Auszug aus dem Datenschutzkonzept

[…]

Verantwortlichkeiten

Vertreter des Unternehmens:

- Erich Krebs, Geschäftsführer
- Torben Krebs, Geschäftsführer

Betriebliche(r) Datenschutzbeauftragte(r):

- Annika Huesmann

[…]

Bestehende technische und organisatorische Maßnahmen (TOM)

Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Sicherheitsschlösser
- Türen mit Knauf Außenseite
- Videoüberwachung
- Schlüsselregelung/Liste
- Empfang/Rezeption/Pförtner
- Sorgfalt bei der Auswahl der Reinigungsdienste

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

- Login mit Benutzername + Passwort
- Anti-Viren-Software Server
- Anti-Virus Software Clients
- Firewall
- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung Smartphones
- Verschlüsselung Notebooks/Tablet
- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortvergabe
- Allgemeine Richtlinie Datenschutz u./o. Sicherheit

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Aktenschredder
- Minimale Anzahl von Administratoren
- Verwaltung Benutzerrechte durch Administratoren

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Physikalische Trennung (Systeme/Datenbanken/Datenträger)
- Festlegung von Datenbankrechten

Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Einsatz von VPN
- Protokollierung der Zugriffe und Abrufe
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- Klare Zuständigkeit für Löschungen

Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher im Serverraum
- RAID System/Festplattenspiegelung
- Kontrolle des Sicherungsvorgangs
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz Management

- Dokumentiertes Sicherheitskonzept
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird min. jährlich durchgeführt
- Interner Datenschutzbeauftragter: Annika Huesmann; E-Mail: a.huesmann@briefdienst-krebs.de
- Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)
- Die Datenschutz-Folgeabschätzung (DSFA) wird bei Bedarf durchgeführt

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/ Daten-Pannen
- Einbindung vom DSB in Sicherheitsvorfälle und Datenpannen

Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

- Es werde nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln