Auftragsverarbeitung gem. Art. 28 EU-DS-GVO

Vereinbarung

Zwischen der

XY GmbH

Straße
D-

Verantwortlicher, nachstehend Auftraggeber genannt

vertreten durch

Herrn

Geschäftsführer

und

FastViewer GmbH

Schwesterhausgasse 11
D-92318 Neumarkt

Auftragsverarbeiter, nachstehend Auftragnehmer genannt

vertreten durch

Charles-Henry Duroyon

Geschäftsführer

wird folgender Vertrag über Auftragsverarbeitung nach Art. 28 Abs. 3 und den weiteren Bestimmungen der Verordnung 2016/679 EU (EU Datenschutz-Grundverordnung) [i.F.: „EU-DS-GVO“], sowie sonstiger anwendbarer datenschutzrechtlicher Bestimmungen geschlossen:

§ 1 Gegenstand und Dauer des Auftrags, Auftragsinhalt

1. Inhalt

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Inhalt des Vertrages ist die Regelung aller datenschutzrechtlicher Fragen zwischen Auftraggeber und Auftragnehmer.

2. Gegenstand des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Bereitstellung der FastViewer Software
- Bereitstellung der FastViewer Kommunikationsserver
- Bereitstellung des FastViewer Onlineportals und der damit verbunden Funktionalitäten (z.B FastViewer Online-Log)
- Erbringung von Fernwartungsleistungen und Support

3. Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

4. Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers:

- Bereitstellung der FastViewer Software
- Bereitstellung der FastViewer Kommunikationsserver
- Bereitstellung des FastViewer Onlineportals und der damit verbunden Funktionalitäten (z.B FastViewer Online-Log)
- Erbringung von Fernwartungsleistungen und Support

5. Ort der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung kann nach Wahl des Nutzers ausschließlich in Deutschland, alternativ in Ländern innerhalb der Europäischen Union stattfinden oder weltweit erfolgen.
Voraussetzung hierfür ist die Anpassung der Einstellung "Folgende Serverfarm" verwenden des FastViewer Kundenportals (https://portal.fastviewer.com). Jede Verlagerung in ein Drittland bedarf der vorherigen Information des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DS-GVO erfüllt sind.

6. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien:

- ✓ *Personenstammdaten*
- ✓ *Kommunikationsdaten (z. B. Telefon, E-Mail)*
- ✓ *Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)*
- ✓ *Kundenhistorie*
- ✓ *Vertragsabrechnungs- und Zahlungsdaten*
- ✓ *Planungs- und Steuerungsdaten*
- ✓ *Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)*

7. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ✓ Kunden
- ✓ Interessenten
- ✓ Abonnenten
- ✓ Beschäftigte
- ✓ Lieferanten
- ✓ Handelsvertreter
- ✓ Ansprechpartner

§ 2 Pflichten / Kontrollrecht des Auftraggebers

1. Der Auftraggeber ist alleine verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchzuführenden Verarbeitung durch den Auftragnehmer im Hinblick auf die Regelungen der EU Datenschutz-Grundverordnung und anderer Vorschriften über den Datenschutz.

2. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

   Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 EU-DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

   Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann z.B. auch erfolgen durch:

   - Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DS-GVO
   - Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DS-GVO
   - Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
   - Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001).

   Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

   Die Verarbeitung von personenbezogenen Daten an anderen als den vertraglich festgelegten Standorten, z.B. Hotel, Bahn, Flughäfen, Heimarbeitsplatz ist nur insoweit möglich, als das Sicherheitsniveau auch dort adäquat zur Sicherheit am Unternehmenssitz und gemäß Art. 32 DSGVO gewährleistet wird.

3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 3 Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Schriftliche Bestellung eines Datenschutzbeauftragten, soweit gesetzlich erforderlich.

   Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr Norbert Rauch, Abt. Datenschutz, Atarax GmbH, Tel: +49-700 22552827, datenschutz@fastviewer.com bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

2. Die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DS-GVO wird gewahrt. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Diese gelten auch nach Beendigung des Auftrags fort. Er verpflichtet sich, auch folgende relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen, sofern Sie für diesen Auftrag relevant sind:

   _____

   (z.B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse §203 StGB etc.)

3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DS-GVO [Einzelheiten in Anlage 1].

4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

6. Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im Rahmen der vertraglich festgelegten Weisungen und der speziellen Einzelweisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (beispielsweise bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt.

   Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
   Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Weisungsberechtigten beim Auftraggeber bestätigt oder geändert wird.

7. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Unterlagen und Daten betroffen sind.

8. Der Auftragnehmer führt das Verzeichnis der Verarbeitungstätigkeit gem. Art. 30 Abs. 2 EU-DS-GVO und stellt dies auf Anfrage dem Auftraggeber zur Verfügung. Der Auftraggeber stellt dem Auftragnehmer die hierzu erforderlichen Informationen zur Verfügung.
   Der Auftragnehmer unterstützt den Auftraggeber seinerseits bei der Erstellung des Verzeichnisses nach Art 30 Abs. 1 EU-DS-GVO.

9. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten.

10. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

11. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

    Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

    Etwaig anfallende Mehrkosten für den Auftragnehmer im Rahmen dieser Pflichten sind diesem durch den Auftraggeber zu ersetzen.

§ 4 Rückgabe und Löschung

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Kopien, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungsfristen erforderlich sind.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 5 Unterauftragsverhältnisse

1. Der Auftragnehmer darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers beauftragen.

   Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner Pflicht zur Auftragskontrolle verbundene Unternehmen im Sinne der §§15ff. AktG sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen. Als genehmigter Unterauftragnehmer gilt insbesondere auch die FastViewer Software Development GmbH, Sinagasse 33, AT-1220 Wien.

2. Vor Hinzuziehung weiterer oder Ersetzung aufgeführter Unterauftragsverarbeiter informiert der Auftragnehmer den Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform.

3. Der Auftraggeber kann gegen die Änderung – innerhalb einer angemessenen Frist, jedoch nicht länger als 2 Wochen – aus wichtigem datenschutzrechtlichem Grund – gegenüber der vom Auftragnehmer bezeichneten Stelle Einspruch erheben. Erfolgt kein Einspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Bei unberechtigtem Einspruch kann es zu entsprechenden Verzögerungen bei der Erbringung der Leistung nach dem Hauptvertrag kommen. Für eine aus einem unberechtigten Einspruch resultierende Einschränkung der Vertragsleistungen ist der Auftragnehmer nicht verantwortlich.

   In Ausnahmefällen ist auch eine nachträgliche Einigung zwischen den Parteien möglich. Der Auftragnehmer hat den Auftraggeber in diesem Fall unverzüglich über den Einsatz eines Unterauftragsverarbeiters zu informieren.

4. Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU / des EWR, stellen Auftraggeber und Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

5. Eine weitere Auslagerung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mindestens Textform); sämtliche vertragliche Regelungen zu den Datenschutzpflichten in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.

6. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

§ 6 Weisungsrechte

Der Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber erteilt alle Weisungen und Aufträge in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und in schriftlicher oder elektronischer Form zu dokumentieren.
Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format.

- Weisungsberechtigte Personen des **Auftraggebers** sind:

……..

- Weisungsempfänger beim **Auftragnehmer** sind:

……

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

Weisungen des Auftraggebers an den Auftragnehmer werden ausschließlich von den o. g. verantwortlichen Sachgebietsbearbeitern erteilt.

§ 7 Rechte betroffener Personen

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2. Etwaige dem Auftragnehmer hierdurch entstehende Mehrkosten sind diesem durch den Auftraggeber zu erstatten.

§ 8 Technisch-organisatorische Maßnahmen

1. Die in der Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.

   Der Auftragnehmer hat damit die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und

Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DS-GVO zu berücksichtigen.

2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

§ 9 Haftung

Für die Haftung aufgrund von Verletzungen der Datenschutzbestimmungen oder dieser Datenschutzvereinbarung gelten die gesetzlichen Vorschriften, sofern in den für die vertragsgegenständlichen Leistungen geltenden Vertragsdokumenten keine abweichende Haftungsvereinbarung getroffen wurde.

10 Sonstiges

1. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

2. Der Gerichtsstand für beide Parteien ist der Sitz des Auftragnehmers.

3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

……, den ……

Für den Auftraggeber:

Name Unterschrift

Für den Auftragnehmer:

Name Unterschrift

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.

3. 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.

4. 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.

Bestellter externer Datenschutzbeauftragter

Herr Norbert Rauch
atarax GmbH & Co. KG
Dr.-Dassler-Straße 57
91074 Herzogenaurach
E-Mail: datenschutz@fastviewer.com