

Q&A Protection des données

1. Qu'est-ce que la protection des données?

Toute personne a le droit de déterminer elle-même si, et dans quel but, les données la concernant peuvent être traitées. C'est le droit constitutionnel à l'autodétermination en matière d'information. En conséquence, la protection des données et la loi sur la protection des données (LPD) servent à mettre en œuvre cette autodétermination.

La protection des données ne concerne donc pas la protection technique des données, c'est-à-dire la sécurité des techniques d'information ou la cyber sécurité. Il s'agit bien plus de la réalisation de l'autodétermination en matière d'information et de la protection des données personnelles contre toute violation de la protection des données. Afin de pouvoir garantir cette sécurité, il faut prendre des mesures techniques et organisationnelles.

2. Que signifie «traiter les données»?

Le terme : «traitement des données» est défini dans la loi et comprend tout, de la sauvegarde à la suppression des données. Ce faisant, peu importe que le traitement se fasse dans le domaine numérique ou analogique. Le fait de noter des données de contact au téléphone constitue également un traitement de données et tombe sous le coup de la LPD.

Le terme: «traitement des données» est volontairement vaste et technologiquement neutre. C'est pour garantir que la LPD s'appliquera également aux futurs développements (technologiques). Pour vous, cela signifie cependant que tous les contacts personnels impliquent dans la règle aussi un traitement des données. Vous devriez en être conscient·e·s.

3. Pourquoi la protection des données est-elle importante pour moi ?

En règle générale, la protection des données vous concerne à deux niveaux: d'une part, vous traitez vous-mêmes des données et, d'autre part, vous êtes la personne concernée. En d'autres termes, vous traitez vous-mêmes des données et vos propres données sont, elles aussi, traitées.

En tant que collaborateur·trice, dans une entreprise, une fondation ou une OBNL vous êtes responsable du traitement des données, qui peut concerner le traitement de données internes concernant le personnel mais aussi des données externes sur la clientèle, les fournisseurs, les destinataires, les donateur·trice·s, etc. Simultanément, vos propres données sont traitées, que ce soit dans Internet ou dans la vie de tous les jours privées ou professionnelles.

Raison suffisante pour vous demander ce que la nouvelle loi sur la protection des données va changer pour vous comme chargé·e du traitement des données et pour vous comme personne concernée.

4. Qu'est-ce qui va changer avec la nouvelle loi sur la protection des données?

La nouvelle LPD doit rendre la protection des données personnelles plus efficace. En outre, il convient de s'assurer que la personne concernée puisse aussi effectivement exercer ses droits. Cela implique, d'une part, que l'on puisse déterminer les données spécifiques qui ont été traitées et au cours de quel processus et, d'autre part, qui est responsable du traitement des données.

La personne chargée du traitement des données doit donc, dès l'acquisition des données, fournir des informations exhaustives sur le traitement des données. Ensuite, et sur demande, elle doit fournir des informations sur le traitement de ces données. En outre, elle doit le documenter de manière adéquate et évaluer en amont s'il existe un risque important pour la personne concernée si ces données sont traitées. La personne chargée du traitement des données doit s'assurer, tant au niveau technique qu'organisationnel, qu'il n'y aura pas de violation de la protection des données. En cas de violation, elle est tenue de le signaler. En bref, la nouvelle LPD prévoit un catalogue complet d'obligations pour la personne chargée du traitement des données.

En même temps, les droits des personnes concernées sont renforcés. Entre autres, le droit à l'information, à la suppression et à la correction ainsi que le droit à la portabilité des données (transfert des données).

5. Qu'est-ce qu'une déclaration de protection des données?

La personne concernée doit être informée dès l'acquisition de ses données sur le traitement de ses données. Il convient donc de communiquer clairement de quelles données il s'agit, comment elles sont traitées et dans quel but. C'est à ça que sert ce qu'on appelle la déclaration de la protection des données. Ce genre de déclaration est le moyen le plus simple de remplir une obligation d'information. Car avec une telle déclaration un nombre

indéterminé de personnes peuvent être informées de tous les traitements de données.

6. Qu'est-ce qu'un registre des activités de traitement?

Les responsables et les sous-traitants doivent tous tenir un registre de leurs activités de traitement. Il s'agit avant tout de l'identité de la personne responsable, du but du traitement, d'une description des catégories des personnes concernées et des données personnelles traitées, des catégories de destinataires, si possible la date de conservation des données personnelles ou des critères de détermination de cette durée ainsi qu'une description générale des mesures visant à assurer la sécurité des données et – si les données doivent être divulguées à l'étranger – l'Etat.

Le but de ce registre des activités de traitement est de renforcer la transparence. Afin de pouvoir se défendre efficacement contre un traitement illégal des données il faut que la personne concernée sache d'abord qui traite les données personnelles la concernant et dans quelle mesure.

7. Que faut-il faire lors d'une analyse d'impact relative à la protection des données?

Les responsables sont tenus de concevoir le traitement des données, techniquement et sur le plan organisationnel afin que les prescriptions en matière de protection des données soient respectées. Dans la mesure où le traitement des données est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée une analyse d'impact relative à la protection des données doit être effectuée. Ce faisant, les risques pour les droits fondamentaux des personnes concernées doivent être identifiés en conséquence, évalués et réduits par des mesures appropriées.

Il faut tout d'abord décrire systématiquement l'activité de traitement prévue des données à caractère personnel. Ensuite, il convient d'apprécier la nécessité et la proportionnalité du traitement ainsi que les risques pour les droits fondamentaux des personnes concernées pouvant découler du processus de traitement. S'il y a des risques, des contre-mesures appropriées doivent être prises pour les réduire ou les éviter.

8. Comment mettre en place la protection des données?

Pour une simplification organisationnelle il est judicieux de nommer à l'interne une personne responsable de la protection des données ou une équipe de responsables de la protection des données, qui vérifieront le respect de la protection des données et agiront en tant que personnes de contact. Dans la mesure du possible, cette équipe comprendra également un membre du service informatique.

Tout d'abord, il convient de faire le point sur le traitement des données en cours dans l'entreprise ainsi que les mesures de protection des données existantes. Il faudrait, entre autres, déterminer qui traite quelles données et dans quel but, qui a accès à ces données, où elles sont stockées et quand elles sont détruites. Idéalement, il faudrait aussi saisir cette occasion pour créer un Répertoire du traitement des données.

Une fois que toutes les informations nécessaires sont réunies, on peut procéder à une première analyse de risques et prendre les éventuelles mesures d'urgence nécessaires. Cela comprend la rédaction de la déclaration de la protection des données et l'obtention des consentements nécessaires. A quoi viennent s'ajouter les autres mesures techniques et organisationnelles pour prévenir les violations de la protection des données telles que la restriction des droits d'accès comme, par ex., l'amélioration de la sécurité informatique ou la formation du personnel. Si nécessaire, il faut également effectuer l'analyse d'impact relative à la protection des données.

Et pour finir: La mise en œuvre de la protection des données est une entreprise exigeante. En cas d'ambiguïté et de doute nous vous recommandons de vous faire aider par une personne spécialisée et qualifiée. N'hésitez pas à nous contacter. Nous nous ferons un plaisir de vous conseiller sur toutes les questions relatives à la protection des données.

proFonds, Association faitière des fondations d'utilité publique de Suisse

Tél. 061 272 10 80
info@proFonds.org
www.proFonds.org

En tant qu'Association faitière, proFonds remplit des tâches importantes au profit de l'ensemble des fondations et des organisations d'utilité publique.

L'objectif étant de maintenir et de continuer à développer des conditions-cadres favorables pour que les fondations et autres organisations d'utilité publique soient en mesure de s'épanouir en Suisse.

En plus de son engagement dans le domaine de la défense des intérêts, **proFonds offre à ses membres une large palette de services** et favorise ainsi le réseautage, l'échange de connaissances et d'expériences ainsi que la professionnalisation au sein du domaine des fondations et des organisations d'utilité publique.