ETAT DE FRIBOURG
STAAT FREIBURG

Kantonale Behörde für Öffentlichkeit und Datenschutz
Chorherrengasse 2, 1700 Freiburg

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

Kantonale Datenschutzbeauftragte

Chorherrengasse 2, 1700 Freiburg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/odsb

—

Referenz:
E-Mail: secretariatatprd@fr.ch

Freiburg, 15. Oktober 2012

Datenschutz für gesetzliche Socialhilfe

Sehr geehrter Herr Y

Wir beziehen uns auf Ihr E-Mail vom xx.yy.zzzz in randvermerkter Sache, mit dem Sie sich an uns gewendet haben.

Es geht um die Frage, welche Vorschriften in den internen Verfahren von den Regionalen Sozialdiensten (RSD) im Hinblick auf den Datenschutz eingehalten werden müssen.

Nach einigen allgemeinen Informationen und Ausführungen über das Beschaffen von Daten finden Sie hier einige nicht abschliessende Angaben zur Bekanntgabe von Daten über die betroffenen Personen sowie Hinweise auf organisatorische und technische Sicherheitsmassnahmen.

1. Allgemeines

Personendaten bezüglich von den RSD betreuter Personen sind **besonders schützenswert** im Sinne von Artikel 3 Bst. c Ziff.3 DSchG[1]. Für sie gilt also eine besondere Sorgfaltspflicht (Art. 8 DSchG), unter Einhaltung der in den Artikeln 4 ff. DSchG aufgezählten Grundsätze, nämlich in erster Linie Gesetzmässigkeit, Zweckmässigkeit, Treu und Glauben, Verhältnismässigkeit.
Das öffentliche Organ, das Personendaten bearbeitet, muss die geeigneten organisatorischen und technischen **Massnahmen** treffen, um die Daten gegen jedes unerlaubte Bearbeiten zu schützen (Art. 22 Abs. 1 DSchG).

Es wird empfohlen, zu Beginn des Arbeitsverhältnisses eine **Vertraulichkeitsvereinbarung** unterzeichnen zu lassen. Am Ende des Arbeitsverhältnisses müsste die/der Angestellte mit einem Schreiben an ihre/seine Geheimhaltungspflicht erinnert werden, wie dies in anderen Behörden bereits üblich ist. Die Schweigepflicht ist in Artikel 28 SHG[2] verankert.

2. Beschaffen von Daten

Personendaten sind grundsätzlich bei der betroffenen Person zu erheben. Sie dürfen nur dann bei einem öffentlichen Organ oder einem Dritten eingeholt werden, wenn eine gesetzliche Bestimmung es vorsieht, die Natur der Aufgabe es erfordert oder wenn besondere Umstände es rechtfertigen (Art. 9 Abs. 1 DSchG). Dazu kann der RSD die betroffene Person eine Vollmacht unterzeichnen lassen (Art. 24 Abs. 4 SHG). In diesem Fall sind der Zweck und die gesetzliche Grundlage des Bearbeitens sowie die Empfänger der Daten anzugeben (Art. 9 Abs. 3 DSchG).

3. Bekanntgabe von Daten

a. Systematische Bekanntgabe

Werden Daten **systematisch** bekanntgegeben (beispielsweise Abgabe einer Personenliste), so muss diese Bekanntgabe auf einer Rechtsgrundlage beruhen (Art. 4 und 10 Abs. DSchG). Da Sozialhilfedaten besonders schützenswert sind, muss die Rechtsgrundlage in einem vom Gesetzgeber verabschiedeten Gesetz verankert sein (Art. 3 und 8 DSchG).

b. Bekanntgabe im Einzelfall

Personendaten dürfen bekanntgegeben werden, wenn im Einzelfall das öffentliche Organ, das die Daten anfordert, diese **für die Erfüllung seiner Aufgabe benötigt** (Art. 10 Abs. 1 Bst. a DSchG). Nach dem Verhältnismässigkeitsprinzip dürfen grundsätzlich nur anonymisierte Informationen weitergegeben werden (anhand derer die betroffenen Personen nicht identifizierbar sind).

Die Bekanntgabe kann im Einzelfall auch erfolgen, wenn die betroffene Person der Bekanntgabe zugestimmt hat (beispielsweise mit der Unterzeichnung einer Vollmacht) oder ihre Einwilligung nach den Umständen vorausgesetzt werden darf (Art. 10 Abs. 1 Bst. c DSchG). Grundsätzlich kann im Sozialhilfewesen das Einverständnis nicht vorausgesetzt werden. Die Person, die Sozialhilfe bezieht, soll nämlich nicht damit rechnen müssen, dass ihre Daten beispielsweise vom RSD an die Wohngemeinde weitergegeben werden und umgekehrt. Wichtig ist der Hinweis darauf, dass die betroffene Person ihre Einwilligung jederzeit zurücknehmen kann. Die Einwilligung ist ausserdem nur dann rechtsgültig, wenn sie frei und aufgeklärt erteilt wird, d.h. ohne Druck und in genauer Sachkenntnis. Sie muss auch für den konkreten Fall erteilt werden (mit Bestimmung der genauen Zwecke), ausdrücklich (was eine aktive mündliche oder schriftliche Antwort voraussetzt) und ohne Zweifel (es darf kein Zweifel an der Absicht der betroffenen Person bestehen, ihre Zustimmung zu erteilen). Ausserdem muss in der Vollmacht klar angegeben werden, welche Daten beschafft werden dürfen, welche Stellen die Daten übermitteln dürfen und wie lange diese – befristete - Vollmacht gültig ist. Nach dem Grundsatz von Treu und Glauben kann übrigens die Zustimmung nicht vom Erfordernis einer genügenden Rechtsgrundlage abgekoppelt werden, weder für die Beschaffung noch für die Bekanntgabe sensibler Daten.

c. Sonderfall

Was die **Zustellung der Dossiers vom Sozialdienst an die Mitglieder der Sozialkommission an ihre Privatadresse** betrifft, so gibt es dafür zunächst einmal keine gesetzliche Grundlage. Ausserdem ist die Weitergabe der Dossiers für die Erfüllung der Aufgabe durch das öffentliche Organ nicht notwendig, denn die Kommissionsmitglieder können die Dossiers vor oder

während der Kommissionssitzung vor Ort einsehen. Eine solche Bekanntgabe wäre auch kaum vereinbar mit dem Verhältnismässigkeitsprinzip. Für die Zustellung per Post und die Aufbewahrung dieser Daten bei den Kommissionsmitgliedern zuhause müssen für solche sensiblen Daten geeignete technische Sicherheitsmassnahmen ergriffen werden. Darauf kann auch nicht mit dem Hinweis darauf verzichtet werden, die Kommissionsmitglieder seien an das Amtsgeheimnis gebunden.

4. Informatik-Sicherheitsmassnahmen

Sensible Daten und vertrauliche Informationen dürfen grundsätzlich nicht **per E-Mail versendet werden**. Sie sollten per Post oder persönlich zugestellt werden. Erfolgt der Versand dennoch per Mail, so sind verschiedene Vorkehrungen zu treffen, um die Vertraulichkeit zu gewährleisten. Das Merkblatt Nr.4 der ÖDSB über die Bekanntgabe von Daten per E-Mail[3] gibt dazu folgende Hinweise:
-Bei Bekanntgabe nur über das kantonale Netz (**Intranet**):
Die übermittelten Dokumente müssen verschlüsselt werden. Mit der Verschlüsselung kann eine E-Mail von niemandem gelesen werden, der den Geheimcode für die Verschlüsselung nicht kennt (statt der Verschlüsselung der Nachricht könnte auch das angehängte Dokument passwortgeschützt werden).
-Bei Bekanntgabe über das öffentlich zugängliche Netz (**Internet**)
1. Die übermittelten Dokumente müssen verschlüsselt werden.
2. Die Integrität der Nachricht müsste überprüft werden, das heisst es müsste garantiert werden, dass die Information auf ihrem Weg im Netz nicht versehentlich oder vorsätzlich verfälscht worden ist.
3. Und schliesslich müssten die Authentifizierungsmechanismen garantieren, dass
der Absender wirklich der ist, der er vorgibt zu sein.
Für den Zugriff auf besonders schützenswerte Personendaten kann nur die betroffene Person einer dritten Person die Genehmigung erteilen, in die übermittelten Daten Einsicht zu nehmen. Für die Zugriffsgenehmigung sind mindestens anzugeben: der Zweck, für den die Daten bekanntgegeben werden, die Bezeichnung der Daten, auf die sich die Genehmigung bezieht, die Person, der Einsicht gewährt wird, und die für die Bearbeitung verantwortliche Person.

Auch weitere Informatik-Massnahmen werden empfohlen, beispielsweise:
Mit der Einrichtung eines **Protokollierungsverfahrens** (Nachverfolgbarkeit der Datenzugriffe) kann nachträglich überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden (Art. 2 Abs. 1 Bst. b und 18 DSchG).

Die Computer und Drucker sollten möglichst **an Orten aufgestellt** werden, an denen nur befugte Personen Zugang dazu haben, beispielsweise in für die Öffentlichkeit nicht zugänglichen, geschlossenen Büros. Für vorübergehende Abwesenheiten vom Arbeitsplatz muss eine automatische Bildschirmsperre aktiviert sein.

Die Daten müssen mit Sicherungskopien und Antivirusprogrammen vor allfälligem **Datenverlust** geschützt werden.

Die **Internetanbindung** muss streng von den sensiblen Daten getrennt sein, weil die Gefahr besteht, dass Dritte über das Internet in das System eindringen.

Die verwendeten Systeme müssen den Standardanforderungen der **Informatiksicherheit** genügen (Art. 14 Abs. 1 DSR[4]). So muss insbesondere nach Artikel 17 Abs. 1 DSR der Zugriff auf Informatiksysteme, mit denen Personendaten bearbeitet werden können, durch ein Authentifikationsverfahren (Identifikation + Passwort) und ein Zugriffskontrollsystem geschützt werden.

5. Physische Sicherheitsmassnahmen

Was die **Aufbewahrung der Unterlagen** betrifft, so ist es nach den Informationen des Kantonalen Sozialamts an die RSD ausgeschlossen, dass die vom RSD angelegten Dossiers seine Büros verlassen. Ganz generell müssen die Unterlagen in einem dazu vorgesehenen Raum aufbewahrt werden. Sie müssen unter Verschluss gehalten werden und vor Beschädigung geschützt sein (Wasser, Feuer, Licht usw.). Die Sitzungsprotokolle müssen bei der Gemeinderätin, die Mitglied der regionalen Sozialkommission ist, zuhause oder in einem abgeschlossenen Aktenschrank in den Gemeinderäumlichkeiten ohne Zugangsmöglichkeit für Dritte aufbewahrt werden. Unterlagen, die nicht archiviert werden, müssen vernichtet werden, sobald das öffentliche Organ sie nicht mehr benötigt (Art. 13 DSchG).

Es werden auch noch weitere physische Massnahmen empfohlen. Insbesondere müssen die **Räumlichkeiten** so eingerichtet sein, dass Diskretion gewährleistet ist. Für die **Vernichtung von Unterlagen** empfiehlt sich ein Aktenvernichter; sie dürfen nicht einfach in den Papierkorb geworfen werden. Beim elektronischen Papierkorb reicht die *Delete*-Funktion nicht, denn damit lässt sich eine Wiederherstellung gelöschter Daten nicht ausschliessen. Das betreffende Dokument sollte vielmehr gelöscht und überschrieben werden und das elektronische Speichermedium mit den Personendaten endgültig vernichtet werden.

Bemerkung: Falls Sie weitere Auskünfte wünschen, informieren wir Sie gerne über das Auskunftsrecht über Personendaten, die Bekanntgabe dieser Daten, die durchzuführenden Kontrollen, die Datenbearbeitung im Auftrag (Outsourcing) oder auch über die Websites mit Zugriffskontrolle.

Wir hoffen, Ihnen damit Ihre Fragen beantwortet zu haben.

Freundliche Grüsse

Dominique Nouveau Stoffel
Kantonale Datenschutzbeauftragte