Datenschutz im Umgang mit Daten von Begünstigten

Merkblatt für Freiwillige

Die nachfolgende Richtlinie gilt für Freiwillige im Umgang mit Personendaten und privaten Informationen von Begünstigten des SRK Kanton Bern.

Generell

Wir behandeln Personendaten[1] sowie private Informationen vertraulich und geben sie nur mit einer Einwilligung oder im Interesse der Begünstigten weiter. Die Weitergabe von Gesundheitsdaten und anderen besonders schützenswerten Personendaten müssen von den betroffenen Personen immer eingewilligt werden.

Informationen zu einem Einsatz verwenden wir ausschliesslich für den Einsatz. Nach Einsatz-Ende werden alle Informationen (inkl. E-Mails) gelöscht.

Daten speichern

Speicherdauer und -ort

Physische Dokumente
Vertrauliche physische Dokumente oder Unterlagen, die besonders schützenswerte Personendaten enthalten, (z.B. Lebenslauf) werden sicher aufbewahrt und nach Einsatzende entweder zurückgeben oder physisch vernichtet.

Elektronische Dokumente
Elektronische Dokumente, E-Mails oder Anhänge von E-Mails speichern wir nur vorübergehend in der Datenablage auf dem privaten Gerät. Nach dem Einsatz vernichten wir diese endgültig.

Die Verwendung von Online-Datenablagen, wie bspw. Dropbox oder WeTransfer ist aufgrund der mangelnden Datensicherheit nicht zulässig.

[1] Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen; Besonders schützenswerte Personendaten sind Daten über: Religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; Gesundheit, Intimsphäre, Zugehörigkeit zu einer Rasse oder Ethnie; Verwaltungs- und strafrechtliche Verfolgung oder Sanktionen; Massnahmen der sozialen Hilfe; Genetische Daten; Biometrische Daten, die eine natürliche Person eindeutig identifizieren.

E-Mail-Kommunikation

Benutzerkonto
Im Rahmen der Tätigkeit für das SRK Kanton Bern verwenden wir ausschliesslich E-Mail-Accounts, auf die niemand ausser wir selbst Zugriff haben.

Versand von Personendaten oder Zugangsdaten
Unverschlüsselte E-Mails können von Dritten mitgelesen oder verändert werden. Daher versenden wir grundsätzlich keine Personendaten und nie Angaben über Passwörter oder andere Zugangsdaten per E-Mail.

Bei der Kommunikation mit den Freiwilligenkoordinatorinnen, Freiwilligenkoordinatoren bzw. den Dienstleistungsverantwortlichen verwenden wir nur die Initialen der Begünstigten.

Bei der Kommunikation mit Dritten versenden wir grundsätzlich keine E-Mails mit Personendaten von Begünstigten. Alternativ unterstützen und befähigen wir die Begünstigten beim Verfassen von E-Mails.

Dokumente mitschicken
Falls in Ausnahmefällen doch Dokumente mit Personendaten von Begünstigten via E-Mail verschickt werden, müssen die Anhänge mit einem Passwort geschützt sein. Das Passwort muss zwingend auf einem anderen Kanal (z.B. Telefon, SMS) mitgeteilt werden.

E-Mail-Verschlüsselung
Wenn eine professionelle Verschlüsselungslösung für E-Mails vorhanden ist, wird diese für den Versand von Personendaten verwendet. Im Betreff der E-Mail dürfen keine Personendaten angegeben werden, weil der Betreff nicht verschlüsselt werden kann.

Messaging-Dienste

Die Datensicherheit ist bei der Verwendung von Messaging-Diensten wie WhatsApp nicht gewährleistet. Wir versenden daher nie sensible Daten (z.B. Informationen über Begünstigte) über Messaging-Dienste.

Wenn die betroffenen Personen die Nutzung von WhatsApp ausdrücklich wünschen, verwenden wir WhatsApp ausschliesslich bei fehlenden Alternativen (z.B. Signal oder Threema) und auch dann nur für niederschwellige Inhalte wie z.B. Terminabsprachen, in der Form von sogenannten «selbstlöschenden Nachrichten».

PC/Laptop (privates Gerät)

Wer für das SRK Kanton Bern mit einem Gerät arbeitet, das auch von anderen Personen genutzt wird (z.B. Familienlaptop), loggt sich nach getaner Arbeit aus dem E-Mail-Account aus. Es wird sichergestellt, dass niemand anderes auf die Daten Zugriff hat, die im Rahmen der Freiwilligentätigkeit bearbeitet werden. Wir schützen den PC/Laptop mit einem sicheren Passwort.

Um die Sicherheit des eigenen Geräts zu gewährleisten, halten wir Virenschutzprogramme (z. B. Windows Defender) aktuell und führen regelmässige Installation von Sicherheitsupdates des Betriebssystems usw. durch.