Technische und organisatorische Maßnahmen zur Datensicherheit

Dieses Dokument ist Teil der Datenschutzdokumentation der Firma CareSocial GmbH, Königsbrücker Straße 96, 01099 Dresden und dient zur Veranschaulichung der Umsetzung der gesetzlichen Forderungen auf den Datenschutz.

Es gilt für alle Mitarbeiter bzw. informationsverarbeitende Systeme und Netzwerke und Dokumente mit denen gearbeitet wird, um personen- und geschäftsbezogene Daten zu erheben, zu speichern und zu verarbeiten.

Das Dokument ersetzt alle früheren Versionen, gesetzliche oder vertragliche Festlegungen haben jedoch Vorrang und sind die alleinige Grundlage für Rechte und Pflichten der Parteien. Aus diesem Dokument lassen sich demnach keine Ansprüche ableiten.

Um ein angemessenes Schutzniveau zu gewährleisten und Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, Dienste und Daten bei der Verarbeitung sicherzustellen, wurden nach Beurteilung der bestehenden Risiken geeignete technische und organisatorische Maßnahmen ergriffen. Das schließt folgende Schritte mit ein:

Die Beratung zur Umsetzung der EU-DSGVO und des BDSG hat stattgefunden. Sie erfolgte durch

den internen Datenschutzbeauftragten Herrn Guido Borchert in enger Zusammenarbeit mit Herrn Rechtsanwalt Sven Hörnich, Fachanwalt für Urheber- und Medienrecht sowie für Gewerblichen Rechtsschutz.

Mitarbeiter verarbeiten Daten nur auf Anweisung des Verantwortlichen und werden dazu bei Einstellung zum Thema Datenschutz belehrt und regelmäßig geschult.

Die Verarbeitungstätigkeiten sind in einem Verzeichnis dokumentiert und werden regelmäßig aktualisiert. Darin ist die Zulässigkeit und Zweckbindung der Erhebung und Verarbeitung der Daten aufgeführt und wird für Betroffene, Verantwortliche und Kontrollinstanzen transparent gemacht, sodass die Rechte der Betroffenen auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden können.

Die Aktualisierung dieses Dokuments, also die Überprüfung, Bewertung und Weiterentwicklung der Wirksamkeit der technischen und organisatorischen Maßnahmen, ist in der Verantwortung von Herrn Guido Borchert.

Im Folgenden werden die passend zum Datensicherheitsrisiko ausgewählten technischen und organisatorischen Maßnahmen aufgeführt. Die Kontrolle des Zutritts zu Orten von Datenverarbeitung, Kontrolle des Zugangs zu IT-Systemen, des Zugriffs auf Daten(-träger), der Übermittlung oder Weitergabe von Daten, der Eingabe bzw. Plausibilität der Datenverarbeitung, der Kontrolle von Auftragsdatenverarbeitern, der Verfügbarkeit von Daten und der Trennung derselben und regelmäßige allgemeine Prüfung der Betriebsorganisation bieten das angemessene Schutzniveau und sind somit die legitimierende Grundlage der Datenverarbeitung der CareSocial GmbH.

I. Zutrittskontrolle

1. Für die lokale Zutrittskontrolle ist die Geschäftsleitung zuständig und legt zu sichernde Bereiche fest. Diese bestimmt auch Verfahren für die Vergabe und den Entzug der Zutrittsrechte. Letztere werden dokumentiert.

2. Im Sicherheitsbereich werden zudem Anwesenheitsaufzeichnungen geführt.

3. Personen, die nicht bei der CareSocial GmbH angestellt sind, verfügen über keine Zutrittsberechtigungen.

4. Physischer Zutritt:

   a) Die Zutrittskontrolle wird durch folgende technische und organisatorische Maßnahmen (TOMs) unterstützt: Alarmanlage, Videoüberwachung, Pfortendienst, Sicherheitsdienst, elektronisches Protokoll

   b) Eingangstüren und Nebentüren sind gesichert, so dass ein Schutz vor unbemerktem Betreten/Verlassen der Gebäude besteht.

   c) Besucher werden kalendarisch erfasst.

   d) Besucher werden abgeholt bzw. begleitet.

   e) Fenster und nach außen gehende Türen werden verschlossen, wenn die Räume, in denen die CareSocial GmbH Daten des Auftraggebers verarbeitet, nicht besetzt sind.

   f) Einstiegsgefährdete Fenster und Türen in Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, sind gegen Einbruch abgesichert.

5. Server

   Es werden externe Server bei professionellen Hosting-Anbietern mit Firmensitz in Deutschland genutzt, mit welchen Auftragsdatenvereinbarungen geschlossen wurden. Es gelten insoweit ergänzend deren Technische und organisatorische Maßnahmen, die unseren Auftragnehmern bei Vertragsschluss bekanntgegeben und mithin Vertragsgrundlage werden.

6. Gefährdung durch sonstige mögliche Störfaktoren

   Folgender störenden Einflüsse in Räumen/Gebäuden, in denen Datenverarbeitung stattfindet sind wir uns bewusst und werden, insbesondere bei der Installation und Nutzung von IT-Komponenten beachtet: Stromausfall, Internetausfall, Diebstahl (lokale Datenverarbeitungsgeräte verschlüsselt, Mobile Datenverarbeitungsgeräte neben Verschlüsselung auch fernlöschbar).

II. Zugangskontrolle

1. Folgende Maßnahmen schützen die lokalen IT-Systeme vor unbefugter Nutzung:

a) Eigene IT-Systeme können nur in den Räumlichkeiten der CareSocial genutzt werden. Die Nutzung außerhalb der Räumlichkeiten ist nur mittels VPN möglich.
b) Der Zugang zu dem verarbeitenden System i.S.d. Buchstaben a) ist durch Passwortvergabe abgesichert. Jeder Benutzer setzt seine Passwörter selbst ohne Kenntnisnahme eines Dritten.
c) Beim Ausscheiden eines Mitarbeiters wird sein VPN Zugang gesperrt (sofern vorhanden) und der physische Zugang zu den Niederlassungen untersagt. Gleichzeitig werden seine Benutzerkonten gesperrt und binnen der gesetzlichen Fristen gelöscht.
d) Neue Mitarbeiter erhalten Benutzerkonten erst bei Bedarf.

2. Passwörter

a Jeder Berechtigte verfügt über ein eigenes Passwort und ist über den Umgang damit belehrt. Die Passwörter dürfen also nicht niedergeschrieben und auch nicht an Dritte oder Kollegen weitergegeben werden. Sie müssen die nachstehend genannte Mindestzeichenanzahl und –qualität aufweisen.

b) Es existieren folgende Richtlinien, die die Struktur des Passworts, die Nutzung und die Änderungsintervalle beschreibt:
Passwort muss mindestens 12 Zeichen haben, diese müssen Zahlen, Buchstaben und mindestens ein Sonderzeichen enthalten.

c) Passwörter für IT-Systeme und Nutzer werden nur verschlüsselt übertragen bzw. gespeichert.

e) Mitarbeiter werden über den Umgang mit administrativen Passwörtern belehrt.

f) Schlüssel für Kryptographie-Verfahren werden separat gesichert aufbewahrt.

g) Der Zugriff für an IT-Systemen wird nach 3 Anmeldeversuchen automatisch gesperrt.

h) Die Entsperrung eines Administrationszuganges im Falle einer Sperrung erfolgt folgendermaßen:
Nach Prüfung und Rücksprache mit dem sowie Identitätsüberprüfung des Kunden werden Kunden gesperrt und vor Neuvergabe erfolgt eine Freischaltung durch den Service Desk.

3. Gruppenpasswörter

Über den Umgang mit Gruppenpasswörtern sind alle Nutzer belehrt. Gruppenpasswörter werden nicht in für Kunden relevanten Bereichen genutzt.

4. Eigene Datenverarbeitungs-Anlagen

a) Über alle Aktivitäten auf DV-Anlagen werden Protokolle erstellt und unter folgendem Ort abgelegt: Digitale Archiv für An- und Abmeldeprotokolle

b) Diese Protokolle werden durch folgende Personen in folgenden Zeitintervallen hinsichtlich eventueller Unregelmäßigkeiten ausgewertet: Sporadische Prüfung bei Unstimmigkeiten durch die Geschäftsführung

5. IT-Systeme werden folgendermaßen gegen unbefugte Nutzung abgesichert:
   Standleitung, Einwahlverfahrung, IP-Restriktionen, Protokollierung

6. Mobile IT-Systeme

   a) Mobile PCs, die Daten des Auftraggebers verarbeiten werden außerhalb der Bürozeit unter Verschluss gehalten.

   b) Sofern schützenswerte Daten auf mobilen IT-Systemen vorhanden sind, werden diese verschlüsselt.

7. Räume in denen IT-Systeme aufgestellt sind, sind mit folgendem Zugangskontrollsystem ausgestattet: Schließsysteme und Videoüberwachung.

8. Die Identifizierung an IT-Systemen findet folgendermaßen statt:
   Benutzername

9. Die Authentifizierung an IT-Systemen findet folgendermaßen statt:
   Passwort

10. Folgende Personen genehmigen die Zugangsberechtigungen bei IT-Systemen:
    Geschäftsführung, CTO in Absprache mit der Geschäftsführung

11. Zugangsberechtigungen werden folgendermaßen dokumentiert:
    Digitale Dokumentation inklusive Organigrammen.

12. Bei Arbeitsunterbrechung wird ein passwortgeschützter Bildschirmschoner aktiviert bzw. wird der Zugriff gesperrt.

III. Zugriffskontrolle

1. Zugriffsmöglichkeit

   a) Mitarbeiter können nur auf Programme und Daten zugreifen, die sie zur Aufgabenerfüllung benötigen.

   b) Die Zugriffsmöglichkeiten eines Berechtigten auf ein IT-System werden durch folgende Maßnahmen beschränkt:

   funktionale Zuordnung einzelner Datenendgeräte, automatische Prüfung der Zugriffsberechtigung, Protokollierung der Zugriffsberechtigung, Protokollierung der Systemnutzung und Protokollauswertung, ausschließlich Menüsteuerung

   c) Diese differenzierte Zugriffsberechtigung ist folgendermaßen aufgeteilt:
   Dateien, Datensätze, Menüstruktur, Anwendungsprogramme, Server/IT-System

   d) Die differenzierten Verarbeitungsmöglichkeiten sind folgendermaßen aufgeteilt:
   Lesen, Ändern, Löschen

2. Die Daten auf mobilen IT-Systemen sind verschlüsselt.

3. Zugriffsrechte

   a) Zugriffsrechte auf IT-Systeme werden auf Veranlassung folgender Personen vergeben:
   Geschäftsführung

   b) Zugriffsberechtigungen auf Daten und Applikationen genehmigen folgende Personen:
   Geschäftsführung, CTO

   c) Zugriffsberechtigungen im System vergeben folgende Personen:
   Administratoren

   d) Die Zugriffsrechte werden dokumentiert.
   Digitales Benutzerrechte Organigramm

   e) Die Zugriffsrechte werden regelmäßig überprüft.
   Bei Mitarbeiterwechsel (Zugang/Abgang)

4. Es werden keine Wechseldatenträgerlaufwerke genutzt.

5. Es gibt Sicherungsmaßnahmen gegen unbefugtes Kopieren von Daten auf lokale Rechner:
   Verpflichtungserklärung Mitarbeiter

VI. Ergänzend wird hinsichtlich der externen Serversysteme auf die Technischen und Organisatorischen Maßnahmen der (dem Auftraggeber benannten) Unterauftragnehmer verwiesen.