FÉDÉRATION ROMANDE DES ÉCOLES DE CONDUITE
ROUTE DU VILLAGE 14 / CH - 1070 PUIDOUX
+ 41 (0)21 625 90 30 / INFO@FREC.CH / WWW.FREC.CH

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.