Inhalt

1. Geltungsbereich 1
2. Zutrittskontrolle 1
3. Zugangskontrolle 1
4. Zugriffskontrolle 2
5. Weitergabekontrolle 2
6. Eingabekontrolle 2
7. Auftragskontrolle 3
8. Verfügbarkeitskontrolle 3
9. Trennungskontrolle 3
10. Überprüfung, Bewertung und Evaluation 3

Informationssicherheit und Datenschutz

1. Geltungsbereich

Die nachfolgenden Kapitel beschreiben die durch Blutspende SRK Schweiz AG (nachfolgend B-CH) getroffenen technischen und organisatorischen Massnahmen der Informationssicherheit und des Datenschutzes in Bezug auf den Schutz von Personendaten. Sie gelten für die Fälle, in denen B-CH selbst als Verantwortliche die relevanten Daten verarbeitet. Findet die Datenbearbeitung durch von B-CH beauftragte Dritte statt, sorgt B-CH mittels geeigneter vertraglicher Vereinbarungen dafür, dass die Dritten vergleichbare Massnahmen einhalten.

2. Zutrittskontrolle

Mit Zutrittskontrolle sind alle Massnahmen gemeint, die den Zutritt von Unbefugten auf Areale, in Gebäude oder Räumlichkeiten, in denen Daten bearbeitet werden oder sich Systeme zur Datenbearbeitung befinden, verhindern.

Technische Massnahmen	Organisatorische Massnahmen
• Sicherung von Fenstern und Türen • Schliesssysteme mit Badge oder physischen Schlüsseln • Zugang zu Serverräumen mittels elektronischem Badge/ biometrischem Zugangsleser gesichert • Datenschutzkonforme Videoüberwachung im externen Serverraum	• Besucheranmeldung am Haupteingang (Klingel) und am Empfang • Begleitung von Besuchern und Besucherprotokolle • Sorgfältige Auswahl von Reinigungspersonal • Weisungen zur physischen und umgebungsbezogenen Sicherheit • Zonierung der Räumlichkeiten

3. Zugangskontrolle

Unter Zugangskontrolle wird die Verhinderung der unbefugten Benutzung von Ablagen und Systemen zur Datenbearbeitung verstanden. Systeme zur Datenbearbeitung (z.B. Applikationen) sind nur durch Personen mit entsprechender Nutzungsberechtigung zu bedienen.

Technische Massnahmen	Organisatorische Massnahmen

• Sichere VPN-Verbindungen für Administratoren und Mitarbeitende
• Verschlüsselung von Datenträgern und mobilen Endgeräten
• Sichere Firewall
• Anti-Viren-Software / Endpoint Detection and Response
• Authentifizierung mittels Benutzername und Passworteingabe
• 2-Faktor-Authentifizierung
• Automatische Desktopsperre
	• Schlüsselregelung
	• Umfassende Richtlinien, u.A.
	  • Passwortregeln inkl. Vorgaben zur Komplexität der Passwörter
	  • Richtlinie "Clean Desk"/ Bildschirmsperre
	  • Zugangsregelungen von extern/ intern
	• Vertrauenswürdiges Personal für die Bereiche Sicherheit und Reinigung
	• Generierung von Benutzerprofilen
	• Zuordnung von Benutzerrechten

4. Zugriffskontrolle

Mit Zugriffskontrolle sind alle Massnahmen gemeint, die die Einhaltung von Zugriffsberechtigungen gewährleisten sollen.

Technische Massnahmen	Organisatorische Massnahmen
• Protokollierung/ Log der Zugriffe auf Anwendungen und Prozesse wie z.B. Datenlöschung • Datenschutzkonforme Vernichtung von Datenträgern (z.B. Akten, Laufwerke) • Verschlüsselung von Datenträgern und mobilen Endgeräten • Identifizierungs- und Authentifizierungssystem • Sichere Aufbewahrung von Datenträgern und Dokumenten in geschützten Räumlichkeiten • Sichere Datenablage mit festgelegten Zugriffsrechten • Pseudonymisierung von Daten auf Testsystemen	• Berechtigungskonzepte • Benutzer- und Rollenkonzepte • Anpassung der Zahl der Administratoren mit vollen Zugriffsrechten • Datenvernichtung (Datenträger und Papierakten) durch zertifizierten Dienstleister

5. Weitergabekontrolle

Unter Weitergabekontrolle werden alle Massnahmen verstanden, welche die Sicherheit von personenbezogenen Daten während einer Datenweitergabe gewährleisten. Unter Datenweitergabe sind in diesem Sinne elektronische Übertragungen, Transport und Speicherung von personenbezogenen Daten zu verstehen.

Technische Massnahmen	Organisatorische Massnahmen
• Sichere VPN-Technologie • Transportverschlüsselung (SSL usw.) • E-Mail-Verschlüsselung im Austausch mit EMDI	• Pflege eines Verzeichnisses der Bearbeitungstätigkeiten • Periodische Kontrolle von Datenempfängern, Pflege der Empfänger im CRM • Einsatz vertrauenswürdiger externer Transportdienste • Qualifizierung von Transportdienstleistern, welche Zugang zu besonders schützenswerten Personendaten haben

6. Eingabekontrolle

Die Eingabekontrolle dient der nachträglichen Überprüfbarkeit der Datenbearbeitung; die Massnahmen sollen die Kontrolle von Dateneingaben, Datenveränderungen und Datenlöschungen gewährleisten.

Technische Massnahmen	Organisatorische Massnahmen
• Automatische Erstellung eines Protokolls/ Log über die Eingabe, Änderung und Löschung von Daten, soweit erforderlich und vom System unterstützt	• Einrichtung und Verwendung von individuellen Benutzernamen • Einrichtung und Verwendung von individuellen Administratoren-Benutzernamen • Vergabe von Zugriffsrechten

7. Auftragskontrolle

Die Auftragskontrolle kommt bei jeder Auftragsbearbeitung zum Zug. Sie dient der Gewährleistung, dass die Auftragsbearbeitung ausschliesslich nach den Weisungen des Auftraggebers erfolgt.

Technische Massnahmen	Organisatorische Massnahmen
• keine	• Sorgfältige Auswahl des Auftragnehmers • Schriftliche Weisungen an den Auftragnehmer • Abschluss von datenschutzkonformen Auftragsbearbeitungsverträgen • Vereinbarung von wirksamen Kontrollrechten beim Auftragnehmer • Regelmässige Bewertung des Auftragnehmers (Lieferantenbewertung)

8. Verfügbarkeitskontrolle

Bei der Verfügbarkeitskontrolle und Wiederherstellbarkeit müssen personenbezogene Daten vor Verlust oder Zerstörung so geschützt werden, dass sie im Falle einer Störung wiederhergestellt werden können.

Technische Massnahmen	Organisatorische Massnahmen
• Datensicherungen • Virenschutz • Firewall • Redundante Server • Klimatisierung von Serverräumen • Temperaturüberwachung Serverräume und Server • USV (unterbruchfreie Stromversorgung) • Notstrom-Generator • Rauch- und Feuermelder • Löscheinrichtungen • Datenschutzkonzept • IT-Notfallmanagement • Krisenmanagement	• geeignete Platzierung von Serverräumen (Schutz vor Risiken, z.B. Hochwasser, Brand) • Regelungen zu Datensicherungen • Tests für Daten-Wiederherstellungen

9. Trennungskontrolle

Werden personenbezogene Daten zu unterschiedlichen Zwecken erhoben, muss sichergestellt werden, dass sie auch getrennt bearbeitet werden (sog. Trennungsgebot).

Technische Massnahmen	Organisatorische Massnahmen
• Trennung von Produktiv- und Testumgebung • Klare Trennung der für unterschiedliche Zwecke gespeicherten Daten • Mandantentrennung auf Servern/ Systemen	• Mandantentrennung • an Datensätze angepasste Datenbankrechte und Berechtigungskonzepte • Steuerung der Trennungskontrolle via Berechtigungskonzept

10. Überprüfung, Bewertung und Evaluation

Massnahmen der Überprüfung, Bewertung und Evaluation stellen sicher, dass die festgelegten Schutzmassnahmen implementiert sind und eingehalten werden.

Technische Massnahmen	Organisatorische Massnahmen
• Regelmässige Penetration-Tests und ISDS-Audits durch das BAG • Systemüberwachung	• Änderungsmanagement • Risikomanagement • Helpdesk und Supportdienstleistungen der IT/ Meldesystem • Lieferantenmanagement