Technische und organisatorische Maßnahmen

Bei CP Corporate Planning GmbH sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i. S. d. Art 32 DSGVO getroffen worden

In der hier vorliegenden Beschreibung über den aktuellen Stand der grundlegenden Maßnahmen zum Schutz der Daten wird einschränkend darauf hingewiesen, dass nicht alle Sicherheitsmaßnahmen im Detail offengelegt werden können. Gerade in Bezug auf Datenschutz und Datensicherheit ist der Verzicht auf vertrauliche und detaillierte Beschreibungen unabdingbar, da der Schutz der Sicherheitsmaßnahmen gegen unbefugte Offenlegung mindestens genauso wichtig ist wie die Sicherheitsmaßnahmen selbst.

Die aufgeführten technischen und organisatorischen Maßnahmen werden regelmäßig in geeigneter Form kontrolliert, um zu gewährleisten, dass die Verarbeitung im Verantwortungsbereich im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der Betroffenen in angemessener Form gewahrt ist. Siehe hierzu auch die Ziffer 4 in diesem Dokument.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Zentraler Empfangsbereich
- Zutrittsberechtigungskonzept
- Schließsystem mit Schlüsselkarten
- Zutrittskontrollsystem im Schließsystem integriert
- Räumlichkeiten sind stets verschlossen
- Zentrale Verwaltung zur Ausgabe von Schlüsselkarten.
- Zentrale Datenhaltung im Rechenzentrum Kaiserslautern
- Serverräume vor Ort stets verschlossen
- Zutritt zu Serverräumen nur für berechtigte Mitarbeiter
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.

- Detaillierte Benutzerprofile
- Zentrale Änderungen von Benutzerprofilen und Zugangsberechtigungen durch IT Verantwortliche
- Authentifikation mit Benutzername und Kennwort
- Passwortregelungen
    - Verwendung von individuellen Passwörtern
    - Passwörter mit einer Mindestlänge
    - Anzahl von aufeinanderfolgenden Fehlanmeldungen ist begrenzt
    - Passworthistorie
    - Regelmäßiger technisch erzwungener Passwortwechsel
- Interne Netze durch Firewall geschützt
- Externe Zugriffe auf interne Netze über verschlüsselte Verbindungen (z. B. VPN)
- Antivirenschutz auf allen Arbeitsplätzen
- Getrenntes WLAN für Gäste
    - Zentraler und separater Internet Zugang über Weilerbach, der durch VLAN und Multi-SSID gekapselt ist.
    - Mittels WLAN-Controller werden alle APs weltweit verwaltet.
    - Auf das Gäste-WLAN kann nur mittels Passwort und WPA2 zugegriffen werden.
    - Der Passwortwechsel erfolgt wöchentlich.
    - Jeder WLAN-Nutzer muss sich den internen Nutzungsbedingungen unterwerfen.

Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

- Detailliertes Berechtigungskonzepts
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (i.d.R. Möglichkeit mit Zertifikat)
- Einsatz von VPN-Technologie
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Einsatz von Antiviren-Software
- Nicht mehr benötigte IT-gestützte Datenträger werden datenschutzgerecht entsorgt.
- Unterlagen und Akten können über Aktenvernichter oder einen Dienstleister entsorgt werden.

Trennungsgebot

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Die Anwendungen erlauben eine logische Datentrennung.
- Eine Mandantentrennung ist über ein Berechtigungskonzept implementiert.
- Im Unternehmen wird zwischen Produktiv- und Testsystemen unterschieden.
- Daten unterschiedlicher Projekte oder Auftraggeber werden, soweit möglich, getrennt verarbeitet.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Nicht relevant für CP Corporate Planning GmbH (CP), weil durch CP direkt keine personenbezogenen Daten im Auftrag verarbeitet werden (siehe auch §1.3 Rahmenvereinbarung und den folgenden Hinweis).

Hinweis: *Die Software von CP arbeitet nicht direkt auf den Datenbanken der Vorsysteme eines Auftraggebers (z.B. FiBu, CRM, etc.).*

Die Datenhaltung von Projekten mit der CP Software erfolgt technisch unabhängig von den Daten eines Vorsystems in eigenständigen CP-spezifischen Datenbanken in der IT Infrastruktur eines Auftraggebers. Die Daten des Auftraggebers werden zum Austausch mit der CP Software über definierte Schnittstellen importiert und exportiert.

CP verarbeitet direkt keine Daten des Auftraggebers und ändert sie auch nicht. Die CP Software enthält kein Datenschema, das die Eingabe und Verarbeitung von personenbezogenen Daten voraussetzt. Die durch den Auftraggeber verarbeiteten Daten kennt CP nicht und hat auch keinen Einfluss auf diese.

Der Auftraggeber ist somit frei darin, welche Daten er in der CP Software verarbeitet und wie er sie abbildet. Der Auftraggeber kann jederzeit beliebige Daten in der Software verarbeiten oder nutzen. Eingabekontrollen müssen deshalb ggf. projektspezifisch definiert werden.

Die CP Software ist in der IT Infrastruktur eines Auftraggebers installiert und wird von diesem eigenständig betrieben und genutzt.

CP kann dabei durch Bereitstellung von IT Infrastruktur, z. B. Cloudhosting, Training & Consulting oder Wartung & Support inklusive Fernwartung nach Maßgabe des Auftraggebers unterstützen.

Sämtliche Dienstleistungen müssen durch den Auftraggeber beauftragt werden. Der Auftragnehmer führt selbständig keine Tätigkeiten für den Auftraggeber durch.

Weitergabekontrolle

Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.

- Im Unternehmen stehen Verfahren zur Verfügung, die einen verschlüsselten Austausch personenbezogener Daten ermöglichen wie E-Mail Verschlüsselung, SFTP, https, verschlüsselte Filesharing Plattform.
- Einsatz von verschlüsselten VPN-Verbindungen
- Aktenvernichter für die sichere Vernichtung von Papierdokumenten
- Homeoffice: Richtlinien zur rechtskonformen Ausgestaltung vorhanden, einschließlich Einsatz von VPN-Verbindungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

- Rechenzentrum in Kaiserslautern
  - ISO 27001 zertifiziert
  - TÜV zertifiziert
- redundante Klimaanlage
- redundante Stromversorgung
- redundanter RZ Bereich
- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung von Datensicherungen an einem sicheren ausgelagerten Ort
- Virenscanner sind unternehmensweit auf den Arbeitsplätzen installiert
- Virenscanner aktualisieren sich automatisch.
- Betriebssysteme auf Arbeitsplätzen werden regelmäßig aktualisiert.
- Betriebssysteme auf Servern werden regelmäßig aktualisiert.
- Firewall- und Router Systeme werden regelmäßig aktualisiert.
- unterbrechungsfreie Stromversorgung (USV) in Serverräumen vor Ort

4. Regelmäßige Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.

Datenschutzmanagement

- Ein Datenschutzbeauftragter ist für die Unternehmengruppe bestellt. Dieser wird in den Unternehmen vor Ort durch Datenschutzkoordinatoren unterstüzt.
- Unternehmensrichtlinien (Code of Conduct) sind vorhanden
- Meldung neuer/veränderte Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Datenschutz Konzept vorhanden
- Mitarbeiter sind mit dem Arbeitsvertrag zur Verschwiegenheit und zur Geheimhaltung verpflichtet.

Auftragskontrolle

- Mit externen Dienstleistern, die personenbezogenen Daten verarbeiten oder im Rahmen ihrer Tätigkeit einsehen können, werden vertragliche Regelungen gemäß den gesetzlichen Vorgaben (Art. 28 DSGVO) vereinbart.
- Die Auswahl von externen Dienstleistern erfolgt unter Anwendung größter Sorgfalt insbesondere bezüglich des Datenschutzes und der Informationssicherheit.
- Beim Einsatz externer Dienstleister, die personenbezogene Daten verarbeiten, wird sichergestellt, dass eine Rechtsgrundlage für die Verarbeitung gegeben ist wie Auftragsverarbeitung, EU-Standardvertragsklauseln.
- Es sind Verfahren implementiert, die sicherstellen, dass personenbezogene Daten nach Auftragsende gelöscht oder vernichtet werden
- Gesetzliche Aufbewahrungsfristen werden dabei berücksichtigt und eingehalten.
- In vertraglichen Regelungen mit Dienstleistern werden Kontrollrechte vereinbart.
- Externe Dienstleister werden zur Verschwiegenheit verpflichtet.