Anhang zur ADV: *Stand: 18.05.2018*

Technisch-organisatorische Maßnahmen zur Einhaltung des Datenschutzes

Einleitung:

Das vorliegende Dokument beschreibt die technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes bei feiten information & telekommunikation GmbH mit Sitz in Rheinböllen, im Folgenden feiten.it genannt.

Als Auftragsverarbeiter verarbeitet feiten.it Daten ihrer Kunden. Ein Verlust oder unbefugtes Lesen oder Ändern dieser Daten hätte sowohl für unsere Kunden als auch für feiten.it selber weitreichende negative Konsequenzen. feiten.it ist sich über die besondere Verantwortung für die Daten ihrer Kunden bewusst. Um dieser Verantwortung gerecht zu werden, hat feiten.it die erforderlichen technischen und organisatorischen Maßnahmen getroffen, diese Daten nach dem aktuellen Stand der Technik zu schützen.

Die Kunden von feiten.it haben sich laut Art. 28 DS-GVO von der Einhaltung der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes, welche in Art. 32 Abs 1 DS-GVO konkretisiert werden, beim Auftragsverarbeiter zu überzeugen. Grundlage hierfür bildet diese Dokumentation. Die Gliederung dieser Dokumentation richtet sich nach dem Aufbau des Art. 32 Abs. 1 DS-GVO.

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

1.1 Zutrittskontrolle

1.1.1 Zutrittskontrolle

Die Zutrittskontrolle stellt den kontrollierten Zutritt zu den Geschäftsräumen der Gesellschaft sicher. Die Geschäftsräume der Gesellschaft befinden sich Simmerner Str.29 und Simmerner Str. 27, 55494 Rheinböllen. Das Gebäude Simmerner Str. 27 wird von einer anderen Mietpartei genutzt. Der Zutritt zum Gebäude ist mit einer elektronischen Schließanlage gesichert. Über die Schließanlage wird der Zutritt zu den Geschäftsräumen geregelt. Jeder Mitarbeiter verfügt dafür über einen personalisierten RFID-Chip um Zugang zur Büroeinheit zu erhalten. Der erste Zutritt (aufschließen) und das abschließende Verlassen (abschließen) der Büroräume werden protokolliert. Buchhaltung und Geschäftsführerbüro ist ebenfalls nur über RFID zu öffen und wird protokolliert. Zusätzlich ist das Gebäude mit einer Alarmanlage gesichert die auf einen Wachschutz aufgeschaltet ist.

Es ist kein zentraler Empfang eingerichtet. Besucher müssen klingeln und erhalten nur dann Zutritt zur Büroeinheit in dem sie von einem Mitarbeiter eingelassen werden. Besucher werden nicht registriert. Innerhalb des Firmenbereichs werden die Besucher geführt. Jeder Mitarbeiter ist für seine Besucher verantwortlich.

Nebenausgänge, Fluchttüren und sonstige Notausgänge können von außen nicht geöffnet werden.

1.2 Zugangskontrolle

Die Zugangskontrolle verhindert, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können.

Die Server der Gesellschaft werden ausschließlich von namentlich benannten Mitarbeitern der feiten.it administriert. Diese verfügen hierzu über entsprechende Benutzerkonten. Soweit die Gesellschaft Systeme ihrer Auftraggeber monitort oder fernwartet, erfolgt auch dies ausschließlich durch namentlich benannte Mitarbeiter der feiten.it, die hierzu über entsprechende Benutzerkonten verfügen. Die Administration erfolgt sowohl über das Intranet als auch über das Internet mittels verschlüsselter Verbindungen.

Um nicht autorisierten Zugang über das Internet zu verhindern sind die Server durch eine hardwarebasierte Firewall geschützt. Die Server sind in ein nur für diesen Zweck eingerichtetes eigenes virtelles Netzwerk ausgelagert.

Es bestehen folgende Maßnahmen zur Sicherstellung der Zugangskontrolle:

a) Zugangsschutz durch hinreichende Authentifizierung;

b) Authentifizierung soweit möglich im Zweifaktor-Authentifizierungsverfahren;

c) Personen mit Zugangsberechtigungen werden dem Auftraggeber bekannt gegeben und auf ein Minimum beschränkt;

d) Der Auftragnehmer richtet eine automatische und manuelle Zugangssperre bei Verlassen des Arbeitsplatzes ein;

e) Sämtliche Zugangsversuche (erfolgreiche und nicht erfolgreiche) werden protokolliert;

1.3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

In den vom Auftragnehmer genutzten Datenverarbeitungssystemen sind Berechtigungsprofile hinterlegt, in denen die zugriffsberechtigten Personen festgelegt sind. Die Rechte werden in einem geregelten Verfahren vergeben, und die Notwendigkeit der bestehenden Rechte wird regelmäßig kontrolliert. Einrichtung und Freigabe werden dokumentiert.

Der Auftragnehmer hat die technischen und organisatorischen Maßnahmen getroffen, die sicherstellen, dass ausscheidenden Mitarbeitern sämtliche Unterlagen, Zugangsberechtigungen und Zugriffsrechte entzogen bzw. gelöscht werden um einen unberechtigten Zugriff auf die Daten des Auftraggebers zu verhindern.

Der Zugang zu Auftraggeberdaten ist für den feiten.it-Support auf ein Mindestmaß beschränkt. Damit ist es möglich Auftraggeberdaten einzusehen, die für den Support notwendig sind.

Zugriffe auf Auftraggebersysteme werden ausschließlich nach vertraglicher Vereinbarung oder auf schriftliche Weisung (Support Ticket) des jeweiligen Auftraggebers vorgenommen. Die Zugriffe erfolgen ausschließlich über protokollierte Teamviewer. Soweit möglich, werden zusätzlich Tätigkeiten auch im Ticketsystem protokolliert.

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

2.1 Weitergabekontrolle

Die Weitergabe-Kontrolle gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Weitergabe-Kontrolle wird durch verschiedene Maßnahmen gewährleistet. Zum einen werden Daten nur auf den Severn der Gesellschaft gespeichert. Zum anderen werden Daten grundsätzlich nur über verschlüsselte Verbindungen zwischen dem Server und dem Client der Auftraggeber übertragen. Hierbei kommt das SSL verschlüsselte HTTP-Protokoll (HTTPS) zum Einsatz.

Eine Übertragung personenbezogener Daten des Auftraggebers außerhalb von Deutschland findet nur auf Weisung des Auftraggebers statt. Dabei liegt es in der Verantwortung des Auftraggebers ob die Übertragung in einen Mitgliedstaat der Europäischen Union oder in einen anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einen Drittstaat erfolgen soll.

2.2 Eingabekontrolle

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

Die Eingabekontrolle wird je nach Datenverarbeitungssystem über entsprechende Protokolleinträge umgesetzt. Die Protokolleinträge sind nicht änderbar oder löschbar.

Darüber hinaus ist es für eine Vielzahl von verschiedenen Datensätzen direkt in der Anwendung ersichtlich, von welchem Benutzer diese zu zuletzt geändert wurden und wann diese Änderung stattfand.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

In Art. 32 Abs.1 Ziff. b heißt es „…treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: … b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der der Verarbeitung auf Dauer sicherzustellen; …“

Ein mehrstufiges Sicherheitskonzept stellt die Verfügbarkeit der Daten sicher. Alle physikalischen Datenträger (Festplatten) sind als RAID-Verbund ausfallsicher angelegt.

Beim Auftraggeber eingerichtete Systeme werden auf vertraglicher Basis mit Datensicherungsmöglichkeiten eingerichtet. Für die Datensicherung auf den Systemen des Auftraggebers vor Ort (beim Auftraggeber) ist dieser eigenverantwortlich zuständig. Soweit der Auftraggeber den Auftragnehmer mit der Überwachung der Datensicherung beauftragt, besteht die Möglichkeit, ein schriftlich fixiertes Datensicherungskonzept zu vereinbaren, um die Sicherungen bei Verlust oder Zerstörung der physikalischen Datenträger auf andere Datenträger zurückzuspielen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutzmanagement

feiten.it ist sich ihrer Verantwortung in Bezug auf Datenschutz sehr bewusst. Deshalb wird dem Datenschutzmanagement eine besondere Stellung in unserem Haus zuteil. Wir haben uns schriftlich im Rahmen einer gesonderten Erklärung und im Rahmen einer Vielzahl von Leitlinien und Konzepten zu einem verantwortungsbewussten Umgang mit dem Thema Datenschutz verpflichtet.

Unsere Mitarbeiter sind umfassend mit dem Thema durch Schulungen und andere Sensibilisierungsmaßnahmen vertraut gemacht worden. Daneben haben die Mitarbeiter eine Erklärung zur Vertraulichkeit personenbezogener Daten auf Grundlage der DSGVO unterzeichnet. Soweit noch Verpflichtungserklärung nach § 5 BDSG vorliegen, behalten diese ihre Wirkung.

Wir sind uns aber auch der Tatsache bewusst, dass Datenschutz und IT-Sicherheit zwei Seiten einer Medaille darstellen und damit untrennbar miteinander verbunden sind. Dem tragen wir in einer Richtlinie zur Informationssicherheit und einer IT-Sicherheitsrichtlinie Rechnung. Deren Umsetzung wird durch sämtliche Mitarbeiter unseres Unternehmens sichergestellt.

Fortlaufende Datenschutz-Audits in Bezug auf die technischen als auch in Bezug auf die organisatorischen Maßnahmen sollen die eigenen Anforderungen überwachen und durch geeignete Prozesse fortlaufende Verbesserungen sicherstellen. Der Auftragnehmer wird entsprechende Prozesse sukzessive einführen.

4.2 Incident-Reponse-Management

Für anerkannte und vermutete Sicherheitsvorfälle haben wir einen Geschäftsprozess erarbeitet, der sowohl mit technischen als auch mit organisatorischen Maßnahmen sicherstellen soll, dass der Geschäftsbetrieb mit minimalen Störungen aufrechterhalten werden kann.

Das Incident-Response-Management der feiten information & telekommunikation GmbH ist dazu konzipiert, um mit Vorfällen und Notfällen verschiedener Art zielgerichtet, schadensbegrenzend und lösungsorientiert umzugehen. Dazu ist es vor allem auch notwendig, klare Melde- und Bearbeitungswege sowie Verantwortlichkeiten zu definieren und die Effizienz dieser zu erfassen, zu evaluieren und regelmäßig den aktuellen Gegebenheiten anzupassen und zu verbessern.

Aus dem sich ständig ändernden und neuausrichtenden Umfeld der modernen IT ergibt es sich aber zur gleichen Zeit, dass gerade Lösungswege zu Sicherheitsvorfällen nicht starr definiert werden dürfen, sondern dass eine Richtlinie zum Incident-Response-Management stattdessen gleichzeitig das notwendige Rüstzeug und die notwendige Flexibilität anbieten muss, die zur Bewältigung aller möglichen denkbaren und auch (noch) nicht denkbaren Sicherheitslagen geeignet ist.

4.3 Auftragskontrolle

Vor Vergabe der Datenverarbeitung im Auftrag durch den Auftragnehmer an Subunternehmer, stellt der Auftragnehmer sicher, dass beim Subunternehmen eine Kontrolle in Bezug auf die Einhaltung der Anforderungen nach Art. 28 DS-GVO durch Auftraggeber und/oder Auftragnehmer durchgeführt werden kann. Diese Kontrolle stellt sicher, dass beim Subunternehmen die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen zur Sicherung des Datenschutzes nach Maßgabe dieser Vereinbarung eingerichtet sind.

Über jeden Unterauftrag wird ein Vertrag unter Einhaltung der Vorschriften der Datenschutz-Grundverordnung abgeschlossen. Dies gilt insbesondere auch für Verträge über Wartungsarbeiten an den Datenverarbeitungssystemen und über Softwarepflege sowie sonstige IT-Unterstützungsverträge, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Die Datenverarbeitung findet ausschließlich in der feiten.it Zentrale (Simmerner Str. 27) statt. Eine Datensicherung erfolgt im Wortmann Rechenzentum in Hüllhorst.

Soweit der Auftraggeber den Auftragnehmer mit der Wartung und Pflege seiner IT-Systeme beauftragt, finden regelmäßige Software-Updates, soweit vertraglich vereinbart, direkt auf den Servern des Auftraggebers statt. Das Software-Update wird sowohl in Bezug auf die technische Version, die Uhrzeit und den für das Up-Date Verantwortlichen protokolliert.

Ansonsten ist der Auftraggeber selbst für die Wartung und Pflege einschließlich der Software-Updates verantwortlich.

Soweit vertraglich eine Datensicherung der Systeme des Auftraggebers durch feiten.it erfolgt und es im Einzelfall erforderlich ist, spielt feiten.it Daten nur in Absprache mit dem Verantwortlichen Daten zurück. Nur die zuständigen Backup-Administratoren des Auftraggebers und Mitarbeiter der feiten.it haben im 4 Augenprinzip Zugriff auf die Backup-Daten.

Aufträge zum Support oder zur sonstigen Verarbeitung von Kundendaten durch feiten.it an andere Firmen werden ohne vorherige Weisung des Auftraggebers nicht erteilt.

Sonstige Angaben

Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu festzuhalten und dem Auftraggeber bekannt zu geben.