SLASCONE

AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

SLASCONE GmbH

AVV 10 - 2024

PRÄAMBEL

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben (Auftragsverarbeitungsvertrag). Sie findet Anwendung auf Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) im Auftrag des Auftraggebers verarbeiten.

1. GEGENSTAND, DAUER UND SPEZIFIZIERUNG DER AUFTRAGSVERARBEITUNG

1.1 Aus der Anlage A und dem Hauptvertrag ergeben sich Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung.

1.2 Die Dauer richtet sich nach den Regelungen aus dem Hauptvertrag.

1.3 Erläuterung zum Sonderkündigungsrecht: Der Auftraggeber kann den zugrundeliegenden Hauptvertrag und den AVV jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses AVV vorliegt.

2. ANWENDUNGSBEREICH UND VERANTWORTLICHKEIT

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

2.2 Die Weisungen werden durch Vertrag festgelegt und können vom Auftraggeber danach schriftlich oder in Textform (z. B. E-Mail) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform vom Auftraggeber zu bestätigen.

3. PFLICHTEN DES AUFTRAGNEHMERS

3.1 Der Auftragnehmer darf personenbezogene Daten, die Gegenstand des Auftrags sind, nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor und dessen Voraussetzungen werden gewahrt.

3.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.3 Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat insbesondere technische und organisatorische Maßnahmen zu treffen, gemessen am Risiko für die Rechte und Freiheiten der betroffenen Personen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer gewährleisten.
Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung zu dokumentieren und dem Auftraggeber zur Prüfung bereitzustellen. Die Einzelheiten dieser technischen und organisatorischen Maßnahmen ergeben sich aus Anlage B.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Diese sind vom Auftragnehmer entsprechend zu dokumentieren. Dabei darf das Sicherheitsniveau der in Anlage B genannten Maßnahmen nicht unterschritten werden.

3.4 Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. (Anmerkung: Im AVV können die Parteien hierzu eine Vergütungsregelung für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder die über die gesetzlichen Pflichten des Auftragnehmers hinausgehen oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, treffen).
Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

3.5 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die mit der Verarbeitung der personenbezogenen Daten zuständigen Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeitsverpflichtung auch nach Beendigung des Auftrags fortbesteht.

3.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Eine Meldung von Datenschutzverletzungen muss mindestens enthalten:

- eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen zur Behebung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

3.7 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen:
Dr. Ilias Michalarias
Geschäftsführer

Für Weisung zu nutzende Kommunikationskanäle:
support@slascone.com

3.8 Der Auftragnehmer gewährleistet, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen (Art. 32 Abs. 1 lit. d DS-GVO).

3.9 Während der Vertragslaufzeit berichtigt oder löscht der Auftragnehmer auf Weisung des Auftraggebers die vertragsgegenständlichen Daten. Sofern eine datenschutzkonforme Löschung dieser Daten nicht möglich ist, stellt der Auftragnehmer eine datenschutzkonforme Vernichtung der Datenträger und Unterlagen, die vertragsgegenständliche Daten enthalten, sicher.
Dem Auftragsverarbeiter vom Auftraggeber übergebene Datenträger und verarbeitete Daten einschließlich gefertigter Kopien.
Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die daten schutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. (Anmerkung: Im Vertrag können die Parteien hierzu eine Vergütungsregelung treffen.)

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

3.10 Daten, Datenträger sowie sämtliche Dokumente sind nach Auftragsende auf Verlangen (schriftlich oder in Textform) des Auftraggebers entweder herauszugeben, sofern sie im Eigentum des Auftraggebers sind, oder zu löschen.
Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

3.11 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, 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.

4. PFLICHTEN DES AUFTRAGGEBERS

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten feststellt.

4.2 Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

5. ANFRAGEN BETROFFENER PERSONEN

Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15 bis 21 DS-GVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Anträge der betroffenen Personen im erforderlichen Umfang.

6. NACHWEISMÖGLICHKEITEN

6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die dokumentierten Kontrollen und erforderlichen Auskünfte zur Verfügung zu stellen. Insbesondere ist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art 32 DS-GVO nachzuweisen.

6.2 Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann erfolgen durch

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT- Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- Selbstaudits
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701)
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
- Vereinbarung zwischen Auftraggeber und Auftragnehmer, dass der Nachweis auch durch folgende Unterlagen / Zertifikate erbracht werden kann

6.3 Kontrollrechte

a) Der Auftragnehmer verpflichtet sich, den Auftraggeber bei seinen Prüfungen gemäß Art. 28 Abs. 3 Satz 2 lit. h DS-GVO zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen.

b) Die Prüfungen werden durch den Auftraggeber selbst oder einen von ihm beauftragten Dritten durchgeführt. Sollte der durch den Auftraggeber beauftragte Dritter in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Beauftragte Dritte müssen durch den Auftraggeber zur Verschwiegenheit verpflichtet werden. Dem Auftragnehmer steht das Recht zu, die Abgabe einer separaten Verschwiegenheitserklärung des beauftragten Dritten zu verlangen. Dies gilt insbesondere für die Abgabe von Erklärungen zur berufsrechtlichen oder gesetzlichen Verschwiegenheit.

Eine Prüfung kann insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch weitere Maßnahmen erfolgen. Zu den weiteren Maßnahmen zählen die Anforderung von Zertifizierungen und Berichte zu Datenschutzaudits.

7. WEITERE AUFTRAGSVERARBEITER (SUBUNTERNEHMER)

7.1 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit im Vertrag vereinbarten Verarbeitung personenbezogener Daten beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

7.2 Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber (ggf. Frist und/oder Regelung für Notfallsituationen hier hinzufügen).

7.3 Folgende Subunternehmer gelten als genehmigt:

Name und Anschrift des Subunternehmers	**Beschreibung der Teilleistungen**
Microsoft Ireland Operations Ltd, One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Irland	Webhosting der SLASCONE Licensing & Analytics Anwendung inkl. Speicherung der Kundendaten (Serverstandort EU)

Der Auftraggeber kann der Änderung – innerhalb von einem Monat – aus wichtigem datenschutzrechtlichem Grund – gegenüber dem Auftragnehmer widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger

datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

7.4 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

7.5 Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

8. ÜBERMITTLUNG IN DRITTSTAATEN

8.1 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in einem Mitglieds-staat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Verlagerungen oder Datenverarbeitungen in einem Drittland dürfen nur erfolgen sofern die Voraussetzungen nach Art. 44ff DS-GVO eingehalten werden.

8.2 Einer der folgenden Optionen wird genutzt, um das angemessene Schutzniveau einzuhalten:

- durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO)
- wird hergestellt durch verbindliche interne Datenschutzvorschriften ggf. inklusive zusätzlicher Schutzmaßnahmen (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO)
- wird hergestellt durch entsprechend modulierte Standarddatenschutzklauseln ggf. inklusive zusätzlicher Schutzmaßnahmen (Art. 46 Abs. 2 litt. c und d DS-GVO)
- wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO)
- wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO)
- Der Auftragnehmer ist berechtigt, das angemessene Schutzniveau auch auf andere in Art. 44ff DS-GVO vorgesehene Art und Weise sicherzustellen

8.3 Ist hierzu nichts im Vertrag vereinbart, ist die Verarbeitung in einem Drittstaat nur mit vorheriger Zustimmung des Auftraggebers zulässig. Der Auftragnehmer teilt dem Auftraggeber vorab mit, um welche(n) Drittstaat(en) es sich handelt und auf welche Weise das angemessene Schutzniveau im Sinne von Art. 44 ff DS-GVO für die Verarbeitung dort sichergestellt ist.

9. HAFTUNG

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

10. INFORMATIONSPFLICHTEN, SCHRIFTFORMKLAUSEL, RECHTSWAHL

10.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz- Grundverordnung liegen.

10.2 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.

10.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

10.4 Es gilt deutsches Recht.

ANLAGE A DETAILS ZUR AUFTRAGSVERARBEITUNG

1. BESCHREIBUNG DES ZWECKS UND DER ART DER VERARBEITUNG PERSONENBEZOGENER DATEN

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

Zwecke der Verarbeitung sind dabei alle zur Erbringung der vertraglich vereinbarten Leistung erforderlichen Vertragszwecke, die sich aus dem Vertrag selbst oder weiterführenden Dokumenten zum Vertrag ergeben. Die Art der Verarbeitung umfasst alle Arten der Verarbeitung im Sinne der DS-GVO, Konkretisierungen ergeben sich aus dem Hauptvertrag nebst Anlagen bzw. dem AVV.

Im Einzelnen sind insbesondere die folgenden Tätigkeiten Bestandteil der Datenverarbeitung. Speicherung der vom Auftraggeber über die Nutzeroberfläche eingegebenen Daten in einer Datenbank, Wiedergabe, Systematisierung, tabellarische und/oder grafische Aus-wertung der Daten sowie Löschung der Daten auf Anforderung des Auftraggebers, Wartung und Hosting der dem Service zugrundeliegenden IT-Systeme, Software und Datenbanken und der Umgang mit Backups.
Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies erfolgt durch die Nutzung von SLASCONE Licensing & Analytics, einer Software-Lösung zum Lizenzmanagement.

2. KATEGORIEN BETROFFENER PERSONEN

- Beschäftigte (inkl. Bewerber)
- Reseller und deren Beschäftigte
- (End-) Kunden und deren Beschäftigte

3. ART DER PERSONENBEZOGENEN DATEN

- Kontakt- und Identifikationsdaten: z. B. Vor- und Nachname, Anschrift, Land, Telefon/ Mobilfunk, E-Mail-Adresse, Titel
- Kommunikations- und Netzwerkdaten: Daten die durch die Verwendung einer Softwarelizenz entstehen.

ANLAGE B TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM) I.S.D. ART. 32 DSGVO

1. VERTRAULICHKEIT GEM. ART. 32 ABS. 1 LIT. B DSGVO

1.1 ZUTRITTSKONTROLLE

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Sämtliche relevanten Datenverarbeitungsanlagen befinden sich in Microsoft Azure Rechenzentren. Hier gelten die Microsoft Maßnahmen bzw. Zertifizierungen.

Sonst gelten folgende Maßnahmen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
Manuelles Schließsystem	Schlüsselregelung / Liste
	Alle Daten werden ausschließlich auf digitalen Datenträgern (Laptops) verarbeitet und gespeichert, es besteht somit für Besucher und Gäste kein physischer Zugang zu auf Papier gespeicherten personenbezogene Daten
	Bei Beendigung der Arbeitszeit sind die Mitarbeiter verpflichtet, ihre Laptops mitzunehmen
	Besucher und Gäste werden jederzeit von einem Mitarbeiter begleitet

1.2 ZUGANGSKONTROLLE

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Firewall	Erstellen von Benutzerprofilen
Verschlüsselung von Notebooks / Tablet	Richtlinie „Sicheres Passwort“
MFA (Multi-Faktor Authentifizierung)	Richtlinie „Löschen / Vernichten“
Automatische Desktopsperre	Allg. Richtlinie Datenschutz und Sicherheit

Antivirus	Trennung von administrativen Benutzern für unterschiedliche Bereiche/Systeme
Einsatz von VPN	Regelmäßige interne Pentests anhand von OWASP (Open Web Application Security Project)
Regelmäßige/Automatisierte Sicherheitsupdates für Client- und Serversysteme	
Segmentierung von Netzwerken	

1.3 ZUGRIFFSKONTROLLE

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

Technische Maßnahmen	**Organisatorische Maßnahmen**
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Einsatz Berechtigungskonzepte
Sperrung von Benutzern bei Falschanmeldung	Minimale Anzahl an Administratoren
	Verwaltung Benutzerrechte durch Administratoren
	Regelmäßige Überprüfung von erteilten Berechtigungen

1.4 TRENNUNGSKONTROLLE

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Trennung von Produktiv- und Test-umgebung	Steuerung über Berechtigungskonzept
Mandantenfähigkeit relevanter Anwendungen	Festlegung von Datenbankrechten

1.5 PSEUDONYMISIERUNG (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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

Technische Maßnahmen	Organisatorische Maßnahmen
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Auf-bewahrung in getrenntem und abge-sicherten System (mögl. verschlüsselt)	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. INTEGRITÄT (ART. 32 ABS. 1 LIT. B DSGVO)

2.1 WEITERGABEKONTROLLE

Maßnahmen, die gewährleisten, 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
Protokollierung der Zugriffe und Abrufe	Weitergabe in anonymisierter oder pseudonymisierter Form
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	Vertragsgestaltung mit Dienstleistern
Verschlüsselung von Festplatten (BitLocker)	Vertragsgestaltung mit Mitarbeitern
Geo-redundante Sicherungen (Microsoft Azure)	Regelmäßige Mitarbeiter-Schulungen zum Thema Datenschutz

2.2 EINGABEKONTROLLE

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

3.1 VERFÜGBARKEITSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Sämtliche relevanten Datenverarbeitungsanlagen befinden sich in Microsoft Azure Rechenzentren. Hier gelten die Microsoft Maßnahmen bzw. Zertifizierungen.

ANLAGE C INCIDENT RESPONSE PLAN (IRP)

Dieser Vorfallreaktionsplan skizziert das Verfahren zur Verwaltung und Eindämmung von Sicherheitsvorfällen. Das Ziel besteht darin, eine strukturierte, effiziente und konforme Reaktion auf Sicherheitsbedrohungen bereitzustellen und gleichzeitig die Auswirkungen auf Kunden, Dienste und das Unternehmen zu minimieren. Weitere Details finden Sie unter https://support.slascone.com/hc/en-us/articles/22297946221725-INCIDENT-RESPONSE-PLAN-IRP