Anlage 1

Allgemeine technische und organisatorische Maßnahmen

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

a. **Zutrittskontrolle**

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

(Beispiele: Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel / Schlüsselvergabe, Türsicherung (elektrische Türöffner usw.), Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Video- / Fernsehmonitor)

Die Zutrittskontrolle wird durch eine dokumentierte und überwachte Schlüsselvergabe gewährleistet. Der Serverraum von FastViewer kann nur von zutrittsberechtigten Personen betreten werden. Die Schließanlage der dort vorhandenen Tür schützt vor unbefugtem Zutritt durch fremde oder dritte Personen.

b. **Zugangskontrolle**

Eine unbefugte Systemnutzung ist zu verhindern.

(Beispiele: sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Einrichtung eines Benutzerstammsatzes pro User)

Der Zugang zu den Räumen der Datenverarbeitungsanlagen ist geschützt und sämtliche Anlagen bzw. IT-Systeme mit stetig wechselnden Passwörtern versehen. Alle Rechnersysteme werden durch das IT-Personal in der Form eingerichtet, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine persönliche Anmeldung mit Benutzerkennung und Passwort erforderlich. Nach der Erstellung/Vergabe ist das Passwort vom jeweiligen Benutzer zu ändern, dies besteht aus Klein-/Großbuchstaben, sowie Ziffern. Durch die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen erfolgt in der Regel personenbezogen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Kennungen und Passwörter weiterzugeben. Die jeweiligen Passwörter werden im Abstand von 30 Tagen geändert. Sollte ein User, etc. dies nicht tun, wird er vom System dazu gezwungen.

c. **Zugriffskontrolle / Benutzerkontrolle**

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.

(Beispiele: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, Auswertungen Kenntnisnahme, Veränderung und Löschung)

Personenbezogene Daten können nur auf Grundlage der nach dem „need to know“ Prinzip vergebenen Berechtigungen verändert werden. Hierzu wird ein dokumentiertes Berechtigungskonzept etabliert. Mitarbeiter sind in Gruppen eingeteilt, die unterschiedliche Zugangsberechtigungen zu den Datensätzen haben. Dies wird mittels einer Windows Serverstruktur in Verbindung mit „Active Directory“ gewährleistet.

d. **Trennungskontrolle**

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.

(Beispiele: Mandantenfähigkeit / Zweckbindung, Sandboxing, Funktionstrennung / Produktion / Test)

Im FastViewer System ist gewährleistet, dass Daten die zu unterschiedlichen Zwecken erhoben wurden auch getrennt voneinander verarbeitet werden können.

e. **Pseudonymisierung und Verschlüsselung (Zugangs- / Weitergabe- / Übertragungs- kontrolle) personenbezogener Daten (Art. 32 Abs. 1 lit a, 25 Abs. 1 EU-DS-GVO)**

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Alle Backups (Veeam) werden mit einer 256 Bit AES Verschlüsselung versehen.

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

a. **Weitergabekontrolle / Übertragungskontrolle**

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

(Beispiele: Verschlüsselung, VPN, elektronische Signatur, Transportsicherung)

Personenbezogene Daten aus dem IT-System sind vor unbefugtem kopieren auf Datenträgern geschützt. Grundsätzlich werden bei FastViewer keine Daten auf Datenträger gespielt und außerhalb der Firma verwendet. Sollte ein Mitarbeiter über eine VPN-Verbindung von unterwegs aus arbeiten, ist der Zugang durch eine Firewall und dementsprechende Antiviren-, Antispy- und Antihackersoftware geschützt. Einmal von Seiten der Server aus aber auch von den User Computern her, durch die Installation dementsprechender Software.

b. **Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle**

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

(Beispiele: Protokollierung, Dokumentenmanagement)

Im FastViewer IT-System wird jegliche Veränderung, Löschung oder Bearbeitung von Daten und Datensätzen gespeichert, sofern es das System zulässt. Hierbei ist jederzeit nachvollziehbar, welcher User, zu welchem Zeitpunkt welche Veränderung, etc. vorgenommen hat.

c. **Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)**

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

(Beispiele: Backup-Strategie (online / offline; on-site / off-site), unterbrechungsfreie Stromversorgung (USV), Spiegeln von Festplatten, z.B. RAID-Verfahren, Getrennte Aufbewahrung, Virenschutz, Firewall, Meldewege und Notfallpläne; darüber hinaus: rasche Wiederherstellbarkeit, Art. 32 Abs. 1 lit. c EU-DS-GVO)

Es kommen skalierbare Server-Systeme auf Basis von Microsoft Hyper-V zum Einsatz, die sich je nach Belastung anpassen lassen. Die Server werden täglich komplett gesichert. Die verwendeten Geräte können jederzeit über die Softwarelösung FastViewer ferngewartet sowie administriert werden. Die hierfür verwendeten Kommunikationsserver befinden sich in Hochsicherheits-Rechenzentren. Für die Verbindungen selbst wird eine der hochwertigsten verfügbaren Verschlüsselung eingesetzt, um einen entsprechenden Sicherheitsstandard zu gewährleisten. (256 Bit-AES)

Alle wichtigen Systeme unterliegen einer permanenten Überwachung durch Monitoringsoftware des Herstellers Paessler. Sollten kritische Werte erreicht werden, betreffend der Verfügbarkeit oder der Leistungsfähigkeit der Netzwerke/der eingesetzten Geräte, so werden die betreuenden Administratoren umgehend per E-Mail/SMS benachrichtigt. Die gezielte Überwachung von Systemkomponenten und -prozessen hilft, Systemengpässe, Überlastungen und Ausfälle zu vermeiden. Durch die Funktionsvielfalt der Monitoringsysteme von Paessler ist es möglich, 24 Stunden täglich den gesamten Status des Netzwerks sowie der einzelnen Geräte zu überwachen und zu dokumentieren. Der Monitoring Report regelmäßig von einem entsprechend befugten Administrator ausgewertet.

d. **Einführung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 EU-DS-GVO); inkl. Datenschutz-Management, Incident-Response-Management, Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DS-GVO)**

Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers.

(Beispiele: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen)

Es bestehen schriftliche Verträge zwischen Auftraggeber und Auftragnehmern. Der Auftraggeber erteilt dem Auftragnehmer die Weisungen in Schriftform. Der Auftragnehmer hat ausreichende betriebsinterne Anweisungen aufgrund des Auftrags und der damit verbundenen Weisungen des Auftraggebers. Ausreichende Maßnahmen zur Einhaltung des Datenschutzes durch einen möglichen Unterauftragnehmer können auch durch den Auftraggeber geprüft werden. Ein Datenschutzmanagementsystem unter Wahrung der Grundsätze des PDCA-Zyklus nebst schriftlicher Niederlegung, wird etabliert.

Weitere Fragen?

Bei Bedarf können Sie sich auch direkt an unseren Beauftragten für Datenschutz wenden, der Ihre Fragen gerne beantworten wird.

Bestellter externer Datenschutzbeauftragter

Herr Norbert Rauch
atarax GmbH & Co. KG
Dr.-Dassler-Straße 57
91074 Herzogenaurach

Datenschutzkoordinator FastViewer:

Herr Christoph Meier
Tel: +49 9181 509 56-15
E-Mail:datenschutz@fastviewer.com