Recommandation sectorielle sur la révision de la loi sur la protection des données – **Mise en œuvre**

01.23fr, Annexe A, Version 1.1

Ce document est subordonné au document «Recommandation sectorielle sur la révision de la loi sur la protection des données – Principes de base».

1. Directives pour la mise en œuvre

La LPD et son ordonnance contiennent des directives détaillées. Pour faciliter leur mise en œuvre concrète, les directives sont détaillées ci-après. La méthode de travail pratique sera décrite ensuite pas à pas au chapitre suivant «Recommandation pour la mise en œuvre».

Le SVIT Suisse conseille dans tous les cas aux entreprises de l'économie immobilière de créer un registre des activités de traitement selon l'art. 12 LPD comme base pour un état des lieux et la mise en œuvre de la LPD. Les entreprises peuvent ainsi s'assurer qu'elles identifieront tous les processus importants pour la LPD et instaureront une gestion adéquate.

2. Devoirs des responsables

Par «responsable» ou personne qui traite les données, on entend en règle générale l'entreprise concernée, respectivement le sous-traitant (par exemple un fournisseur informatique). Le responsable, respectivement le sous-traitant, doit en effet respecter les obligations décrites ci-après. Dans l'application pratique, une entreprise devrait mettre en œuvre l'exigence suivante pour chaque processus consigné dans le registre des activités, pour autant qu'elle s'applique. Cette énumération a donc une fonction de check-list pour la mise en œuvre.

1. La personne qui traite les données doit conserver une information adéquate sur la personne concernée. Il est donc judicieux d'intégrer pour tous les formulaires (en ligne et physiques) la politique de confidentialité dans les conditions générales de ventes (CGV) (ou comme disposition contractuelle) et la politique de confidentialité en ligne sur le site de l'entreprise.

2. Dans le cas où la sélection du locataire se fait sur la base d'une décision individuelle automatisée, il n'y a pas d'obligation d'informer si la décision individuelle automatisée est directement liée à la conclusion ou à l'exécution d'un contrat entre le responsable et la personne concernée. Il n'y a pas non plus d'obligation d'informer si la personne concernée a consenti explicitement à ce que la décision soit automatisée. Dans tous les autres cas, il existe une obligation d'informer et il faut offrir à la personne concernée qui le demande la possibilité de faire valoir son point de vue. La personne concernée peut exiger que la décision individuelle automatisée soit contrôlée par une personne physique.

3. Le responsable est tenu d'assurer au moyen de préréglages (paramètres par défaut) que le traitement des données personnelles reste limité au niveau minimal nécessaire pour le but d'utilisation. Ainsi, il convient par exemple de renoncer au préréglage (champ coché) pour l'envoi de newsletter ou l'enregistrement obligatoire dans une banque de données clients.

4. Le responsable doit tenir un registre qui renseigne sur les activités de traitement. Les entreprises ou les organisations de droit privé qui occupent moins de 250 personnes au début d'une année, de même que les personnes physiques sont exemptées, selon l'art. 26 LPD, de l'obligation

de tenir un registre des activités de traitement, sauf si l'une des conditions suivantes est remplie:
- Des données sensibles sont traitées à grande échelle.
- Elles pratiquent un profilage à risque élevé. Le SVIT Suisse recommande néanmoins dans tous les cas de créer un tel registre.

5. Il convient de noter que l'extrait du registre des poursuites d'une personne est considéré comme sensible au sens de la LPD. Le SVIT Suisse défend le point de vue selon lequel, lors d'une demande d'extrait du registre des poursuites, on ne recueille pas encore des données sensibles **à grande échelle**. C'est la raison pour laquelle le SVIT Suisse part du principe que tous les membres de l'association qui occupent moins de 250 collaborateurs bénéficient d'une dérogation.

6. Du point de vue du SVIT Suisse, il n'est pas nécessaire pour les entreprises du secteur immobilier de procéder à une analyse d'impact sur la protection des données personnelles, car en règle générale, elles ne surveillent ni le traitement de données sensibles à grand échelle ni de vastes portions du domaine public de manière systématique.

7. En raison de la dérogation dont les entreprises immobilières bénéficient pour l'analyse d'impact sur la protection des données personnelles, le SVIT Suisse estime qu'elles peuvent renoncer à une consultation avec le Préposé fédéral à la protection des données (PFPDT).

8. Il existe en principe une obligation d'annoncer au PFPDT les violations constatées de la sécurité des données. Toutefois, cette obligation ne s'applique que si l'on peut supposer que cette violation entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Le SVIT Suisse estime qu'un tel cas de figure est rarissime dans l'économie immobilière, car il est exceptionnel que des données qui entraînent un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée soient stockées.

9. Le responsable du traitement ou le sous-traitant est tenu d'informer lorsque des données personnelles sont collectées. Dans le cas du secteur immobilier, on pense ici aux informations sur la solvabilité. En règle générale, cette information se fait par le biais de la politique de confidentialité.

10. En ce qui concerne la collaboration entre le responsable du traitement et le sous-traitant, une attention particulière doit être accordée à la protection des données, notamment avec les sous-traitants établis à l'étranger. Le responsable qui confie le traitement de données personnelles à un sous-traitant reste responsable de la protection des données. Il doit s'assurer que les données sont traitées conformément au contrat ou à la loi.

11. La LPD prévoit un droit d'accès. Toute personne concernée peut demander à connaître les données enregistrées à son sujet. Il faut s'assurer que les informations soient fournies exclusivement à la personne concernée (l'identification par le seul expéditeur du courriel ne suffit pas). Les informations suivantes doivent lui être communiquées:
    - L'identité et les coordonnées du responsable du traitement
    - Les données personnelles traitées en tant que telles
    - La finalité du traitement
    - La durée de conservation des données personnelles ou, si ce n'est pas possible, les critères qui déterminent cette durée. La question de la conservation des contrats de bail et des décomptes de charges est ici particulièrement pertinente (voir ci-dessus).
    - Les informations disponibles sur l'origine des données personnelles, dans la mesure où elles n'ont pas été obtenues auprès de la personne concernée.
    - Le cas échéant, l'existence d'une décision individuelle automatisée ainsi que la logique sur laquelle repose ladite décision. Pour le secteur immobilier, cela peut éventuellement revêtir de l'importance, mais uniquement pour le formulaire de demande de location. Comme indiqué ci-dessus, celui-ci doit être détruit le plus

rapidement possible si aucun contrat n'a été conclu.
- Le cas échéant, les destinataires ou les catégories de destinataires auxquels les données personnelles et les informations visées à l'art. 19, al. 4 (informations à l'étranger) sont communiquées. Il convient de noter ici que dès que les données relatives au locataire sont communiquées au propriétaire par la gérance, le locataire doit en être informé dans le cadre de cette demande.

12. Exigences en matière de sécurité des données dans l'entreprise: l'entreprise doit mettre en place des procédures pour la sécurité des données (art. 1 seq. RGPD). Voir par exemple à ce sujet le Centre national pour la cybersécurité NCSC de la Confédération.

Personne de référence

En raison de la complexité que représente la réponse à de telles demandes, le SVIT Suisse conseille de confier cette tâche à une seule personne et de mettre en place une procédure adéquate afin de respecter le délai de 30 jours. Il faut également veiller à ne pas confirmer l'exactitude ou l'exhaustivité des données. Ce point n'est pas prévu par la loi. Il ne peut donc pas être exigé et n'est pas juridiquement valable. Il en va de même pour l'obligation de remise. Une obligation d'information n'est pas une obligation de remise. Une obligation de remise n'existe que pour les données que la personne concernée a communiquées elle-même.

Il faut veiller à ne pas fournir intentionnellement des informations fausses ou incomplètes, car de tels actes sont punissables.

Données personnelles existantes

Dès l'entrée en vigueur de la LPD, il faut s'assurer que les données personnelles sensibles enregistrées soient soit effacées, soit anonymisées, soit utilisées de manière légale en obtenant le consentement pour qu'elles soient traitées et enregistrées.

3. Recommandation pour la mise en œuvre

Les dix points ci-après portent sur la mise en œuvre de la loi révisée sur la protection des données (LDP) et de l'ordonnance révisée sur la protection des données (OPDo) dans les entreprises. Ils proposent une recommandation basée sur l'activité typique de l'économie immobilière. Si nécessaire, ils doivent être adaptés au cas par cas et aux conditions spécifiques de l'entreprise ainsi qu'à la manière dont elle gère les données personnelles.

1. Définir les responsabilités: Une personne doit être désignée comme préposé à la protection des données. En règle générale, il s'agit d'un membre de la direction. Car la protection des données est une affaire de chef.

2. Evaluer les points de contact avec la LPD et l'OPDo: Lors d'une première étape, il s'agira de déterminer où les données personnelles sont traitées dans l'entreprise et si, le cas échéant, ce sont des données sensibles. Il faut notamment penser aux sites Internet et au traitement par les collaborateurs dans leur environnement de travail personnel (par exemple sauvegarde d'e-mails, d'une banque de données d'adresses sur un ordinateur ou des appareils mobiles). Il convient de vérifier si les données stockées sont concernées par un devoir d'information ou une obligation de déclaration. Et enfin vérifier également si des données personnelles peuvent être communiquées à l'étranger (art. 16 et seq. LPD).

3. Définir la gestion des données personnelles: Suivant l'opération commerciale, il faut déterminer la manière dont les données personnelles sont traitées pour différentes catégories, notamment le moment où elles doivent être effacées. Ce point doit être précisé dans la politique de confidentialité et appliqué en interne (voir ci-dessous).

4. Examiner la collaboration avec des tiers: Il s'agit de déterminer si, dans le cadre de la collaboration, la répartition du travail concernant les données personnelles est non problématique ou si l'on a affaire à une «sous-traitance» de données personnelles au sens de l'art. 9 LPD. Dans ce cas, le responsable doit contrôler que son sous-traitant respecte la protection des don-

nées et ce dernier doit s'engager contractuellement à l'observer (voir art. 9 al.1 et 2 LPD). Pour ce faire, le responsable conclut avec le sous-traitant une «commande de sous-traitance». Le sous-traitant devrait de son côté exiger également une commande de sous-traitance de la part de son mandant. Le SVIT Suisse renvoie à cet effet aux instructions correspondantes (insérer le lien) et au modèle de convention pour le traitement des commandes avec documents complémentaires (insérer le lien) de l'organisation de la branche «The Branch».

5. Adapter les formulaires et les modèles de contrat pour les personnes physiques: Il convient de vérifier si les directives relatives à la protection des données sont suffisamment explicites et si les consentements sont demandés lorsque c'est nécessaire.

6. Adapter les processus automatiques: Les systèmes informatiques doivent être adaptés pour que le traitement (en particulier l'effacement) se fasse automatiquement, par exemple dans le cas des cookies.

7. Adapter les directives et les règlements internes: Les collaborateurs doivent être informés de manière adéquate de la politique de confidentialité et de la gestion conforme au droit de données personnelles, et recevoir des instructions à ce sujet.

8. Adapter la politique de confidentialité: Les documents existants doivent être adaptés à la LPD. Il faut préciser de manière intelligible et appropriée la manière dont les différentes catégories de données personnelles doivent être gérées suivant le processus d'affaires.

9. Définir des procédures: Des procédures doivent être établies pour les cas de demande d'information ou de violation de la protection des données.

10. Etablir un système de gestion pour la protection des données: La gestion de la protection des données est un processus continu d'implémentation, de surveillance et, le cas échéant, d'adaptation des directives.

Éditeur:

SVIT Suisse
Greencity, Maneggstrasse 17
8041 Zurich
Telefon 044 434 78 88
info@svit.ch, www.svit.ch

Avec l'aimable soutien de:

thebranch