Technisch-organisatorische Maßnahmen der CCV GmbH

1. Vertraulichkeit (Art. 32 Abs. 1 lt. b DS-GVO)

Zutrittskontrolle

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

- Elektronisches Schließsystem (Chipkarten)
- Schlüsselregelung
- Alarmanlage
- Besucherregelung mit Protokollierung
- Tragepflicht von Berechtigungsausweisen
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Zuordnung von Benutzerrechten
- Verwendung von sicheren Kennwörtern mit Ablaufzeit
- Erzwingen von automatischen Sperrmechanismen und Komplexitätsanforderungen
- Sperren von externen Schnittstellen (USB usw.)
- Einsatz von Anti-Viren-Software
- Einsatz von VPN-Technologie

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.

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern

Trennungskontrolle

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

- Berechtigungskonzept
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

Pseudonymisierung und Verschlüsselung

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) Wird nach gesetzlichen Vorgaben oder auf Verlangen Betroffener oder Auftraggeber durchgeführt und protokolliert. Verschlüsselung wird bei mobilen Datenträgern eingesetzt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

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, und das überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Ausschließlich verschlüsselte Datenübertragungswege werden verwendet
- Ausschließlich verschlüsselte Datenträger werden verwendet
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung

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.

- Eingaben erfolgen teilweise automatisiert, eine manuelle Bearbeitung der Daten ist dann nicht vorgesehen
- Einsatz von Protokollierungsmechanismen wie Dokumentenmanagement- und Ticketsystem
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

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

- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Klimaanlage in Serverräumen
- Automatische Löschanlage in Serverräumen
- Vorhandenes Backup- und Recoverykonzept
- Notfallplan
- Serverraum nicht unter sanitären Anlagen

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c)

Maßnahmen, die gewährleisten, dass nach einer Unterbrechung schnellstmöglich der Datenzugriff wiederhergestellt wird.

- Vorhandenes Backup- und Recoverykonzept
- Cold Standby Systeme
- Schattenkopien

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Maßnahmen, die gewährleisten, dass Anforderungen der DS-GVO nachprüfbar umgesetzt werden.

- Regelmäßige Datenschutz Audits
- Interne Revision
- Jährliche Mitarbeiter Datenschutz Schulungen

Incident-Response-Management

Maßnahmen, die gewährleisten, dass nach einer Störung der Auftraggeber eine Information über die Störung erhält, sofern seine Daten betroffen sind.

- Bereitstellung von Infos über ContactCenter

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Maßnahmen, die gewährleisten, dass nach einer zeitlichen Vorgabe personenbezogene Daten gelöscht werden.

- Manuelle Softwareunterstützung
- Manuelle Löschung nach gesetzlicher Vorgabe
- Manuelle Löschung auf Anforderung

Auftragskontrolle

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

- Daten werden nicht ohne konkreten Auftrag verarbeitet
- Schriftliche Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Sorgfältige Auswahl von Unterauftragnehmern
- Vereinbarungen zur Auftragsverarbeitung mit den Unterauftragnehmern geschlossen