Anlage 3

Technische und organisatorische Maßnahmen nach EU-DSGVO

Stand Februar 2020

Bei all-connect sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO getroffen worden:

1. Vertraulichkeit

Zutrittskontrolle

Die Büroräume der all-connect befinden sich im 1. Obergeschoss in einem Gewerbebereich eines Bürohauses in München. Die Zugänge zum Bürohaus sowie innerhalb des Gebäudes zu den Büroräumen der all-connect sind Tag und Nacht verschlossen. Zugang zum Bürohaus haben nur der Vermieter und Mieter.

Schließsystem Bürohaus:

- Elektronisches und mechanisches Schließsystem
- Verwaltung elektronisches Schließsystem: all-connect
- Verwaltung mechanisches Schließsystem: Vermieter
- Autorisierung eines Schließmediums: Einfach (elektronisch oder mechanisch)

Schließsystem Geschäftsräume all-connect – primärer Sicherheitsbereich „Büros“:

- Elektronisches und mechanisches Schließsystem
- Verwaltung elektronisches Schließsystem: all-connect
- Verwaltung mechanisches Schließsystem: all-connect
- Autorisierung elektr. Schließmedium (Hauptzeit): Einfach (Ausweis oder biometrisches Merkmal)
- Autorisierung elektr. Schließmedium (Nebenzeit): Zweifach (Ausweis und biometrisches Merkmal)
- Autorisierung mech. Schließmedium: Einfach (Nur über Notfall-Kontakte)
- Ausgabe Schließmedien: Personalabteilung der all-connect

Schließsystem Geschäftsräume all-connect – sekundärer Sicherheitsbereich „Rechenzentrum“:

- Zugang nur über primären Sicherheitsbereich möglich
- Elektronisches Schließsystem
- Verwaltung elektronisches Schließsystem: all-connect
- Autorisierung elektr. Schließmedium (Hauptzeit): Einfach (Ausweis oder biometrisches Merkmal)
- Autorisierung elektr. Schließmedium (Nebenzeit): Einfach (Ausweis mit Sonderzugangsrechten)
- Ausgabe Schließmedien: Personalabteilung der all-connect

Die Ausweisvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten durch die Geschäftsführung erst erteilt, wenn dies durch den jeweiligen Vorgesetzten angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zum Bürohaus und dann zu den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.

Jeder Besucher wird über ein Ticketsystem angemeldet und protokolliert. Sie werden von der Empfangsperson zum jeweiligen Ansprechpartner begleitet. Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Der Eingang des primären Sicherheitsbereichs ist mit einer Alarmanlage gesichert, die nicht deaktiviert werden kann. Sie überwacht ständig den verschlossenen Zustand des Zugangsbereichs und wird nur durch ein valides elektronisches Schließmedium für wenige Sekunden außer Kraft gesetzt. Der sekundäre Sicherheitsbereich ist an Fenstern mit einer zusätzlichen Stahlkonstruktion gesichert. Die Schleuse ist durch doppelten Türen mit erhöhter Widerstandskraft gesichert.

Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von all-connect getroffen worden:

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag kann auch über die Personalabteilung gestellt werden.

Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme der all-connect erfolgen stets über verschlüsselte Verbindungen.

Auf den Servern der all-connect ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen der all-connect werden ausschließlich von einem Administrator (ausführend) und einem Mitarbeiter der Qualitätssicherung (Kenntnis des Passworts) gemeinsam eingerichtet.

Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken, Netzwerke oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.

Es gibt ein benutzerbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet. Alle Mitarbeiter bei all-connect sind angewiesen, Informationen mit personenbezogenen Daten und/ oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.

Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren. Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

Trennung

Alle von all-connect für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme bzw. Backup-Verfahren mit eingebauten Verschlüsselungsmechanismen im Einsatz.

2. Integrität

Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von all-connect im Auftrag verarbeitet werden, wird grundsätzlich im Ticket-System protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzerkonten dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von all-connect erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt, oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert. Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei all-connect im Zusammenhang mit Kundenprojekten untersagt.

Mitarbeiter bei all-connect werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet und darauf sensibilisiert worden.

3. Verfügbarkeit und Belastbarkeit

Daten auf Serversystemen von all-connect werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verwahrt bzw. gebracht.

Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie CO2-Löschgeräte. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es gibt bei all-connect einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei all-connect ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es besteht ein Team für Datenschutz und IT-Sicherheit, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.

Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich der Geschäftsführung oder Qualitätssicherung gemeldet werden. Diese werden den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.

Auftragskontrolle

Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union.

Bei all-connect ist ein externer Datenschutzbeauftragter benannt.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführten Audit durch den Datenschutzbeauftragten von all-connect abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bei all-connect wird schon bei der Entwicklung der Software (z.B. web-connect Hosting Plattform oder Kunden-Portal) Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird (z.B. Logfile Einstellungen zur automatisierten Löschung und Anonymisierung von IP-Adressen).

Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.

5. Sicherheitskonzept im Rechenzentrum

Alle IT-Systeme, auch diese, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden, werden im eigenen Rechenzentrum betrieben.

Neben den technischen und organisatorischen Maßnahmen nach DSGVO besteht für das all-connect Rechenzentrum ein detailliertes Sicherheitskonzept das den technischen Schutzmaßnahmen nach § 109 TKG genügt und bei der Bundesnetzagentur als zuständige Aufsichtsbehörde hinterlegt ist. Als öffentlicher Telekommunikationsanbieter sind wir bei der Bundesnetzagentur, unter Reg-Nr. 13/040 registriert.