

10 wichtige Datenschutzregeln

für Ehrenamtliche und Freiwillige

Datenschutzgesetz (revDSG, in Kraft seit 1. September 2023).

1. Vertraulichkeit bewahren

Alle personenbezogenen und besonders schützenswerte* Daten (nachfolgend: "Daten"), die im Rahmen der Tätigkeit bekannt werden, sind vertraulich zu behandeln – auch nach Beendigung des Engagements.

Beispiel: Keine Gespräche über Klient:innen, Angebots-Teilnehmende etc. oder interne Abläufe in der Öffentlichkeit oder mit Dritten (z. B. Familie, Freunde).

2. Nur notwendige Daten bearbeiten

Bearbeite nur jene Daten, die du für deine Aufgabe wirklich brauchst („Datenminimierung“).

Beispiel: Wenn du nur für die Betreuung eines Projekts zuständig bist, brauchst du keine vollständigen Mitgliederlisten.

3. Daten nur für den vorgesehenen Zweck nutzen

Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden.

Beispiel: Eine E-Mail-Adresse, die für den Versand eines Newsletters erhoben wurde, darf nicht für Werbung oder private Zwecke verwendet werden.

4. Keine Daten weitergeben ohne Erlaubnis

Daten dürfen nicht an Dritte weitergegeben werden – ausser mit ausdrücklicher Zustimmung der betroffenen Person oder gemäss interner Weisung.

Beispiel: Niemals Daten von Klienten, Angebotsnutzenden, anderen Freiwilligen etc. an andere Organisationen, Medien oder Behörden weitergeben, ohne Rücksprache mit der vorgesetzten Stelle.

5. Sichere Aufbewahrung

Bewahre Unterlagen, Listen und elektronische Daten sicher auf – vor unbefugtem Zugriff, Verlust oder Diebstahl.

Beispiel: Dokumente mit Personendaten nicht auf privaten Geräten speichern, keine unverschlüsselten USB-Sticks verwenden.

6. Sichere Kommunikation

Verwende für die elektronische Kommunikation nur autorisierte Kanäle der Organisation.

Keine Daten über private E-Mail-Adressen oder Messenger (z. B. WhatsApp) versenden.

7. Korrekte Datenpflege

Achte darauf, dass Daten richtig und aktuell sind. Fehlerhafte oder veraltete Angaben sollten gemeldet oder korrigiert werden.

8. Löschpflicht beachten

Daten dürfen nur so lange aufbewahrt werden, wie sie für den Zweck nötig sind. Danach müssen sie sicher gelöscht oder vernichtet werden.

Beispiel: Teilnehmerlisten nach einem Event löschen, sobald die Nachbearbeitung abgeschlossen ist.

9. Meldepflicht bei Datenpannen (Data Breach)**

Wenn du merkst, dass Daten verloren gegangen, offengelegt oder falsch behandelt wurden, melde dies sofort der zuständigen Person oder Datenschutzverantwortlichen.

Beispiel: Ein verlorener USB-Stick oder eine fehlgeleitete E-Mail kann eine meldepflichtige Datenschutzverletzung sein.

10. Sensibilisierung und Rückfragen

Wenn du unsicher bist, frage nach, bevor du Daten bearbeitest oder weitergibst. Datenschutz ist Teamarbeit.

Beispiel: Lieber einmal zu viel nachfragen, als versehentlich gegen das Datenschutzgesetz zu verstossen.

*Zu besonders schützenswerten Daten werden Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, über Massnahmen der sozialen Hilfe; verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen und ab Inkrafttreten des revidierten Datenschutzgesetzes am 1. September 2023 auch genetische und biometrische Daten, die eine natürliche Person eindeutig identifizieren, subsumiert.

**Data Breach: Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn die Daten, für die Ihr Unternehmen/Ihre Organisation verantwortlich ist, von einem sicherheitsrelevanten Ereignis betroffen sind, das zu einer Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität führt.

Die Datenschutzerklärung des Blauen Kreuzes St. Gallen – Appenzell ist zu finden unter:
www.blaueskreuz-sg-app.ch/datenschutzerklaerung



Der Datenschutzverantwortliche des Blauen Kreuzes St. Gallen – Appenzell ist

Daniel Lieberherr, Geschäftsführer

daniel.lieberherr@blaueskreuz.ch

071 231 00 31