Directive sur la protection des données

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 la Fédération romande des écoles de conduite.

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.

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).

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.

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.

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 défaut 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.

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.

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.

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 préposé fédéral à la protection des données et à la transparence (PFPDT) «dans les meilleurs délais», c'est-à-dire rapidement.

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.

Richtlinie zum Datenschutz

Allgemeines

1. Einführung

1.1. Die im Unternehmen verfügbaren Daten sind für das Unternehmen von großem Wert. Diese Daten müssen daher vor unberechtigtem Zugriff und anderen Bedrohungen geschützt werden.

1.2 Die Kunden, Partner und Mitarbeiter des Unternehmens erwarten, dass die dem Unternehmen anvertrauten Daten besonders geschützt werden und dass mit ihnen sorgfältig umgegangen wird.

1.3 Wenn Sie Fragen zum Datenschutz oder zur Verarbeitung Ihrer persönlichen Daten haben, können Sie sich an die Fédération romande des écoles de conduite wenden.

2. Ziel der Datenschutzrichtlinie

2.1 Die vorliegende Datenschutzrichtlinie soll einheitliche Standards für den Datenschutz im Unternehmen schaffen.

2.2 Durch die Einhaltung der in dieser Datenschutzrichtlinie festgelegten Standards erfüllt das Unternehmen seine datenschutzrechtlichen Verpflichtungen und stellt sicher, dass die Interessen und Rechte der betroffenen Personen ausreichend berücksichtigt werden.

2.3 Die Einhaltung dieser Datenschutzrichtlinie ist eine Voraussetzung für den sicheren Austausch von personenbezogenen Daten innerhalb des Unternehmens und mit Dritten.

3. Anwendungsbereich der Datenschutzrichtlinie

3.1 Diese Datenschutzrichtlinie gilt für jede Verarbeitung personenbezogener Daten, einschließlich insbesondere des Sammelns, Speicherns, Aufbewahrens, Verwendens, Änderns, Weitergebens, Archivierens, Löschens oder Vernichtens von Daten. Sie gilt für alle Arten von personenbezogenen Daten, einschließlich der Daten von Mitarbeitern, Kunden, Lieferanten und anderen Geschäftspartnern.

3.2 Die Datenschutzrichtlinie beschreibt, konkretisiert oder ergänzt auch die gesetzlichen Bestimmungen, insbesondere die des Schweizerischen Datenschutzgesetzes (DSG).

4. Definitionen

4.1 **Personenbezogene Daten** im Sinne dieser Unternehmensrichtlinie sind alle Angaben, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

4.2 **Betroffene Personen** sind die natürlichen Personen, über die personenbezogene Daten verarbeitet werden.

4.3 **Der Verantwortliche** ist eine Privatperson, die allein oder gemeinsam mit anderen über den Zweck und die Mittel der Verarbeitung entscheidet.

4.4 **Der Auftragsverarbeiter** ist ein Dritter, der personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

Grundregeln der Datenverarbeitung

5. Rechtmäßigkeit

5.1 Persönliche Daten müssen rechtmäßig verarbeitet werden. Die Verarbeitung gilt nur dann als rechtmäßig, wenn sie durch (a) die Einwilligung der betroffenen Person, durch (b) ein überwiegendes privates oder öffentliches Interesse oder durch (c) ein Gesetz gerechtfertigt ist.

6. Transparenz

6.1 Die Verarbeitung von Daten muss grundsätzlich so erfolgen, dass die betroffene Person davon Kenntnis hat.

7. Grundsatz der Verhältnismäßigkeit

7.1 Bei der Verarbeitung von Daten muss der Grundsatz der Verhältnismäßigkeit beachtet werden. Gemäß diesem Grundsatz dürfen nur Daten erhoben werden, die für den verfolgten Zweck notwendig und angemessen sind.

7.2 Außerdem dürfen personenbezogene Daten nur so lange aufbewahrt werden, wie es für den jeweiligen Zweck (siehe unten) erforderlich ist.

8. Zweck

8.1 Persönliche Daten dürfen nur für einen bestimmten, von der betroffenen Person identifizierbaren Zweck erhoben und nur in einer mit diesem Zweck zu vereinbarenden Weise verarbeitet werden.

8.2 Wenn die personenbezogenen Daten für den Zweck der Verarbeitung nicht mehr notwendig sind, müssen sie vernichtet oder anonymisiert werden.

9. Richtigkeit

9.1 Alle Mitarbeiterinnen und Mitarbeiter müssen dafür sorgen, dass die persönlichen Daten korrekt sind und auf dem neuesten Stand gehalten werden.

9.2 Alle angemessenen Schritte müssen unternommen werden, um unrichtige oder unvollständige Daten zu berichtigen oder zu vernichten.

10. Sicherheit der Daten

10.1 Für das Unternehmen ist es sehr wichtig, dass die Datensicherheit jederzeit gewährleistet ist. In diesem Zusammenhang müssen personenbezogene Daten durch technische und organisatorische Maßnahmen geschützt werden, insbesondere vor Verlust, unberechtigtem Zugriff und anderen Gefahren.

10.2 Die konkreten Schutzmaßnahmen müssen für die einzelnen Datenverarbeitungsvorgänge dokumentiert und auf ihre Angemessenheit hin überprüft werden.

10.3 Die IT-Abteilung kann im Interesse der Datensicherheit strengere Richtlinien erlassen, insbesondere im Hinblick auf die Nutzung von IT-Systemen im Unternehmen.

11. Zustimmung und Widerspruch

11.1 Die Zustimmung der betroffenen Person zur Datenverarbeitung durch ein Unternehmen ist in der Regel nicht erforderlich, auch nicht bei sensiblen personenbezogenen Daten.

11.2 Widerspricht die betroffene Person hingegen ausdrücklich einer Datenverarbeitung, so ist diese nur dann gerechtfertigt, wenn überwiegende Interessen des Verantwortlichen oder eine gesetzliche Grundlage vorliegen.

12. Informationspflicht

12.1 Die betroffenen Personen müssen, soweit möglich, vorab über den Zweck informiert werden, für den ihre personenbezogenen Daten erhoben und verarbeitet werden. Wenn die Daten nicht direkt bei der betroffenen Person erhoben werden, wird diese innerhalb eines Monats nach Erhalt der Daten informiert.

12.2 Wenn die betroffene Person dem Verantwortlichen ihre personenbezogenen Daten von sich aus zugänglich macht, gilt sie als informiert.

12.3 Wenn sich der Zweck der Datenverarbeitung ändert, müssen die bereits informierten Personen erneut informiert werden.

13. Unterauftragsvergabe

13.1 Wenn Dienstleister des Unternehmens personenbezogene Daten im Auftrag des Unternehmens verarbeiten (sog. Auftragsverarbeiter), ist zu beachten, dass die gleichen Sorgfaltsanforderungen, die für das verantwortliche Unternehmen gelten, auch für den Auftragsverarbeiter gelten. Insbesondere müssen die Zweckbindung und die Datensicherheit vertraglich garantiert werden.

14. Übermittlung von personenbezogenen Daten ins Ausland :

14.1 Die Übermittlung von Personendaten ins Ausland ist nur in Staaten zulässig, in denen der Bundesrat ein gleich hohes Datenschutzniveau wie in der Schweiz festgestellt hat. Die Einhaltung der schweizerischen Datenschutzstandards kann zudem unter anderem durch den Abschluss zusätzlicher vertraglicher Vereinbarungen erreicht werden.

Interne Prozesse

15. Anforderungen an die Mitarbeiter

15.1 Alle Mitarbeiter des Unternehmens sind zur Einhaltung des Datenschutzes verpflichtet. Sie sind insbesondere darüber zu informieren, dass es verboten ist, Personendaten für private Zwecke zu verwenden, an Unbefugte weiterzugeben oder Unbefugten zugänglich zu machen. Die Verpflichtung zur Wahrung des Datenschutzes gilt über das Ende des Beschäftigungsverhältnisses hinaus.

15.2 Auch innerhalb des Unternehmens ist darauf zu achten, dass nur diejenigen Mitarbeiter Zugriff auf personenbezogene Daten haben, die diese benötigen, um ihre Aufgaben für das Unternehmen zu erfüllen.

15.3 Alle Mitarbeiter müssen bei ihrer Einstellung und danach regelmäßig in Datenschutzfragen geschult und sensibilisiert werden.

16. Register der Verarbeitungstätigkeiten

16.1 Das Unternehmen führt ein Verzeichnis der Verarbeitungstätigkeiten im Zusammenhang mit personenbezogenen Daten. Darin muss Folgendes festgehalten werden: die Identität des Verantwortlichen oder des Auftragsverarbeiters, der Zweck der Verarbeitung, eine Beschreibung der Kategorien der betroffenen Personen und der Kategorien der verarbeiteten personenbezogenen Daten, die Kategorien der Empfänger, die Aufbewahrungsdauer oder die Kriterien für ihre Festlegung, wenn möglich eine Beschreibung der Maßnahmen, die zur Gewährleistung der Datensicherheit ergriffen wurden, sowie die möglichen Zielländer, wenn die Daten ins Ausland gesendet werden. Das Register sollte immer auf dem neuesten Stand sein und einen Überblick über die Datenschutzaktivitäten im Unternehmen geben.

17. Datenschutz durch Technik, Datenschutz durch Voreinstellungen und Datenschutzanalyse Datenschutz-Folgenabschätzung

17.1 Die Systeme, die zur Bearbeitung von Personendaten eingesetzt werden, müssen von Anfang an so gestaltet sein, dass der Datenschutz eingehalten werden kann. Insbesondere müssen die technischen und organisatorischen Massnahmen dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angepasst werden (Privacy by Design).

17.2 Die Verantwortlichen müssen die Standardeinstellungen des Geräts oder der Software so wählen, dass die Verarbeitung personenbezogener Daten auf das für den jeweiligen Verwendungszweck erforderliche Minimum beschränkt wird, sofern die betroffene Person nichts anderes bestimmt. Dies betrifft z. B. die Annahme von Cookies auf der Website.

17.3 Eine Datenschutz-Folgenabschätzung (DSFA) muss durchgeführt und dokumentiert werden, insbesondere wenn eine geplante Datenverarbeitung ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen darstellt.

Rechte der Betroffenen

18. Recht auf Zugang

18.1 Auf Anfrage ist einer betroffenen Person mitzuteilen, ob sie betreffende personenbezogene Daten von dem Unternehmen verarbeitet werden. Ist dies der Fall, hat die betroffene Person das Recht, Auskunft über die betreffenden personenbezogenen Daten zu erhalten. Das Auskunftsrecht besteht darin, zu erfahren, ob personenbezogene Daten verarbeitet werden und wenn ja, welche, damit die betroffene Person ihre anderen Rechte geltend machen kann. Dazu gehören neben den personenbezogenen Daten, die als solche verarbeitet werden, auch Informationen über die Identität des Verantwortlichen, den Zweck der Verarbeitung, die Speicherdauer, die Herkunft der Daten und ggf. Informationen über automatisierte Einzelentscheidungen und die Empfänger (auch als Kategorien).

18.2 Bei der Erteilung von Auskünften ist sicherzustellen, dass die Identität der betroffenen Person überprüft wird. Außerdem ist darauf zu achten, dass im Rahmen der Auskunftserteilung keine

personenbezogenen Daten Dritter offengelegt werden. In der Regel muss die Auskunft kostenlos und innerhalb von 30 Tagen erteilt werden.

19. Datenübertragbarkeit / Recht auf Mitteilung und Übermittlung von Daten

19.1 Die betroffenen Personen können verlangen, die Daten, die sie einem Unternehmen übermittelt haben, in einem gängigen elektronischen Format abzurufen, wenn die Daten automatisiert verarbeitet werden und die betroffene Person ihre Einwilligung zur Verarbeitung gegeben hat oder die Verarbeitung im Rahmen eines entsprechenden Vertrags erfolgt.

20. Recht auf Berichtigung

20.1 Gemäss Art. 32 Abs. 1 DSG kann eine betroffene Person verlangen, dass unrichtige Personendaten berichtigt werden.

21. Recht auf Löschung von Daten

21.1 Wenn personenbezogene Daten entgegen der ausdrücklichen Willenserklärung der betroffenen Person verarbeitet werden und es weder eine gesetzliche Grundlage noch überwiegende private Interessen Dritter gibt, kann die betroffene Person die Löschung ihrer personenbezogenen Daten verlangen.

Kompetenz

22. Verantwortung

22.1 Die Verantwortung für die Einhaltung der Bestimmungen dieser Datenschutzrichtlinie liegt in erster Linie bei den Mitarbeitern, die mit der Verarbeitung von Daten betraut sind.

22.2 Alle Mitarbeiter des Unternehmens haben auf die Einhaltung dieser Datenschutzrichtlinie zu achten und damit zu hohen und einheitlichen Datenschutzstandards im gesamten Unternehmen beizutragen.

22.3 Bei Verstössen gegen datenschutzrechtliche Pflichten drohen den Zuwiderhandelnden strafrechtliche Konsequenzen (Busse bis CHF 250 000.-) und dem Unternehmen zivilrechtliche Konsequenzen (bis hin zu Schadenersatz) sowie Rufschädigung. Die strafrechtliche Verantwortung liegt in erster Linie bei der natürlichen Person, d. h. bei dem/der vorsätzlich fehlbaren Mitarbeiter/in. Datenschutzverletzungen können auch unternehmensinterne disziplinarische Konsequenzen nach sich ziehen.

23. Meldung von Verstößen und Zusammenarbeit mit den Aufsichtsbehörden

23.1 Die Mitarbeiter müssen ihrem Vorgesetzten oder dem Datenschutzbeauftragten unverzüglich Bericht erstatten, wenn sie Kenntnis von einem Verstoß gegen diese Datenschutzrichtlinie oder gegen gesetzliche Bestimmungen zum Schutz personenbezogener Daten erhalten.

23.2 *Datensicherheitsverletzungen* (z.B. Offenlegung gegenüber Unbefugten, Datenverlust, Cyberangriffe usw.), die für die betroffenen Personen ein hohes Risiko für ihre Persönlichkeit oder ihre Grundrechte bedeuten, muss das Unternehmen dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) "so rasch wie möglich", d.h. umgehend, melden.

Andere Bestimmungen

24. Veröffentlichung

24.1 Die vorliegende Unternehmenspolitik muss allen Mitarbeitern des Unternehmens auf geeignete Weise zugänglich gemacht werden (insbesondere über das Intranet).

24.2 Eine allgemeine Veröffentlichung dieser Datenschutzrichtlinie ist nicht vorgesehen.

25. Änderungen

25.1 Das Unternehmen behält sich das Recht vor, diese Datenschutzrichtlinie bei Bedarf zu ändern. Eine Änderung kann insbesondere erforderlich sein, um gesetzlichen Anforderungen, Anfragen von Aufsichtsbehörden oder unternehmensinternen Verfahren nachzukommen.

25.2 In regelmäßigen Abständen sollte auch geprüft werden, inwieweit technologische Veränderungen eine Anpassung dieser Unternehmensrichtlinie erforderlich machen.