# Notre directive sur la protection des données.

Organisation :

## De quoi s'agit il ?

La présente directive régit le traitement des données personnelles* au sein de notre entreprise. Elle est contraignante pour tous les collaborateurs-trices (y.c. les personnes intégrées dans l'entreprise).

Adoptée par/le/à partir de :

## Qui est responsable de quoi en matière de protection des données ?

1. Pour chaque traitement de données au sein de notre entreprise, il y a une **personne responsable** (**PR**). La PR est propriétaire de l'activité commerciale concernée (à moins que la direction n'en décide autrement), de même que toute personne qui détermine les aspects essentiels du traitement des données. Les supérieurs hiérarchiques de la PR sont chargés de sélectionner, d'instruire et de superviser la PR. La PR les informe de sa propre initiative des évènements importants.
2. Chaque PR doit s'assurer que les exigences de la loi sur la protection des données (**LPD**) sont respectées, en particulier celles figurant dans la feuille de route "nLPD : Ce qu'il faut faire" (ensemble les **exigences de la LPD**). Les exceptions doivent être justifiées. Les traitements de données nouveaux ou modifiés doivent être annoncés au/à la coordinateur-trice de la protection des données (**CPD**).
3. Chaque PR doit s'assurer que les prescriptions en matière de **conservation** et d'**effacement** des documents et des données personnelles sont respectées.
4. Le CPD désigné par la direction organise la mise en œuvre et le respect des exigences de la LPD et conseille la PR. Le CPD n'a pas un pouvoir de décision, mais il signale à la direction les violations importantes de la LPD.
5. Les règles de protection des données établies et les décisions prises par une PR sont en principe contraignantes pour les **collaborateurs-trices**. Les collaborateurs-trices doivent en outre respecter les exigences de la LPD et en particulier annoncer sans retard les violations de la sécurité des données ainsi que les demandes de tiers concernant la protection des données (cf. page suivante).
6. Chacun respecte le **secret professionnel**. Une communication à un tiers ne peut avoir lieu qu'en cas de levée du secret.

**Le non-respect de ces responsabilités et de cette directive peut entraîner des conséquences disciplinaires, civiles et pénales, pouvant aller jusqu'au licenciement.**

## Y a t il d'autres règles ?

## Quelle est la durée de conservation ?

**Principe :** Nous archivons tout ce dont nous n'avons plus besoin pour nos activités quotidiennes. Nous détruisons/effaçons les données conformément aux délais suivants (et nous le documentons) :

| | |
|---|---|
| Dossier personnel | 10 ans après départ |
| Données RH temp. pertinentes | 3-5 ans (p. ex. qualifications, absences) |
| Candidatures | 4 mois après rejet |
| Contrats | 10 ans après exp. (20 ans si risques de santé) |
| Comptabilité | 15 ans après EF |
| Correspondance sur un sujet | Analogue au sujet en question (ex. contrats) |
| Cas d'assurance | 20 ans |
| | |
| | |
| | |

☐ Nous avons une liste séparée/autre liste

## Nos règles pour la sécurité des données ?

Nous ne partageons jamais notre MdP et ne l'utilisons pas pour des comptes privés ou d'autres comptes.

Nous ne laissons jamais sans surveillance des données confidentielles ou des appareils contenant de telles données.

Nous ne stockons pas de données professionnelles sur des ordinateurs privés ou dans des e-mails privés.

Nous ne cliquons pas sur des pièces jointes ou des liens provenant de sources inconnues/peu sûres.

Nous maintenons nos appareils à jour, mais nous n'installons des logiciels qu'avec autorisation.

Nous n'entrons pas de données confidentielles dans des services en ligne non autorisés à cet effet.

Nous sommes discrets lors de conversations et lorsque nous travaillons sur l'ordinateur en présence de tiers

Nous ne jetons pas les données personnelles de tiers à la poubelle, mais dans un broyeur.

Nous évitons les doublons de données.

Nous ne communiquons des données personnelles à des personnes autorisées que si cela est nécessaire.

## Personnes responsables ?

| Traitement de données | Qui ? |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

CPD :

## Que faisons nous des données de nos employés ?

Nous collectons les données personnelles que vous nous fournissez, ainsi que les données personnelles provenant de registres publics, d'autorités, d'Internet, des médias, de fichiers d'activités informatiques et d'e-mails.

Nous traitons les données personnelles pour interagir avec vous, pour exécuter la relation de travail (y.c. utiliser les prestations/résultats de travail), pour le développement du personnel, à des fins de sécurité, à des fins opérationnelles, pour se conformer au droit applicable, pour les procédures, les enquêtes, les évènements et le marketing.

Nous communiquons les données personnelles à des prestataires, aux autorités, à des clients et à d'autres partenaires, ainsi qu'aux sociétés du groupe, aux médias, au public et à d'autres employeurs.

Notre décl. de protection des données s'applique pour le surplus.

☐ Décl. séparée pour les données du personnel.

Version 08.01.2024 – Mises à jour : www.rosenthal.ch

* Les données personnelles sont les données qui se rapportent à des personnes identifiables directement (p. ex. par leur nom, leur photo) ou indirectement par le biais de sources tierces (p. ex. description de la fonction).

Abréviations : expiration (**exp.**), exercice financier (**EF**), déclaration (**décl.**), mot de passe (**MdP**), etc.

Auteur : David Rosenthal, drosenthal@vischer.com, Contact : Samira Studer, sstuder@vischer.com.


VISCHER
SWISS LAW AND TAX

# Une directive simple et générale sur la protection des données pour les PME.



Destinée aux petites et moyennes entreprises, la page précédente propose une directive sur la protection des données simple mais couvrant les points essentiels de la protection des données. Cette directive est également conforme à la nouvelle loi sur la protection des données (**LPD**) qui est entrée en vigueur le 1er septembre 2023.

Elle complète notre "guide de survie" sur la LPD, qui contient aussi sur une seule page les exigences essentielles de la LPD. La direction d'une organisation peut adopter cette directive et également fixer les responsabilités nécessaires. Selon notre expérience, une attention insuffisante est trop souvent accordée à ce dernier point alors qu'il revêt une importance particulière compte tenu du renforcement des dispositions pénales de la LPD (cf. en outre notre blog https://www.vischer.com/en/knowledge/blog/know-how/blog/how-to-avoid-criminal-liability-under-the-revised-swiss-dpa-1-1-1/)


https://www.rosenthal.ch/downloads/VISCHER-nLPD-Survival-Guide.pdf

Afin d'adopter la directive, vous devez d'abord remplir les champs de la première page. Inscrivez le **nom de la société** ; vous pouvez également ajouter votre propre logo en haut à droite.

Dans un deuxième temps, vous devez compléter le tableau des **délais de conservation**. Nous avons déjà inscrit quelques délais de conservation typiques, vous pouvez en ajouter d'autres dans ce formulaire ou sur une liste séparée. La règle de base est que vous devez détruire ou effacer les documents et les données personnelles lorsqu'un délai légal de conservation a expiré et qu'il n'est plus nécessaire de les conserver (p. ex. parce que les documents peuvent encore servir de moyen de preuve tant que les délais de prescription n'ont pas expiré). Ces délais de conservation ne font formellement pas partie d'une directive sur la protection des données mais ils manquent fréquemment dans la pratique. Nous les avons donc intégrés à notre modèle, comme "bonus" en quelque sorte.

Vous devez déterminer quelle **personne** est **responsable** (la "**PR**") de quel traitement de données. Pour chaque activité dans laquelle des données personnelles sont traitées, une personne doit être responsable du respect de la protection des données, c'est-à-dire qu'elle doit prendre les décisions nécessaires. Il s'agit en principe du "business owner", parce que le traitement des données est effectué pour lui. Il bénéficie de cette activité et en supporte les coûts.

Il doit donc disposer du pouvoir de décision. En pratique, il dira à un/une collaborateur-trice effectuant un traitement de données ce qu'il faut faire. P. ex. celui qui dirige le service des RH détermine combien de temps tels documents sont conservés, qui y a accès, quelles données sont traitées, où elles sont traitées etc. Dans une toute petite société, il peut s'agir de la direction.

Cette personne (PR) doit veiller – elle-même, par des employés, par une instance externe – que les règles de protection des données sont appliquées comme prévu dans le guide de survie. Elle doit s'assurer qu'une déclaration de protection des données existe, que les "10 commandements" sont respectés, que les contrats nécessaires sont conclus avec les tiers, que la sécurité des données est assurée et que les droits des personnes concernées sont garantis en cas de requête. La directive peut indiquer la PR pour certains traitements de données (p. ex. la direction).

Le/la **coordinateur-trice de la protection des données** doit aussi être indiqué-e (si il/elle existe ; dans les petites entreprises, la PR assume ce rôle). Sans être spécialiste, cette personne a une fonction de coordination et de conseil. Elle doit savoir où se renseigner et se charger des tâches opérationnelles. Son nom devrait apparaître dans le guide avec ses tâches (sous le titre "nous avons quelqu'un qui sait ce qu'il faut faire quand…" et "Questions" en bas à droite).

Enfin, la directive permet d'ajouter des commentaires et de mentionner d'autres **directives ou règles individuelles** (p. ex. d'autres choses à observer ou des documents). Tout en haut à gauche, on peut indiquer qui a **adopté** la directive, quand et à partir de quand elle est valable.

**Remarque :** À titre de "bonus", nous avons intégré une brève déclaration de protection des données pour les collaborateurs-trices (en bas à droite) car un tel document est recommandé par la LPD. Comme il n'y a pas de place pour tout et que nous supposons que toutes les entreprises ont une déclaration "ordinaire", nous renvoyons simplement à celle-ci pour davantage d'informations.

Avez-vous des questions ou besoin de modèles plus complets, de matériel de formation ou de l'aide? Adressez-vous à votre interlocuteur de confiance ou à nous à l'adresse e-mail dataprivacy@vischer.com.