Remarque préliminaire:

Le modèle de politique de protection des données ci-dessous se concentre sur l'essentiel et donne une structure possible. Il est judicieux de le compléter ou de l'adapter en fonction de la situation concrète de votre entreprise. Pour cela, il peut être utile de faire appel à un spécialiste.

* * * * *

Directive sur la protection des données

I. Généralités

1. Introduction

1.1. Les données disponibles dans l'entreprise sont d'une grande valeur pour l'entreprise. Ces données doivent donc être protégées contre les accès non autorisés et autres menaces.

1.2 Les clients, partenaires et collaborateurs de l'entreprise attendent que les données confiées à l'entreprise soient particulièrement protégées et qu'elles soient traitées avec soin.

1.3 Pour toute question relative à la protection des données ou au traitement des données personnelles, vous pouvez contacter le responsable de la protection des données [nom, adresse électronique/numéro de téléphone ou autre].

1.4 […]

2. Objectif de la directive sur la protection des données

2.1 La présente directive sur la protection des données vise à créer des normes uniformes pour la protection des données dans l'entreprise.

2.2 En respectant les normes définies dans la présente politique de protection des données, l'entreprise remplit ses obligations en matière de protection des données et veille à ce que les intérêts et les droits des personnes concernées soient suffisamment pris en compte.

2.3 Le respect de la présente directive sur la protection des données est une condition préalable à l'échange sécurisé de données personnelles au sein de l'entreprise et avec des tiers.

2.4 […]

3. Champ d'application de la directive sur la protection des données

3.1 La présente directive sur la protection des données s'applique à tout traitement de données personnelles, y compris notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données. Elle s'applique à tous les types de données personnelles, notamment les données relatives aux collaborateurs, clients, fournisseurs et autres partenaires commerciaux.

3.2 La directive sur la protection des données décrit, concrétise ou complète également les dispositions légales, notamment celles de la loi suisse sur la protection des données (LPD).

3.3 […]

4. Définitions

4.1 **Les données personnelles** au sens de la présente directive d'entreprise sont toutes les indications qui se rapportent à une personne physique identifiée ou identifiable.

4.2 **Les personnes concernées** sont les personnes physiques au sujet desquelles des données personnelles sont traitées.

4.3 **Le responsable** est une personne privée qui, seule ou conjointement avec d'autres, décide du but et des moyens du traitement.

4.4 **Le sous-traitant** est un tiers qui traite des données personnelles pour le compte du responsable du traitement.

[…]

II. Règles de base du traitement des données

5. Légalité

5.1 Les données personnelles doivent être traitées de manière licite. Le traitement n'est considéré comme licite que s'il est justifié par (a) le consentement de la personne concernée, par (b) un intérêt privé ou public prépondérant ou par (c) la loi.

6. Transparence

6.1 Le traitement des données doit en principe être effectué de manière à ce que la personne concernée en ait connaissance.

7. Principe de proportionnalité

7.1 Lors du traitement des données, le principe de proportionnalité doit être respecté. Conformément à ce principe, seules les données *nécessaires* et *appropriées* au but poursuivi peuvent être collectées.

7.2 En outre, les données personnelles ne peuvent être conservées que pendant la durée nécessaire à la réalisation du but poursuivi (cf. ci-après).

8. Finalité

8.1 Les données personnelles ne peuvent être collectées que dans un but précis et identifiable par la personne concernée et ne peuvent être traitées que de manière compatible avec ce but.

8.2 Si les données personnelles ne sont plus nécessaires au but du traitement, elles doivent être détruites ou rendues anonymes.

9. Exactitude

9.1 Tous les collaborateurs doivent veiller à ce que les données personnelles soient exactes et tenues à jour.

9.2 Toutes les mesures raisonnables doivent être prises pour rectifier ou détruire les données inexactes ou incomplètes.

10. Sécurité des données

10.1 Pour l'entreprise, il est très important que la sécurité des données soit garantie à tout moment. Dans ce contexte, les données personnelles doivent être protégées par des mesures techniques et organisationnelles, notamment contre la perte, l'accès non autorisé et d'autres dangers.

10.2 Les mesures de protection concrètes doivent être documentées pour les différentes opérations de traitement des données et leur adéquation doit être vérifiée.

10.3 Le service informatique peut édicter des directives plus strictes dans l'intérêt de la sécurité des données, notamment en ce qui concerne l'utilisation de systèmes informatiques dans l'entreprise.

11. Consentement et opposition

11.1 Le consentement de la personne concernée au traitement des données par une entreprise n'est en principe pas nécessaire, même pour les données personnelles sensibles.

11.2 En revanche, si la personne concernée s'oppose expressément à un traitement de données, celui-ci n'est justifié que s'il existe des intérêts prépondérants du responsable ou une base légale.

12. Obligation d'information

12.1 Les personnes concernées doivent, dans la mesure du possible, être informées au préalable de la finalité pour laquelle des données personnelles les concernant sont collectées et traitées. Si les données ne sont pas collectées directement auprès de la personne concernée, celle-ci est informée dans un délai d'un mois à compter de la réception des données.

12.2 Si la personne concernée rend ses données personnelles accessibles au responsable de sa propre initiative, elle est considérée comme informée.

12.3 Si la finalité du traitement des données change, les personnes déjà informées doivent l'être à nouveau.

13. Sous-traitance

13.1 Lorsque des prestataires de services de l'entreprise traitent des données personnelles pour le compte de celle-ci (appelés sous-traitants), il convient de noter que les mêmes exigences de diligence que celles qui s'appliquent à l'entreprise responsable s'appliquent également au sous-traitant. Il convient notamment de garantir par contrat la limitation des finalités et la sécurité des données.

14. Transmission de données personnelles à l'étranger:

14.1 La transmission de données personnelles à l'étranger n'est autorisée que dans les États dans lesquels le Conseil fédéral a constaté un niveau de protection des données aussi élevé qu'en Suisse. Le respect des normes suisses de protection des données peut en outre être obtenu, entre autres, par la conclusion d'accords contractuels supplémentaires.

IV. Processus internes

15. Exigences envers les collaborateurs

15.1 Tous les collaborateurs de l'entreprise sont tenus de respecter la protection des données. Ils sont notamment informés qu'il est interdit d'utiliser des données personnelles à des fins privées, de les transmettre à des personnes non autorisées ou de les rendre accessibles à des personnes non autorisées. L'obligation de respecter la confidentialité s'applique au-delà de la fin de l'engagement.

15.2 Au sein de l'entreprise également, il faut veiller à ce que seuls les collaborateurs qui en ont besoin pour accomplir leurs tâches pour l'entreprise aient accès aux données personnelles.

15.3 Tous les collaborateurs doivent être formés et sensibilisés aux questions de protection des données dès leur recrutement et régulièrement par la suite.

16. Registre des activités de traitement

16.1 L'entreprise tient un registre des activités de traitement en rapport avec les données personnelles. Il doit y être consigné: l'identité du responsable ou du sous-traitant, le but du traitement, la description des catégories de personnes concernées et des catégories de données personnelles traitées, les catégories de destinataires, la durée de conservation ou les critères pour la déterminer, si possible la description des mesures prises pour assurer la sécurité des données ainsi que les éventuels pays de destination si les données sont envoyées à l'étranger. Le registre doit toujours être à jour et donner une vue d'ensemble des activités liées à la protection des données dans l'entreprise.

17. Protection des données dès la conception, protection des données par dafaut et analyse d'impact sur la vie privée

17.1 Les systèmes utilisés pour le traitement des données personnelles doivent être conçus dès le départ de manière à ce que la protection des données puisse être respectée. Les mesures techniques et organisationnelles doivent notamment être adaptées à l'état de la technique, à la nature et à l'ampleur du traitement des données ainsi qu'au risque que le traitement comporte pour la personnalité ou les droits fondamentaux des personnes concernées (Privacy by Design).

17.2 Les responsables doivent choisir les paramètres par défaut de l'appareil ou du logiciel de manière à ce que le traitement des données personnelles soit limité au minimum nécessaire pour l'utilisation prévue, à moins que la personne concernée n'en décide autrement. Cela concerne par exemple l'acceptation de cookies sur le site Internet.

17.3 Une analyse d'impact relative à la protection des données (AIPD) doit être effectuée et documentée, notamment lorsqu'un traitement de données prévu présente un risque élevé pour la personnalité et les droits fondamentaux des personnes concernées.

17.4 […]

V. Droits des personnes concernées

18. Droit d'accès

18.1 Sur demande, une personne concernée doit être informée si des données personnelles la concernant sont traitées par l'entreprise. Si tel est le cas, la personne concernée a le droit

d'accéder aux données personnelles en question. Le droit d'accès consiste à savoir si des données personnelles sont traitées et, si oui, lesquelles, afin que la personne concernée puisse faire valoir ses autres droits. En font partie, outre les données personnelles traitées en tant que telles, des informations sur l'identité du responsable, le but du traitement, la durée de conservation, l'origine des données et, le cas échéant, des informations sur les décisions individuelles automatisées et les destinataires (également en tant que catégories).

18.2 Lors de la communication de renseignements, il convient de s'assurer que l'identité de la personne concernée est vérifiée. Il convient en outre de veiller à ce qu'aucune donnée personnelle de tiers ne soit divulguée dans le cadre de la communication de renseignements. En règle générale, les renseignements doivent être fournis gratuitement et dans un délai de 30 jours.

19. Portabilité des données / droit à la communication et à la transmission des données

19.1 Les personnes concernées peuvent demander à récupérer les données qu'elles ont communiquées à une entreprise dans un format électronique courant, lorsque les données sont traitées de manière automatisée et que la personne concernée a donné son consentement au traitement ou que le traitement est effectué dans le cadre d'un contrat correspondant.

20. Droit à la rectification

20.1 Conformément à l'art. 32 al. 1 LPD, une personne concernée peut exiger que des données personnelles inexactes soient rectifiées.

21. Droit à la suppression des données

21.1 Lorsque des données personnelles sont traitées contrairement à la déclaration de volonté expresse de la personne concernée et qu'il n'existe aucune base légale ni aucun intérêt privé prépondérant de tiers, la personne concernée peut demander la suppression de ses données personnelles.

[…]

VI. Compétence

22. Responsabilité

22.1 La responsabilité du respect des dispositions de la présente directive sur la protection des données incombe en premier lieu aux collaborateurs qui sont chargés du traitement des données.

22.2 Tous les collaborateurs de l'entreprise doivent veiller au respect de la présente directive sur la protection des données et contribuer ainsi à l'établissement de normes élevées et uniformes en matière de protection des données dans toute l'entreprise.

22.3 En cas de violation des obligations légales en matière de protection des données, les contrevenants s'exposent à des conséquences pénales (amende jusqu'à CHF 250 000.-) et l'entreprise à des conséquences civiles (pouvant aller jusqu'à des dommages-intérêts) ainsi qu'à des atteintes à sa réputation. La responsabilité pénale incombe en premier lieu à la personne physique, c'est-à-dire au collaborateur intentionnellement fautif. Les violations de

la protection des données peuvent également avoir des conséquences disciplinaires internes à l'entreprise.

22.4 […]

23. Signalement des infractions et coopération avec les autorités de surveillance

23.1 Les collaborateurs doivent immédiatement faire rapport à leur supérieur hiérarchique ou au responsable de la protection des données s'ils ont connaissance d'une violation de la présente politique de protection des données ou de dispositions légales relatives à la protection des données à caractère personnel.

23.2 Les violations de la *sécurité* des données (p. ex. divulgation à des personnes non autorisées, perte de données, cyberattaque, etc.) qui font courir aux personnes concernées un risque élevé pour leur personnalité ou leurs droits fondamentaux doivent être signalées par l'entreprise au PFPDT «dans les meilleurs délais», c'est-à-dire rapidement.

23.3 […]

VII. Autres dispositions

24. Publication

24.1 La présente politique d'entreprise doit être mise à la disposition de tous les collaborateurs de l'entreprise par des moyens appropriés, [notamment via l'Intranet].

24.2 Il n'est pas prévu de publication générale de la présente directive de protection des données.

25. Modifications

25.1 L'entreprise se réserve le droit de modifier la présente directive de protection des données si nécessaire. Une modification peut notamment s'avérer nécessaire pour répondre à des exigences légales, à des demandes des autorités de surveillance ou à des procédures internes à l'entreprise.

25.2 Il convient également d'examiner à intervalles réguliers dans quelle mesure des changements technologiques rendent nécessaire une adaptation de la présente directive d'entreprise.

26. […]