Directive sur la protection des données

SVK CPSA Parifonds Bau

I Contenu

1 De quoi s'agit-il ?

La présente directive définit la manière dont nous traitons les données personnelles conformément à la loi suisse sur la protection des données (LPD) et à l'ordonnance correspondante (OPDo). Tous les collaborateurs et collaboratrices (y compris les sous-traitants et les autres personnes travaillant au sein de notre organisation commune) sont tenus de la respecter lorsqu'ils traitent des données personnelles pour notre compte ou chez nous.

Traitement des données personnelles

La protection des données concerne les données personnelles. Il s'agit d'informations concernant une personne physique identifiée ou identifiable (personne concernée). Les personnes concernées peuvent être par exemple des collaborateurs et collaboratrices, des clients ou d'autres personnes. Toute opération relative à des données personnelles est qualifiée de traitement, notamment la collecte, l'utilisation, l'enregistrement, la communication ou l'effacement de ces données. Le droit de la protection des données prévoit des règles plus strictes pour les données personnelles sensibles.

Qu'entend-on par données personnelles sensibles ?

- Données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales
- Données sur la santé, la sphère intime, l'origine raciale ou ethnique
- Données génétiques
- Données biométriques identifiant une personne physique de manière univoque
- Données sur des poursuites ou sanctions pénales et administratives
- Données sur des mesures d'aide sociale

2 Principes

Lorsque nous traitons des données personnelles selon la LPD, aucune base légale particulière n'est requise, tant que nous respectons les principes de traitement définis dans la présente section (fond bleu). Nous avons toutefois besoin d'un motif justificatif si :

- nous ne respectons pas l'un de ces principes ;
- la personne concernée s'oppose au traitements ; ou
- des données personnelles sensibles sont transmises à des tiers pour leurs propres finalités.

Quand avons-nous un motif justificatif ?

Il y a justification au sens de la LPD lorsqu'il existe un consentement, qu'une loi prévoit le traitement des données ou qu'il existe un intérêt prépondérant, comme dans les situations suivantes :

- traitements en relation directe avec la conclusion ou l'exécution d'un contrat, ou
- traitements de données de clients en vue d'améliorer nos propres produits et services.

Consentement

Dans la mesure du possible, nous évitons de compter sur un consentement, car :

- obtenir un consentement juridiquement valable est difficile, ce consentement devant être libre et éclairé ;
- un consentement peut être révoqué à tout moment ;
- nous devons veiller à pouvoir cesser le traitement à tout moment, sans efforts disproportionnés.

Il convient de consulter le **service de protection des données.**

Transparence et équité

Nous faisons preuve de transparence et d'équité dans le traitement des données personnelles :

- en informant les personnes concernées lors de la collecte des données ;
- en mettant à disposition une déclaration de protection des données à jour qui énumère toutes nos collectes de données ;
- en vérifiant si les nouveaux traitements sont déjà couverts par la déclaration de protection des données ;
- en considérant également les collaborateurs et collaboratrices comme des personnes concernées ;
- en respectant la bonne foi.

Directive sur la protection des données

SVK CPSA Parifonds Bau

Principe de finalité et minimisation des données

- Nous n'utilisons les données personnelles qu'aux fins pour lesquelles nous les avons collectées.
- Nous informons les personnes concernées de ces finalités et d'une éventuelle transmission de données.
- Nous ne collectons que les données personnelles nécessaires et les traitons avec parcimonie.
- Si nous souhaitons utiliser les données personnelles à une autre fin que celle pour laquelle elles ont été collectées, nous contactons le **service de protection des données**.

Conservation, accès et exactitude

- Nous limitons l'accès aux données personnelles aux personnes qui en ont réellement besoin (principe du « *need to know* »).
- Nous ne conservons les données personnelles qu'aussi longtemps que nous en avons besoin pour la finalité concernée ou pour des raisons légales, puis nous les effaçons ou les anonymisons.
- Nous veillons à ce que les données personnelles soient correctes et rectifiées lorsqu'elles ne le sont plus.

Confidentialité et compliance

- Nous ne transmettons des données personnelles secrètes, qui nous sont confiées dans le cadre de nos activités professionnelles, à des tiers que si la personne concernée s'y attend, si la loi l'exige ou si nous l'avons annoncé.
- Dans la mesure du possible, nous laissons le choix aux personnes concernées. En cas d'opposition à un traitement, nous nous y conformons, dans la mesure où cela est acceptable pour nous et autorisé par la loi.
- Nous veillons toujours au respect des principes du traitement des données et faisons appel au **service de protection des données**.

Sécurité des données

Nous veillons à une sécurité appropriée des données (confidentialité, disponibilité, intégrité et traçabilité des données) sur le plan technique et à tout autre égard :

- Cela ne concerne pas seulement ceux qui s'occupent de l'infrastructure (informatique, bâtiments), mais l'ensemble des collaborateurs et collaboratrices.
- Nous respectons les prescriptions de la présente directive (chiffre 7) ainsi que les prescriptions du service informatique.
- Nous annonçons les violations de la sécurité des données (chiffre 8).

3 Situations particulières

Dans certaines situations particulières, d'autres règles et prescriptions à respecter s'appliquent.

La **personne responsable du traitement des données** est responsable du respect de ces règles et prescriptions (chiffre 4).

Elle fait appel suffisamment tôt au **service de protection des données** pour des conseils.

Recours à des tiers

En cas de recours à des tiers (p. ex. fournisseurs de services informatiques), nous tenons compte des points suivants :

- Nous clarifions le rôle du tiers (« sous-traitant », « responsable du traitement » ou « responsable conjoint »).
- Nous vérifions la qualification, la fiabilité et la sécurité des données.
- Nous concluons un contrat (p. ex. contrat de sous-traitance) qui régit les finalités du traitement des données par le tiers.
- Nous faisons appel au **service de protection des données**.

Communication à l'étranger

La communication de données à des destinataires situés en dehors de la Suisse n'est autorisée que si :

- le destinataire se trouve dans un pays assurant un niveau de protection des données adéquat, ou
- en l'absence d'un niveau de protection adéquat :
  - nous évaluons le risque d'un accès par des autorités étrangères, nous concluons une convention et prenons d'autres mesures si nécessaire,
  - nous trouvons une autre solution, si nécessaire.

Il convient de consulter le **service de protection des données.**

Décisions individuelles automatisées

Chaque fois que nous laissons un ordinateur prendre une décision discrétionnaire au sujet d'une personne concernée (décision individuelle automatisée) et que cela est susceptible d'avoir des effets juridiques ou similaires significatifs pour cette personne (p. ex. refus d'un contrat), les restrictions prévues par le droit de la protection des données s'appliquent, raison pour laquelle nous faisons appel au préalable au **service de protection des données**.

Directive sur la protection des données

SVK CPSA Parifonds Bau

4 Rôles et responsabilités

Le **secrétariat** (**direction**) est responsable sur le plan opérationnel du respect du droit de la protection des données. Les tâches de la **personne responsable du traitement** sont déléguées par la direction au service de protection des données. La personne qui délègue reste responsable du soin apporté à la sélection, à l'instruction et à la surveillance (« *reporting* »).

Responsable du traitement des données

La **personne responsable du traitement** est responsable, conjointement avec le supérieur hiérarchique, le secrétariat et les personnes qui décident concrètement du traitement des données (p. ex. parce qu'elles le « font » tout simplement) :

- du respect de la présente directive et de la mise en œuvre de la protection des données dans son domaine ;
- de la documentation relative à la mise en œuvre ;
- des décisions en matière de protection des données.
- Si la personne responsable du traitement ne peut ou ne veut pas prendre de décision, il appartient au supérieur hiérarchique de le faire.

Service de protection des données

Tâches et droits du **service de protection des données** :

- appliquer la présente directive dans l'entreprise ;
- conseiller et former la direction, la personne responsable du traitement et les collaborateurs et collaboratrices en matière de protection des données ;
- fournir un soutien dans le cadre de projets ;
- contrôler le respect de la protection des données ;
- faire un rapport à la direction sur la situation en matière de protection des données ;
- mettre à jour la déclaration de protection des données, avec le soutien de la personne responsable du traitement ;
- exécuter ses obligations selon la présente directive.

Tous les collaborateurs et collaboratrices

Les collaborateurs et collaboratrices ont les responsabilités suivantes :

- respecter la présente directive et d'autres directives ;
- suivre les formations proposées ;
- connaître les informations relatives à la protection des données mises à la disposition des personnes concernées (p. ex. déclaration de protection des données) ;
- demander des précisions au service de protection des données en cas d'incertitudes ;
- traiter les données selon les consignes de la personne responsable du traitement.

5 Processus et gouvernance

En cas de nouveaux projets ou de modifications de projets, la personne responsable du traitement doit :

- garantir le respect des principes de protection des données et d'autres prescriptions conformément à la présente directive ;
- consulter le **service de protection des données** ;
- annoncer le traitement au service de protection des données afin que celui-ci puisse compléter la déclaration de protection des données et, le cas échéant, le registre des activités de traitement et d'autres documents ; et
- établir une analyse d'impact relative à la protection des données personnelles en cas de risque potentiellement élevé.

Demandes des personnes concernées

Nous accordons aux personnes concernées leurs droits :

- renseignements sur les données personnelles traitées ;
- rectification de données inexactes ;
- opposition au traitement des données ;
- effacement des données ;
- transmission des données à un autre responsable du traitement.

Le **service de protection des données** traite ces demandes. Tous les collaborateurs et collaboratrices transmettent les demandes sans délai au service de protection des données et lui apportent leur soutien pour les traiter et y répondre.

Registre des activités de traitement

- Le service de protection des données tient un registre des activités de traitement conformément aux prescriptions légales.
- La personne responsable du traitement annonce les activités de traitement au service de protection des données et lui apporte son soutien.
- Si une exception à l'obligation de tenir un registre de traitement s'applique à nous, la direction décide s'il faut tenir un registre simplifié ou y renoncer.
- Le registre comprend la liste des personnes responsables du traitement.

Règlement relatif au traitement et journalisation

Nous édictons un règlement relatif au traitement des données et assurons la journalisation :

- lorsque nous traitons des données sensibles à grande échelle, ou
- lorsque nous effectuons un profilage à risque élevé.

La responsabilité incombe à la personne responsable du traitement, qui doit au préalable consulter le service de protection des données.

Directive sur la protection des données

SVK CPSA Parifonds Bau

6 Conservation et effacement

Nous conservons les données personnelles aussi longtemps :

- qu'elles sont nécessaires aux fins pour lesquelles elles ont été collectées ;
- que leur conservation est prescrite ;
- que cela est nécessaire à un autre but professionnel légitime (p. ex. preuve dans le cadre d'un litige, historique de l'entreprise).

Nous archivons les données qui ne sont plus nécessaires à un usage quotidien, limitons l'accès à ces données et tenons un journal des accès.

Mise en œuvre de la conservation

- Les délais de conservation figurent dans un document séparé.
- Des dérogations sont autorisées dans des cas justifiés en accord avec le service de protection des données.
- La direction et le service de protection des données peuvent ordonner un blocage de l'effacement (*legal hold*).
- La personne responsable du traitement est responsable de l'effacement dans son domaine d'activité.
- Si l'effacement ne peut pas être raisonnablement effectué, l'accès aux données est limité en accord avec le service de protection des données.

7 Utilisation de l'informatique et confidentialité

- Nous ne partageons jamais notre mot de passe et ne l'utilisons pas pour des comptes privés ou autres.
- Nous ne laissons jamais de données confidentielles ni d'appareils contenant de telles données sans surveillance.
- Nous n'enregistrons pas de données professionnelles sur des ordinateurs privés ou des services cloud et les stockons aux emplacements prédéfinis.
- Nous utilisons uniquement des services de messagerie professionnels pour nos communications professionnelles.
- Nous ne saisissons aucune donnée confidentielle dans des services en ligne dont l'utilisation à cette fin n'a pas été autorisée.

Utilisation de l'informatique et confidentialité

- Nous ne cliquons pas sur les pièces jointes et les liens provenant de sources inconnues ou incertaines.
- Nous maintenons nos appareils à jour et n'installons des logiciels que si nous avons l'autorisation de le faire.
- Nous faisons preuve de discrétion lorsque nous menons des discussions et que nous travaillons sur ordinateur à proximité de tiers.
- Nous ne jetons pas de documents contenant des données personnelles de tiers à la poubelle, mais utilisons un broyeur pour les éliminer.
- Nous évitons les clichés instantanés des données.
- Nous veillons à ne transmettre les données personnelles qu'aux personnes autorisées et uniquement dans la mesure nécessaire.

8 Violation de la sécurité des données

En cas de violation de la sécurité des données, c'est-à-dire en cas de divulgation, de modification ou de perte non autorisée ou illicite de données personnelles traitées, il convient d'agir immédiatement.

Tout collaborateur ou toute collaboratrice doit immédiatement informer le service de protection des données et le service informatique lorsqu'il ou elle a connaissance d'une violation de la sécurité des données.

Réaction aux violations de la sécurité des données

- Le service informatique et le service de protection des données prennent immédiatement des mesures d'urgence pour faire cesser la violation et atténuer les conséquences néfastes.
- Le service de protection des données informe immédiatement la direction.
- Dans les cas graves : convocation de la task force, composée du service informatique, du service de protection des données et de la direction, recours immédiat à des conseillers en matière de droit et de sécurité informatique.
- La task force évalue les éventuelles obligations d'annoncer et d'informer.

9 Sanctions

- Les personnes qui violent intentionnellement le droit de la protection des données risquent une amende pénale pouvant aller jusqu'à CHF 250 000.
- Nous pouvons recevoir l'ordre d'arrêter ou d'adapter des activités de traitement.
- Les violations peuvent entraîner des prétentions civiles et des atteintes à la réputation.
- Le respect de la présente directive est obligatoire pour tous les collaborateurs et collaboratrices.
- Le non-respect de la présente directive peut entraîner des sanctions, allant jusqu'au licenciement.

10 Interlocuteurs et modifications

Les coordonnées du service de protection des données et des autres interlocuteurs sont les suivantes :

- Vladan Lazic : vlazic@svk-bau.ch / 044 542 01 42
- Giulio Enea : genea@svk-bau.ch / 044 542 01 46

Le propriétaire de la présente directive est le service de protection des données. Il la révise si nécessaire et la vérifie au moins une fois par an.

Édicté formellement au sens d'une directive par la direction le 01.01.2026.