatives de phishing.

Après l’incident : renforcer les mesures

Un ransomware révèle souvent :

— mot de passe faible,
— absence de double authentification,
— sauvegarde inexistante,
— faille de mise à jour.

Après restauration :

— changer tous les mots de passe,
— activer la 2FA,
— vérifier les mises à jour,
— renforcer la sauvegarde.

Une attaque peut survenir même avec des mesures en place.

Ce qui fait la différence :

- **la rapidité de réaction,**
- **la qualité des sauvegardes,**
- **la documentation,**
- **la transparence.**

Renvoi : Annexe 4 – Checklist ransomware (pages 80 à 83)

🔎 Que faire si plusieurs postes sont connectés au même réseau ?

Dans de nombreuses entreprises, plusieurs ordinateurs sont connectés :
— au même WiFi,
— au même routeur,
— parfois à un dossier partagé.
En cas de ransomware, la question se pose : faut-il couper tout le réseau ?

Priorité : isoler le poste suspect

La première action concerne toujours :
— le poste infecté,
— ses disques externes,
— sa synchronisation cloud.
Il ne faut pas immédiatement éteindre tous les autres postes sans évaluation.

Vérifier les autres postes

Après isolement :
— observer les autres ordinateurs,
— vérifier si des fichiers sont modifiés,
— contrôler les messages d’alerte,
— vérifier les dossiers partagés.
Si aucun signe suspect n’apparaît, il n’est pas nécessaire de tout couper.

🔎 Encadré – Que faire si plusieurs postes sont connectés au même réseau ? (suite)

Quand faut-il couper le réseau complet ?

Il peut être nécessaire de :
— couper le routeur,
— désactiver le WiFi,
— arrêter temporairement le serveur.
Si :
— plusieurs machines montrent des signes d'infection,
— des fichiers partagés sont chiffrés,
— le chiffrement est en cours sur plusieurs postes.
Dans ce cas, la priorité devient la limitation de propagation.

Cas d'une micro-entreprise (1 à 3 postes)

Dans une petite structure sans serveur dédié :
— couper, temporairement le routeur peut être prudent,
— vérifier chaque poste individuellement.
L'objectif reste toujours :
Limiter la propagation avant d'analyser.

🎯 Principe clé

On n'agit pas dans la panique.
On agit de manière graduée :

1. isoler,
2. observer,
3. étendre les mesures si nécessaire.

La proportionnalité reste le principe directeur.

PARTIE V – RISQUES, CONTRÔLES ET RESPONSABILITÉ

Introduction

La question revient souvent :
“Suis-je réellement exposé ?”

La protection des données ne fonctionne pas comme un contrôle fiscal automatique.
Il est important de comprendre :
— qui contrôle,
— dans quelles situations,
— et comment se déroule une procédure.

Chapitre 11 – Les erreurs fréquentes en matière de protection des données

La majorité des manquements à la LPD ne provient pas d’une intention malveillante.
Ils proviennent :
— d’un manque d’organisation,
— d’habitudes anciennes,
— d’une sous-estimation du risque,
— d’une confusion entre simplicité et négligence.

Identifier les erreurs fréquentes permet de les corriger rapidement.

1. Mélanger vie privée et activité professionnelle

— utiliser une adresse email personnelle pour facturer,
— stocker des documents clients dans des dossiers privés,
— partager un ordinateur familial.

Risque :
Données dispersées, difficulté en cas de demande d'accès, perte de maîtrise.
Correction :
Séparer strictement les outils professionnels.

2. Conserver les données sans limite

Conserver des anciens devis, dossiers inactifs, copies inutiles.

3. Utiliser des mots de passe faibles ou identiques

— mot de passe identique partout,
— absence de double authentification.

Risque :
Un seul piratage peut ouvrir l'accès à tout le système.
Correction :
— Gestionnaire de mots de passe + double authentification.

4. Partager des identifiants par email ou message

— fichier Excel partagé,
— mot de passe envoyé par WhatsApp.

Risque :

— aucune traçabilité,
— accès incontrôlable en cas de départ.

Correction :

Gestionnaire de mots de passe en version équipe.

5. Ignorer les mises à jour

Reporter systématiquement les mises à jour.

Risque :

— failles de sécurité exploitables.

Correction :

Activer les mises à jour automatiques.

6. Ne pas documenter

— procédures existantes mais non écrites.

Risque :

— impossible de démontrer une organisation en cas de plainte.

Correction :

Tenir des notes simples : accès, sauvegardes, incidents.

7. Sous-estimer l’erreur humaine

— email envoyé au mauvais destinataire,
— lien malveillant ouvert.

Risque :
— incident involontaire.
Correction :
Sensibilisation minimale annuelle.

8. Penser que “ça n’arrive qu’aux grandes entreprises”

Les petites structures sont souvent ciblées parce qu’elles sont moins protégées.

9. Réagir dans la panique en cas d’incident

— supprimer tout,
— redémarrer sans stratégie,
— payer immédiatement.

Correction :
Suivre une procédure structurée.

10. Attendre d’avoir un problème pour agir

La protection des données est préventive.

📊 Tableau synthétique

Erreur	Risque	Correction
Mélange privé / pro	Données dispersées	Séparer les outils
Mots de passe faibles	Piratage global	Gestionnaire + 2FA
Conservation excessive	Risque accru	Politique de suppression
Partage par email	Fuite d’accès	Gestionnaire équipe
Pas de sauvegarde	Paralysie	Sauvegarde régulière
Absence de documentation	Difficulté en cas de plainte	Registre simple
Pas de sensibilisation	Erreur humaine	Rappel annuel

🧠 Mini auto-diagnostic

Si plus de trois réponses sont “Non”, une mise à niveau organisationnelle est recommandée.

Question	Oui	Non
Ai-je séparé mes outils privés et professionnels ?		
Est-ce que j’utilise un gestionnaire de mots de passe ?		
La double authentification est-elle activée sur mes comptes essentiels ?		
Mes sauvegardes sont-elles régulières et testées ?		
Ai-je une procédure en cas d’incident ?		
Est-ce que je sais précisément où sont stockées les données clients ?		
Ai-je défini une durée de conservation ?		
Les accès des collaborateurs sont-ils limités et documentés ?		
Puis-je répondre à une demande d’accès dans un délai raisonnable ?		
Ai-je documenté mes principales mesures de sécurité ?		

En 2026, un incident impliquant un outil d'intelligence artificielle d'entreprise a montré qu'un assistant IA pouvait contourner certaines règles de confidentialité internes.
L'incident n'était pas lié à une "cyberattaque classique", mais à une faille d'architecture.

Cet exemple illustre que la conformité ne repose pas uniquement sur les outils choisis :
— les outils évoluent rapidement,
— les promesses marketing ne remplacent pas la vigilance,
— la responsabilité juridique reste celle de l'entreprise utilisatrice.

À retenir

Les erreurs les plus fréquentes ne sont pas techniques.
Elles sont organisationnelles.
La conformité ne repose pas sur la perfection.
Elle ne se délègue pas entièrement à un fournisseur technologique.

Chapitre 12 – Faut-il souscrire une assurance cyber ?

Avec la numérisation croissante des activités, le risque cyber est devenu une réalité, même pour les petites structures.

La question n’est plus :
“Est-ce que cela peut arriver ?”
Mais :
“Que se passe-t-il si cela arrive ?”

1. Qu’est-ce qu’une assurance cyber ?

Une assurance cyber est un contrat qui couvre certains risques liés :
— aux attaques informatiques,
— aux pertes de données,
— aux interruptions d’activité,
— aux frais juridiques liés à une violation de données.

Elle ne remplace pas les mesures de sécurité.
Elle intervient en complément.

2. Que peut couvrir une assurance cyber ?

Selon les contrats :

— assistance technique en cas d'attaque,
— frais de restauration des données,
— interruption d'activité,
— frais d'expertise informatique,
— frais juridiques,
— frais de notification aux personnes concernées,
— gestion de crise.

Certaines assurances incluent un accompagnement spécialisé 24/7.

3. Ce qu'elle ne couvre généralement pas

— négligence grave,
— absence totale de mesures de sécurité,
— amendes pénales intentionnelles,
— absence de sauvegarde.

Les assureurs demandent souvent :

— antivirus actif,
— sauvegarde existante,
— mots de passe sécurisés,
— mesures minimales en place.

4. Est-ce utile pour une micro-entreprise ?

Cela dépend :
— du volume de données traitées,
— de la sensibilité des données,
— de la dépendance à l'informatique,
— de la capacité financière à absorber un incident.

Un indépendant qui :
— dépend fortement de son cloud,
— traite des données sensibles,
— n'a pas de prestataire IT interne,
peut envisager cette couverture.

5. Cas concret

Peintre indépendant :
— quelques devis,
— peu de données sensibles,
— sauvegarde régulière.
Risque limité.

Clinique esthétique :
— données médicales,
— dossiers sensibles,
— forte exposition.
Risque élevé.

La proportionnalité s'applique ici aussi.

6. Assurance cyber ou prévention ?

L’assurance ne remplace pas :

— la sauvegarde,
— la gestion des accès,
— la double authentification,
— la mise à jour des systèmes.

Elle intervient lorsque la prévention n’a pas suffi.

7. Questions à poser à son assureur

— quels incidents sont couverts ?
— les frais de notification sont-ils inclus ?
— l’assistance IT est-elle incluse ?
— les rançons sont-elles couvertes ?
— une plainte est-elle exigée ?
— quelles mesures préventives sont obligatoires ?

8. Coût estimatif

Pour une petite structure :

— quelques centaines de francs par an, à plusieurs milliers selon :
— chiffre d’affaires,
— volume de données,
— niveau de couverture.

9. Conclusion du chapitre

L’assurance cyber n’est pas obligatoire.

Elle peut être pertinente si :

— l’activité dépend fortement du numérique,
— les données traitées sont sensibles,
— l’impact d’un incident serait critique.

La décision doit être rationnelle, pas émotionnelle.

Chapitre 13 – Le rôle du PFPDT et la procédure de plainte

En Suisse, l'autorité chargée de surveiller l'application de la Loi sur la protection des données (LPD) est :
Le Préposé fédéral à la protection des données et à la transparence (PFPDT).
Son rôle n'est pas de sanctionner automatiquement, mais de veiller au respect de la loi.

1. Quel est le rôle du PFPDT ?

Le PFPDT :
— surveille l'application de la LPD,
— examine les plaintes,
— peut ouvrir des investigations,
— peut formuler des recommandations,
— peut ordonner des mesures correctives dans certains cas.

Il agit principalement :
— à la suite d'une plainte,
— en cas d'incident important,
— en cas de signalement.

Il ne procède pas à des contrôles massifs aléatoires comme une autorité fiscale.

2. Qui peut déposer une plainte ?

Toute personne concernée peut saisir le PFPDT si elle estime que :

— ses données sont mal traitées,
— elle n’a pas obtenu de réponse à une demande d’accès,
— ses droits n’ont pas été respectés.

Cela peut être :

— un client,
— un ancien client,
— un collaborateur,
— un partenaire,

3. Comment se déroule une procédure ?

En général :

— une plainte est déposée,
— le PFPDT examine la recevabilité,
— l’entreprise peut être contactée pour fournir des explications,
— l’autorité analyse les éléments transmis,
— elle peut formuler des recommandations ou ouvrir une enquête formelle.

La coopération est essentielle.

4. Les sanctions possibles

La LPD prévoit des sanctions pénales en cas de :

— violation intentionnelle,
— refus de coopérer,
— communication d’informations inexactes,
— manquement grave aux obligations.

Les amendes peuvent viser les personnes responsables.
Cependant, dans la pratique :
La majorité des situations concernent des problèmes d’organisation ou de négligence.
La transparence et la coopération réduisent fortement les risques.

5. Comment réagir si le PFPDT contacte l’entreprise ?

En cas de demande :

— ne pas ignorer,
— respecter les délais,
— répondre de manière claire et factuelle,
— fournir les documents demandés,
— expliquer les mesures mises en place.

Une entreprise organisée peut démontrer :

— ses procédures,
— sa gestion des accès,
— ses sauvegardes,
— sa réponse aux demandes d’accès.

6. Principe clé : démontrer la démarche

Le PFPDT cherche à vérifier :

— si l’entreprise a réfléchi aux risques,
— si elle a mis en place des mesures adaptées,
— si elle agit de bonne foi.

Ce qui protège le plus une entreprise :

— la documentation,
— la proportionnalité,
— la cohérence.

7. Où trouver les informations officielles ?

Les informations, recommandations et formulaires sont disponibles sur le site officiel du PFPDT.

Il est possible d’y trouver :

— des guides,
— des explications pratiques,
— les modalités de notification en cas d’incident.

À retenir

Le PFPDT n’est pas un adversaire.
C’est une autorité de surveillance.

PARTIE VI – PASSER À L’ACTION

Introduction

Comprendre ne suffit pas.

La conformité devient concrète lorsque l’on agit.
Cette partie propose :

— un plan progressif,
— des checklists adaptées,
— une méthode simple.

Chapitre 14 – Plan de mise en conformité en 30 jours

La conformité à la LPD ne se fait pas en une journée.
Elle se met en place progressivement.
L’objectif n’est pas la perfection immédiate,
mais une démarche structurée et cohérente.

🔹 Étape 1 – Faire un état des lieux

Avant toute action :
— identifier où sont stockées les données,
— identifier quels types de données sont traités,
— identifier qui y a accès,
— identifier les outils utilisés (email, cloud, logiciels).

Sans cartographie, aucune organisation n’est possible.

🔹 Étape 2 – Sécuriser les accès essentiels

Commencer par les éléments critiques :

— installer ou vérifier l'antivirus,
— activer les mises à jour automatiques,
— activer la double authentification sur les comptes clés,
— mettre en place un gestionnaire de mots de passe.

Cette étape réduit immédiatement le risque principal.

🔹 Étape 3 – Organiser le stockage

— choisir un cloud principal,
— structurer les dossiers,
— supprimer les doublons,
— nettoyer les données inutiles,
— définir une logique de conservation.

La clarté organisationnelle réduit le risque juridique.

🔹 Étape 4 – Formaliser les accès

Si plusieurs personnes sont impliquées :

— créer un compte par collaborateur,
— limiter les accès selon les besoins,
— documenter les droits,
— prévoir une procédure de départ.

🔹 Étape 5 – Mettre en place les sauvegardes

— vérifier qu'une sauvegarde existe,
— vérifier qu'elle fonctionne,
— tester la restauration,
— documenter la fréquence.

Une sauvegarde testée vaut plus qu'une sauvegarde supposée.

🔹 Étape 6 – Prévoir la gestion des incidents

— conserver la checklist ransomware,
— identifier un prestataire IT,
— noter la procédure de notification,
— documenter les incidents éventuels.

L'anticipation réduit la panique.

🔹 Étape 7 – Préparer la réponse aux demandes d'accès

— identifier les sources de données,
— préparer un modèle de réponse,
— définir un responsable interne.

🔹 Étape 8 – Documenter la démarche

Tenir un document simple indiquant :

— mesures mises en place,
— date de mise à jour,
— responsable,
— incidents éventuels.

La documentation est une preuve de bonne foi.

🔹 Étape 9 – Évaluer la pertinence d'une assurance cyber

Analyser :
— dépendance au numérique,
— sensibilité des données,
— impact potentiel d'un incident.

Décision rationnelle, pas émotionnelle.

🔹 Étape 10 – Réviser une fois par an

La conformité n'est pas figée.
— vérifier les accès,
— vérifier les sauvegardes,
— mettre à jour les procédures,
— sensibiliser les collaborateurs.

🎯 Approche progressive recommandée

— semaine 1 : Sécurisation des accès,
— semaine 2 : Organisation du cloud,
— semaine 3 : Formalisation des procédures,
— semaine 4 : Documentation et vérification.

Une mise en conformité peut être réalisée en un mois de manière structurée.

🧠 Principe clé

La conformité LPD repose sur :
— la proportionnalité,
— la cohérence,
— la continuité.

Une petite entreprise n’a pas besoin d’un service juridique interne.
Elle a besoin :
— d’organisation,
— de méthode,
— de discipline.

À retenir

La conformité est un processus,
pas un document unique.
Elle se construit pas à pas.

Conclusion générale – Une conformité proportionnée et maîtrisée

La protection des données n’est pas une contrainte administrative supplémentaire.
Elle est une composante naturelle d’une entreprise organisée.

La LPD ne demande pas :
— une perfection technique,
— une infrastructure complexe,
— des moyens disproportionnés.

Elle demande :
— une réflexion,
— une organisation,
— des mesures adaptées,
— une capacité à réagir.

Une micro-entreprise peut être conforme avec :
— des outils simples,
— une méthode claire,
— une discipline régulière.

La conformité n’est pas un état figé.
C’est une démarche continue.

Ce qui protège réellement une entreprise

Ce ne sont pas uniquement les logiciels.
Ce sont :
— la séparation des outils,
— la gestion rigoureuse des accès,
— les sauvegardes testées,
— la documentation,
— la cohérence des pratiques.

Une entreprise qui peut démontrer :

— qu’elle a identifié ses risques,
— qu’elle a mis en place des mesures adaptées,
— qu’elle agit de bonne foi.

réduit fortement son exposition juridique.

Message final

La conformité à la LPD n’est pas réservée aux grandes structures.

— elle est accessible,
— elle est proportionnée,
— elle est maîtrisable.

MAIS

— elle n’est pas un état figé,
— les technologies évoluent,
— les responsabilités demeurent.

Avec méthode, elle devient un élément de professionnalisation.

Références officielles et ressources utiles

Préposé fédéral à la protection des données et à la transparence (PFPDT)

https://www.edoeb.admin.ch

Texte officiel de la Loi fédérale sur la protection des données (LPD)

https://www.fedlex.admin.ch

Portail officiel de la Confédération suisse

https://www.admin.ch
Il est recommandé de consulter les sources officielles pour toute évolution législative.

ANNEXES

Annexe 1 – Modèle d’inventaire des données

Annexe 2 – Tableau de gestion des accès

Annexe 3 – Modèle de réponse à une demande d’accès

Annexe 4 – Checklist ransomware

Annexe 1 – Modèle d’inventaire des données (outil directement exploitable)

Type de données	Finalité	Outil utilisé	Accès autorisé	Durée de conservation
Clients				
Fournisseurs				
Collaborateurs				
Newsletter				
Comptabilité				

Annexe 2 Tableau de gestion des accès

Collaborateur	
Fonction	
Outils accessibles	
Niveau d’accès	
Date de création	
Date de suppression	

Ce tableau permet de documenter le principe du moindre privilège.

📄 Annexe 3 – Modèle de réponse à une demande d’accès

(*Modèle adaptable)*

Objet : Réponse à votre demande d’accès aux données personnelles

Madame / Monsieur,
Nous accusons réception de votre demande relative aux données personnelles vous concernant.
Après vérification de votre identité, nous vous transmettons ci-dessous les informations détenues dans le cadre de notre relation professionnelle.

1. Données détenues

- *Nom, prénom*
- *Coordonnées (adresse, email, téléphone)*
- *Données contractuelles (devis, factures, correspondances)*

2. Finalité du traitement

Ces données sont utilisées dans le cadre :

- *de l’exécution du contrat*
- *de la facturation*
- *du respect des obligations légales*

3. Durée de conservation

Les données comptables sont conservées conformément aux obligations légales en vigueur.
Les autres données sont conservées aussi longtemps que nécessaire à la relation contractuelle.
Si vous souhaitez exercer un autre droit (rectification, suppression lorsque possible), nous vous invitons à nous en informer.
Nous restons à disposition pour toute précision complémentaire.
Avec nos salutations distinguées,
Nom
Fonction
Entreprise

🔴 ANNEXE 4 - CHECKLIST – RANSONWARE

RANSONWARE (suite)

(à conserver et imprimer)

Isoler immédiatement la machine

Dès suspicion :

□ débrancher le câble réseau,
□ désactiver le WiFi,
□ déconnecter tous les disques durs externes,
□ suspendre la synchronisation cloud si possible.

Objectif : empêcher la propagation vers :

— le cloud,
— les sauvegardes,
— les autres postes.

Ne pas attendre.

Décider s'il faut éteindre l'ordinateur

Deux situations possibles :

🔹 **Si le chiffrement est en cours (fichiers qui disparaissent, extensions modifiées en temps réel)**

□ éteindre immédiatement l'ordinateur.
(Coupure rapide si nécessaire)
Cela peut limiter le nombre de fichiers chiffrés.

🔴 ANNEXE 4 - CHECKLIST – RANSONWARE (suite)

(à conserver et imprimer)

🔹 Si le chiffrement semble terminé

□ ne pas redémarrer,
□ laisser l'ordinateur isolé,
□ attendre l'intervention d'un professionnel IT.

Un redémarrage peut :

— déclencher une nouvelle phase,
— compliquer l'analyse.

Supprimer des traces utiles

Ne pas reconnecter prématurément

□ ne pas reconnecter au réseau,
□ ne pas brancher de disque externe.

Ne pas "tester" la connexion

Contacter un professionnel informatique

□ contacter un prestataire IT,
□ évaluer si les données ont été copiées (exfiltration),
□ vérifier l'état des sauvegardes.

ANNEXE 4 - CHECKLIST – RANSONWARE (suite)

(à conserver et imprimer)

Vérifier les sauvegardes

□ existe-t-il une sauvegarde récente ?
□ est-elle isolée du réseau ?
□ est-elle intacte ?
Si oui, une restauration peut être envisagée.

Déposer plainte

□ contacter la police cantonale,
□ obtenir un procès-verbal,
□ informer l'assurance si applicable.
Certaines assurances cyber exigent un dépôt de plainte.

Évaluer l'impact juridique

□ quelles données sont concernées ?
□ sont-elles sensibles ?
□ combien de personnes sont impactées ?
□ existe-t-il un risque élevé pour les personnes concernées ?

🔴 ANNEXE 4 - CHECKLIST – RANSONWARE (suite)

(à conserver et imprimer)

Notification si nécessaire

Si le risque est élevé :

□ notifier le Préposé fédéral à la protection des données et à la transparence (PFPDT),

□ informer les personnes concernées.

Après l'incident : renforcer la sécurité

□ changer tous les mots de passe,

□ activer la double authentification partout,

□ mettre à jour tous les systèmes,

□ revoir la politique de sauvegarde,

□ documenter l'incident.

🧠 À retenir

L'ordre logique est :

1. isoler,
2. stabiliser,
3. évaluer,
4. restaurer,
5. notifier si nécessaire,
6. renforcer.

La rapidité d'isolement fait souvent la différence.

Checklist finale – Synthèse de conformité

Organisation

□ Séparation outils privés / professionnels,
□ Cloud principal structuré,
□ Politique de conservation définie.

Sécurité

□ Antivirus actif,
□ Mises à jour automatiques,
□ Double authentification activée,
□ Gestionnaire de mots de passe.

Accès

□ Comptes individuels,
□ Accès limités selon les besoins,
□ Procédure de départ documentée.

Sauvegarde

□ Sauvegarde régulière,
□ Test de restauration effectué,
□ Procédure ransomware imprimée.

Droits des personnes

□ Modèle de réponse aux demandes d’accès,
□ Délai de réponse maîtrisé.

Documentation

□ Mesures notées,
□ Incidents documentés,
□ Révision annuelle planifiée.

Audit administratif pour indépendants

Contenu possible :

— analyse rapide de la situation de l'indépendant
— vérification des bases administratives
— vérification organisation des données
— recommandations simples.

Durée :

30 à 45 minutes.

Prix possible :

80 à 150 CHF selon la formule.

simplE-IAdmin
L'intelligence administrative au service des artisans et PME suisses

Catherine Dos Santos
Route du Zémont 17
1912 Produit
Tél. 078 744 35 81
contact@simple-iadmin.com