Technische und organisatorische Maßnahmen, Art. 32 DSGVO

Stand 07.05.2018

CSG Clinische Studien Gesellschaft mbH
Friedrichstraße 180
10117 Berlin

www.csg-germany.com

1. Technische und organisatorische Maßnahmen, Art. 32 DSGVO

Zum Schutz der genannten personenbezogenen Daten hat die CSG technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO getroffen, die nachfolgend aufgeführt werden.

Gemäß Art. 32 DSGVO haben verantwortliche Stellen und Auftragsverarbeiter, die personenbezogene Daten verarbeiten,

unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

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

Die CSG trifft die nachfolgenden technischen und organisatorischen Maßnahmen zur angemessenen Sicherung personenbezogener Daten vor Missbrauch und Verlust. Unbefugten wird der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, durch folgende Maßnahmen verwehrt (Zutrittskontrolle):

Serverseitig getroffene Zutrittskontrollmaßnahmen: Server der CSG befinden sich in der Friedrichstraße 180, 10117 Berlin im 4. Und 5.Obergeschoss. Diese sind fensterlos und mit einer Einbruchmeldeanlage alarmgesichert. Wenn die Einbruchmeldeanlage ausgelöst wird, werden automatisch der beauftragte Wachdienst, der Administrator, der Leiter IT sowie die Geschäftsführung informiert. Außerdem existiert ein elektronisches Schließsystem mit RFID an der Tür des Serverraums. Zutrittsrechte zum Serverraum werden personalisiert durch das IT-Büro vergeben. Der Serverraum wird neben seiner eigentlichen Funktion als Aufbewahrungsraum für die Telefonanlage sowie für Werktische und Werkzeug für die Computerreparatur genutzt.

Clientseitig getroffene Zutrittskontrollmaßnahmen: Das Gebäude, in dem sich die Clientarbeitsplätze befinden, ist mit einer Einbruchmeldeanlage alarmgesichert. Wenn die Einbruchmeldeanlage ausgelöst wird, werden automatisch der beauftragte Wachdienst, der Administrator, der Leiter IT sowie die Geschäftsführung informiert. Es existiert ein Empfangsbereich vor den Büros, dort wird auch ein Besucherbuch geführt. Zudem kommen Videoüberwachungsanlagen zum Einsatz, deren Aufzeichnungen für 4 Tage gespeichert werden. Die Büroetagen sind mit einem elektronischen Schließsystem versehen. Als Zutrittstechnik kommt hierbei die

Ausschließlich zum Zweck der besseren Lesbarkeit wird auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind geschlechtsneutral und beziehen sich auf Angehörige aller Geschlechter.

RFID-Technologie zum Einsatz. Die Zutrittstechniken sind personenbezogen vergeben. Es werden sowohl erfolgreiche als auch erfolglose Zutrittsversuche im Zutrittssystem für 24 Stunden gespeichert. An den Bürotüren befinden sich mechanische Schlösser. Betriebsfremde Personen werden am Eingang bzw. Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.

Durch folgende Maßnahmen wird verhindert, dass Unbefugte Datenverarbeitungssysteme genutzt werden können (Zugangskontrolle):

Um zu verhindern, dass Unbefugte Datenverarbeitungsanlagen nutzen können, sind bei der CSG Maßnahmen zur Zugangskontrolle im Einsatz.

Benutzerzugang: Der Zugang zu Informationssystemen von der CSG wird ausschließlich auf Need to know-Basis gewährt. Das Benutzermanagement ist so konfiguriert, dass jeder nicht öffentlich zugänglich CSG-Informationsbestand über ein definiertes Zugangskontrollmanagement verfügt. Durch einen Benutzernamen und ein persönliches Passwort wird der Zugang zu den Systemen, mit denen die Daten verarbeitet werden, geschützt. Die Zugangsberechtigungen werden auf Antrag durch die IT-Abteilung vergeben. Der Antrag muss durch den Vorgesetzten genehmigt sein. Eine Passwortrichtlinie setzt verbindliche Passwortparameter bei der CSG fest: Ein Passwort muss mindestens zehn Zeichen lang sein, mindestens eine Ziffer sowie einen Klein- und Großbuchstaben enthalten. Das IT-System zwingt den Nutzer zur Einhaltung der Passwortvorgaben. Die Anmeldeversuche sind auf 10 erfolglose Versuche begrenzt. Dann wird das System für 30 Minuten gesperrt. Außerdem ist eine automatische, passwortgeschützte Bildschirmsperre im Einsatz, die sich nach 15 Minuten Inaktivität des Nutzers aktiviert. Die Aktualität der Zugangsberechtigungen wird im Falle eines konkreten Anlasses kontrolliert. Bei Verlust, Vergessen oder Ausspähen des Passwortes setzt der Admin ein neues Passwort, das der Nutzer nach der Erstanmeldung zu ändern hat.

Fernzugänge: Der Zugang auf CSG-Ressourcen von außerhalb ist nur von Geräten aus möglich, die mit bestimmten Sicherheitsmaßnahmen ausgestattet wurden. Bei Fernzugängen erfolgt die Authentisierung per VPN-Zertifikat und Passwort. Das Passwort des Fernzuganges muss eine Länge von mindestens zehn Zeichen haben und muss mindestens eine Ziffer sowie einen Klein- und Großbuchstaben enthalten. Die Anmeldeversuche sind auf zehn Versuche begrenzt. Der Fernzugang wird nach 180 Minuten Inaktivität getrennt. Die Zugänge der Mitarbeiter laufen über individuelle Einzelkennungen.

Firewall: Die Systeme, auf denen die Daten verarbeitet werden, werden über eine Firewall abgesichert. Die Firewall wird extern administriert.

Die CSG trägt dafür Sorge, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

Die CSG gewährleistet, dass ausschließlich Personen Zugriff auf Daten erlangen, die mit der Erfüllung der damit verbundenen Aufgabe beschäftigt sind. Hierzu sind entsprechende Zugriffsberechtigungsmaßnahmen (Profile, Gruppen, Rollen etc.) eingerichtet.

Es existiert ein differenzierendes Berechtigungskonzept auf Need-to-know-Basis, das den Zugriff der Mitarbeiter der CSG auf die Daten regelt. Zugriffsberechtigungen der Mitarbeiter werden auf Antrag durch die IT-Abteilung vergeben. Der Antrag muss durch den Vorgesetzten genehmigt sein.

Über personelle Veränderungen wird die IT Abteilung durch die Personalabteilung und die zuständigen Vorgesetzten informiert. Bei Abteilungs-/Funktionswechsel und/oder Ausscheiden eines Mitarbeiters werden die Zugriffsberechtigungen durch die IT-Abteilung aktualisiert bzw. entzogen. Die Berechtigungen werden nach Art der Änderungen/des Wechsels angepasst bzw. entzogen.

Nicht mehr benötigte Datenträger werden durch externe Dienstleister physikalisch zerstört. Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden.

Die CSG trägt durch die nachfolgenden Maßnahmen dafür Sorge, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle):

Die CSG sorgt dafür, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten wird so gestaltet, dass eine Vermischung von Daten für unterschiedliche Verarbeitungszwecke oder anderer Vertragspartner nicht möglich ist. Die zur Verarbeitung der Daten eingesetzten Verfahren sind mandantenfähig.

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

Nach Art. 32 Abs. 1 lit b DSGVO ist die Integrität der Datenverarbeitung zu gewährleisten.

Die CSG trägt dafür Sorge, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle).

Verschlüsselung: Die Mitarbeiter der CSG werden angewiesen, für die Speicherung, den Versand und Transport von personenbezogenen Daten auf mobilen Datenträgern (CD, USB-Stick, Speicherkarten etc.) die systemseitig vorhandene Möglichkeit zur Verschlüsselung zu verwenden. Der Zugriff bei Fernwartungs- bzw. Serviceleistungen auf Datenverarbeitungsanlagen von der CSG sowie eine drahtlose Übertragung (WLAN, Bluetooth etc.) von personenbezogenen Daten erfolgen

innerhalb des Unternehmensnetzwerkes nur über sichere verschlüsselte Verbindungen.

Datentransfer: Der Datentransfer zwischen der CSG und Vertragspartnern erfolgt via: E-Mail mit (verschlüsselten) Anhängen, Fax; Schriftverkehr, Telefon, FTP-Server und Einsichtnahme am Monitor. Dieser Transfer erfolgt verschlüsselt per PGP/SMimer, per VPN, per https / TLS sowie per SFTP.

Mobile Endgeräte: Die Auftragsdaten des Auftraggebers werden bei der CSG auch auf mobilen Endgeräten verarbeitet. Die Endgeräte sind hierbei entweder durch die Benutzerkennung mit Passwort geschützt oder durch eine VPN-Verbindung zum eigenen Firmennetz.

Private Geräte: Eine Verarbeitung von Daten auf privaten Geräten der Mitarbeiter ist nicht gestattet.

Die CSG gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

Informationssysteme werden in der Form konfiguriert, dass eine Vorgangsprotokollierung zur Verfügung steht, die das Betriebs-, Sicherheits- und Datenschutzmanagement in ausreichender Weise unterstützt. Bei zentralen Softwareapplikationen, die Möglichkeiten zur Protokollierung und Änderungshistorie bieten, ist diese Funktion aktiviert. Protokolle werden im Bedarfsfall zweckgebunden ausgewertet.

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

Gemäß Art. 32 Abs. 1 lit. d DSGVO ist ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu etablieren.

Gemäß Art. 32 Abs. 1 lit. d DSGVO, Art. 28 Abs. 1 DSGVO ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Mit externen Dienstleistern, die personenbezogene Daten im Auftrag verarbeiten, werden schriftliche Verträge zur Auftragsverarbeitung nach Maßgabe von Art. 28 Abs. 3 DSGVO abgeschlossen.

Die CSG hat schriftlich einen Beauftragten für den Datenschutz bestellt. Die CSG führt ein Verzeichnis von Verarbeitungstätigkeiten, das den Anforderungen des Art. 30 DSGVO entspricht.

Alle Beschäftigten sind gemäß auf das Datengeheimnis verpflichtet und mit den Themen Datenschutz und Datensicherheit vertraut gemacht.

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

Die CSG trägt dafür Sorge, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

Der Serverraum der CSG verfügt über eine feuerfeste bzw. feuerhemmende Tür sowie über ein Löschsystem (CO2-Löscher) sowie Rauchmelder und eine Klimaanlage. Er ist mit Rauchmeldern und einer Brandmeldezentrale ausgestattet. Die Außenwände des Serverraumes bestehen aus einer Massivwand.

Alle CSG-Dienste, die für die Weiterführung des Geschäftsbetriebs wichtig sind, werden vor den Auswirkungen durch Stromschwankungen oder Stromausfälle geschützt. Dies erfolgt im Wesentlichen durch den Einsatz unterbrechungsfreier Stromversorgungen. Die Funktionalität wird regelmäßig getestet.

Backups der Systeme, auf denen die personenbezogenen Daten gespeichert werden, werden täglich angefertigt. Die Backups werden auf einem zweiten redundanten Server sowie auf Festplatten und einem mobilen NAS gespeichert. Die Backups sind verschlüsselt und werden in einem Bankschließfach aufbewahrt.

Die CSG sorgt dafür, dass Daten gegen Zerstörung oder Verlust geschützt sind. Dazu hat die CSG Schutzmaßnahmen eingerichtet, die Angriffe durch unbefugte Dritte verhindern (Virenschutz, Firewall, Spyware Detection, Spamfilter).

Die von der CSG eingesetzten Virenschutzprogramme sind auf allen Servern und Endbenutzer-Arbeitsplätzen implementiert. Updates werden automatisiert verteilt. Eingehende Dateien (E-Mails, Downloads, Dokumente etc.) werden durch den Echtzeitschutz auf Virenbefall gescannt.