Vereinbarung über die Auftragsverarbeitung

zwischen

dem FUMO Solutions GmbH Kunden

– Verantwortlicher im Sinne des Art. 24 DSGVO,
nachfolgend als „**Auftraggeber**“ bezeichnet –

und der

FUMO Solutions GmbH
Lerchenbergstraße 27
89160 Dornstadt

– Auftragsverarbeiter im Sinne des Art. 28 DSGVO,
nachfolgend als „**Auftragnehmer**“ bezeichnet –

Stand: 29.01.2020

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags zur Verarbeitung personenbezogener Daten ist die Durchführung der Aufgaben durch den Auftragnehmer gemäß dem zwischen den Parteien geschlossenen Vertrag („Hauptvertrag“), welcher durch den Registrierungsprozess der jeweiligen Module und ggf. künftig hinzukommenden Module bzw. durch eine schriftliche Bestellung zustande gekommen ist.

1.2 Die Dauer des Auftrags entspricht der Laufzeit des Vertrages, welcher durch den Registrierungsprozess der jeweiligen Module und ggf. künftig hinzukommenden Module bzw. eine schriftliche Bestellung zustande gekommen ist.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der Aufgaben des Auftragnehmers ergeben sich aus dem Hauptvertrag.

2.2 Die Datenverarbeitung im Auftrag findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2.3 Gegenstand der Verarbeitung personenbezogener Daten sind folgende Arten personenbezogener Daten:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkte- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Daten zu Fahreigenschaften von Beschäftigten wie Führerscheinklassen, Fahrtzeiten, gefahrene Fahrzeuge und Verträge.

2.4 Die Kategorien betroffener Personen im Rahmen dieses Auftrags Betroffenen umfassen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer ergreift die erforderlichen Maßnahmen gemäß Art. 25 und 32 DSGVO und stellt sicher, dass personenbezogene Daten gemäß Art. 5 DSGVO rechtmäßig verarbeitet werden. 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 gemäß Art. 32 Abs. 1 DSGVO zu berücksichtigen (vgl. **Anlage**).

3.3 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.

4. Berichtigung, Einschränkung der Verarbeitung und Löschung von Daten

4.1 Der Auftragnehmer hat nur nach dokumentierter Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung der Daten einzuschränken. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Soweit dies vom Hauptvertrag umfasst ist, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags die Pflichten gemäß Art. 28 bis 33 DSGVO, insbesondere:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38, 39 DSGVO ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

- Die Wahrung der Vertraulichkeit gemäß Art. 32 Abs. 4 DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen zuvor auf die Vertraulichkeit verpflichtet und über die relevanten Datenschutzpflichten belehrt worden sein. Der Auftragsnehmer und jede dem Auftragnehmer unterstellte Person, die im Rahmen des Auftrages Zugang zu personenbezogenen Daten hat, dürfen diese Daten gemäß Art. 29 DSGVO ausschließlich auf Weisung des Auftraggebers verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 25 und 32 DSGVO und der **Anlage** zu dieser Vereinbarung.

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

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde in Bezug auf den Auftrag. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens 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.

— Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags, um zu gewährleisten, dass die Verarbeitung durch den Auftragnehmer rechtmäßig erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

— Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

6. Unterauftragsverhältnisse

6.1 Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer (weitere Auftragsverarbeiter gemäß Art. 28 DSGVO) einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

— Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit Zustimmung des Auftraggebers in Textform (Telefax oder E-Mail genügt) gestattet. Ohne eine solche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Ziffer 5 erläuterten Pflicht zur Auftragskontrolle Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung in Textform mitteilt und der Auftraggeber der Verlagerung der Datenverarbeitung nicht innerhalb eines Monats nach Zugang der Mietteilung in Textform widersprochen hat.

— Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer sowie Art. 28 DSGVO entsprechen.

— Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten

Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

— Die Einschaltung des Unterauftragnehmers ist unzulässig, solange nicht alle vorgenannten Voraussetzungen erfüllt sind.

— Die vorgenannten Voraussetzungen gelten entsprechend, wenn der Unterauftragnehmer seinerseits ein Unterauftragsverhältnis begründen will.

— Bereits jetzt genehmigt der Auftraggeber die Einschaltung des folgenden Unterauftragnehmers: 1&1 Internet SE, Elgendorfer Str. 57, 56410 Montabaur (DE) (Hosting der Webplattform)

6.2 Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

6.3 Erbringt der Unterdienstleister seine Leistungen nicht in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder ist dies bei einem vom Unterauftragnehmer eingesetzten Dienstleister gemäß Absatz 6.2 der Fall, stellt der Auftragnehmer sicher, dass die Verarbeitung personenbezogener Daten rechtmäßig ist.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, Kontrollen im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtungen nach Art. 28 DSGVO erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

7.2 Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 25 und 32 DSGVO und der **Anlage** nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision,

Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) oder der Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder der Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO erbracht werden.

8. Unterstützung des Auftraggebers

8.1 Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

8.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung seiner Pflichten gemäß Art. 32 ff. DSGVO durch

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

9. Weisungsbefugnis des Auftraggebers

9.1 Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. Art. 29 DSGVO). 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 zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

9.2 Mündliche Weisungen wird der Auftraggeber unverzüglich in Textform (Telefax oder E-Mail genügt) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

9.3 Der Auftragnehmer verarbeitet gemäß Ziffer 9.1 und 9.2 die Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

10. Löschung von Daten und Rückgabe von Datenträgern

10.1 Der Auftragnehmer ist nicht berechtigt, Kopien der personenbezogenen Daten zu erstellen. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind

10.2 Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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.

10.2 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.

11. Schlussbestimmungen

11.1 Dieser Vertrag ergänzt den Hauptvertrag, welche durch den Registrierungsprozess der jeweiligen Module und ggf. künftig hinzukommenden Module, oder eine schriftliche Bestellung zustande gekommen ist. Es bestehen keine mündlichen Nebenabreden. Von den in diesem Vertrag niedergelegten Bestimmungen abweichende oder sonstige Vereinbarungen sind nur wirksam, wenn sie schriftlich vereinbart sind. Dies gilt auch für die Aufhebung dieser Schriftform.

11.3 Sollten eine oder mehrere Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder nicht durchführbar sein, so wird die Gültigkeit der übrigen

Bestimmungen hierdurch nicht berührt. Die unwirksame oder undurchführbare Bestimmung ist durch die Vertragspartner durch eine gültige Regelung zu ersetzen, die dem beabsichtigten Zweck der unwirksamen Klausel am nächsten kommt.

Im Falle einer schriftlichen Bestellung hier unterschreiben:

Für den Auftragnehmer	Für den Auftraggeber
Dornstadt, den_____	_____, den _____
_____	_____
(FUMO Solutions)	

Anlage: Allgemeine technische und organisatorische Maßnahmen gemäß Art. 25 Abs. 1 und Art. 32 DSGVO

1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Zentraler Empfangsbereich
- Aufenthalt von Fremden im gesamten Unternehmensgebäude nur in Anwesenheit von Mitarbeitern
- Protokollierung der Zu- und Abgänge von Mitarbeitern
- Festlegung der zutrittsberechtigten Personen für Rechner-/ Serverraum
- Schlüsselregelung (verschlossene Türen; Schlüsselausgabe nur an Befugte; Aufbewahrung und Verwendung eines Generalschlüssels)
- Gebäudesicherung durch Alarmanlage
- Manuelles Schließsystem mit Sicherheitsschlössern
- Protokollierung von Besuchern
- Sorgfältige Auswahl des Reinigungspersonals

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Identifizierung der Benutzer mittels Kennwort gegenüber dem Datenverarbeitungssystem
- Authentifikation der Benutzer durch Passwort
- Regelungen zur Passwortvergabe Persönliches Passwort (Mindestens 8 Zeichen, darunter auch Sonderzeichen / Zahlen, Vergabe durch Nutzer selbst, Keine Weitergabe an Dritte, Regelung für Fall der Abwesenheit (Urlaub, Krankheit etc.))
- Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern
- Regelmäßige Kontrolle der Gültigkeit von Berechtigungen
- Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System
- Abschottung interner Netze gegen Zugriffe von außen (Firewall und VPN)
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von Anti-Viren Software
- Einsatz einer Soft- und Hardware Firewall

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Berechtigungskonzept
- Reduzierung der Anzahl der Administratoren auf das „Notwendigste“
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung
- Verwaltung der Rechte durch Systemadministrator
- Regelungen zur Passwortvergabe Persönliches Passwort (Mindestens 8 Zeichen, darunter auch Sonderzeichen / Zahlen, Vergabe durch Nutzer selbst, Keine Weitergabe an Dritte, Regelung für Fall der Abwesenheit (Urlaub, Krankheit etc.))
- Verschlüsselung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Protokollierung der Vernichtung von Datenträgern

4. Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Verschlüsselte Datenübertragung
- Verwendung von Standleitungen bzw. VPN-Tunneln
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Verpflichtung aller Mitarbeiter zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (VERORDNUNG (EU) 2016/679)

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Protokollierung und Nachvollziehbarkeit der Dateneingabe von Benutzern
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- Auswahl der Auftragnehmer unter Sorgfaltsgesichtspunkten
- Auftragsverarbeitungsvertrag mit Auftragnehmern und Auftraggebern
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags • Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Verfügbarkeit und Belastbarkeit

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.
Maßnahmen zur Datensicherung (physikalisch / logisch):

- Unterbrechungsfreie Stromversorgung (USV) wird gewährleistet
- Datenhosting durch Cloud-Anbieter
- Notfallhandbücher mit definierten Verantwortlichkeiten ○ Regelmäßige, dokumentierte Datensicherung
- Aufbewahrung der Datensicherungen an einem anderen Ort, als das zu sichernde System
- Limitierter Zugang zu Backup-Software auf dedizierte Backup-Administratoren
- Durchführung von stichprobenhaften Funktionalitätstest der Datenbackups
- Sichere Lösch- und Überschreibungsverfahren (Empfehlungen des BSI) der Speichermedien von Datenbackups
- Hochredundante Netzwerk-Infrastruktur
- Brandfrüherkennungsanlage und Argon-Löschanlage

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 Buchstabe c DSGVO)

- Durchführung regelmäßiger Tests zur Datenwiederherstellung

- Dokumentierter Notfallplan
- Dokumentiertes Backup & Recoverykonzept
- Datenhosting durch Cloud-Anbieter o Regelmäßige, protokollierte und dokumentierte Überprüfung des Wiederanlaufplans der Systeme
- Regelmäßige, protokollierte und dokumentierte Simulationen von Notfallsituationen
- Erprobung der Eskalationspfade im Praxisbetrieb
- Aufbewahrung der Datensicherungen an einem anderen Ort, als das zu sichernde System

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern • Berechtigungskonzept
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (software-seitig)
- Trennung von Produktiv- und Testsystem

9. Pseudonymisierung (Art. 32 Abs. 1 Buchstabe a DSGVO)

Eine Pseudonymisierung von Daten findet nicht statt.

10. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 Buchstabe d DSGVO)

Datenschutzmanagement und Meldung von Datenschutzverletzungen (Art. 33 DSGVO)

- Regelmäßige Überprüfung und kontinuierliche Verbesserung des Datenschutzkonzepts
- Regelmäßige Überprüfung und kontinuierliche Verbesserung des Verarbeitungsverzeichnisses
- Durchführung von regelmäßigen Mitarbeiterschulungen
- Durchführung von Risikobewertungen
- Durchführung von regelmäßigen Penetrationstests
- Regelmäßige Aktualisierung der Soft- und Hardware Firewall
- Regelmäßige Aktualisierung der Anti-Viren Software