Datenverarbeitungsnachtrag

I. Einführung

Datenverarbeitungsnachtrag gemäß Art. 28 DSGVO zwischen der oculavis GmbH, Vaalser Str. 259, 52074 Aachen, Deutschland (nachfolgend "*Auftragnehmer*" genannt) und dem Auftraggeber (nachfolgend auch "*Kunde*" genannt).

Dieser Datenschutz-Zusatz ist Teil des Vertrages zwischen dem Kunden und oculavis , der die Nutzung der Dienste durch den Kunden abdeckt ("Vertrag") und gilt automatisch für Kunden, die einen aktiven Dienstleistungsvertrag mit uns haben ("oculavis"). Sollten sich Änderungen an dieser Vereinbarung ergeben, werden die Kunden entsprechend informiert.

Definitionen

- ***"Personenbezogene Daten"*** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ("betroffene Person") beziehen, wie z. B. Name, E-Mail-Adresse oder ein oder mehrere Faktoren, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

- ***"Auftragnehmer"*** *ist* die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. In diesem Fall "oculavis".

- ***"Dienstleistungsvertrag"*** ist ein rechtsgültiger Vertrag zwischen dem Kunden und der oculavis GmbH über die Nutzung unserer Software und die Erbringung damit verbundener Dienstleistungen.

- ***"Kundendaten"*** sind alle Kundeninhalte, bei denen es sich um personenbezogene Daten handelt, die oculavis im Rahmen der Erbringung der Dienstleistungen im Auftrag des Kunden verarbeitet.

- ***"Leistungen"*** sind die von der oculavis GmbH ggf. zur Verfügung gestellte Software und Dienstleistungen, die vom Kunden genutzt werden.

- ***"oculavis-Datenschutzrichtlinie"*** bezeichnet die Datenschutzrichtlinie für die Dienste, die in ihrer aktuellen Fassung unter https://oculavis.de/en/imprint/ abrufbar ist.

II. Einzelheiten der Verarbeitung

1. **Art und Zweck der Verarbeitung**

oculavis verarbeitet personenbezogene Daten, soweit dies zur Erbringung der Leistungen aus dem Dienstleistungsvertrag erforderlich ist.

Die Softwareplattform oculavis SHARE dient der Fernbetreuung von Technikern oder Kunden mit Datenbrillen, Smartphones und Tablets. Darüber hinaus können technische Dokumentationen wie Anleitungen bereitgestellt und Dokumentationen prozessintegriert erstellt werden. Personenbezogene Daten werden auf der Plattform zur Benutzeridentifikation, Dokumentation, Plattformverwaltung und Wartung gespeichert und verarbeitet.

Die Nutzung der Softwareplattform oculavis SHARE erfordert die Verarbeitung personenbezogener Daten auf der Plattform.

1.1. Rechtsgrundlage für die Verarbeitung personenbezogener Daten (gesetzliche Bestimmungen, Vereinbarung oder Vertragsanbahnung mit der betroffenen Person, Einwilligung der betroffenen Person, Interessenausgleich usw.)

Die folgenden Vereinbarungen werden zwischen der oculavis GmbH und dem SHARE-Anwender für die Nutzung der oculavis SHARE-Software getroffen:

- Dienstleistungsvertrag
- Allgemeine Geschäftsbedingungen der oculavis GmbH und oculavis SHARE https://oculavis.de/en/gtc/
- Datenverarbeitungsnachtrag

2. Art der Daten, Kategorien von betroffenen Personen

Die folgenden Daten können in der oculavis SHARE Software erfasst werden:

- Stammdaten: Vorname, Name/Nachname, E-Mail, Telefonnummer, Firmenname, Abteilung, Nutzername
- Bilder
- Videos
- Dokumente (PDFs, Bilder, Videos, etc.)
- Online-Status
- Chat-Nachrichten (Teilnehmer, Zeit, Nachricht)
- Zeit und Teilnehmer von Videoanrufen: Metadaten (Erstellungsdatum, Beginn und Ende, Teilnehmer)
- Die genannten Daten sind teilweise in der Software miteinander verknüpft und werden von den Nutzern der Softwareplattform selbst eingegeben/erhoben/erzeugt
- Die folgenden Daten werden im Backend der Softwareplattform erfasst:
  - Anmeldedaten (Zeiten, Häufigkeit der Anmeldungen)
  - Verlauf von Chat-Nachrichten, Metadaten von Videoanrufen

Die Durchführung der vertraglich vereinbarten Datenverarbeitung erfolgt ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Eine Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. der Datenschutz-Grundverordnung erfüllt sind. Das angemessene Schutzniveau wird durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO) und durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO) festgelegt.

3. Dauer der Verarbeitung

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit der Dienstleistungsvereinbarung(en). Eine automatische oder halbautomatische Löschung von personenbezogenen Daten findet während der Vertragslaufzeit nicht statt. Bei Beendigung des Vertrages hat der Kunde die Möglichkeit, Daten von

seiner Softwareplattform SHARE zu speichern. Alle personenbezogenen Daten werden nach Ablauf der Aufbewahrungsfrist (in der Regel 90 Tage) oder auf Wunsch des Kunden oder nach Beendigung des Vertrages kontrolliert gelöscht bzw. vernichtet. Mit der Löschung der Daten endet die Verantwortung für diesen Vertrag.

III. Berichtigung, Einschränkung und Löschung von Daten

(1) oculavis ist nicht berechtigt, Daten, die im Auftrag des Kunden verarbeitet werden, eigenmächtig zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, sondern nur nach dokumentierter Weisung des Kunden. Soweit sich ein Betroffener diesbezüglich direkt an oculavis wendet, wird oculavis diese Anfrage unverzüglich an den Auftraggeber weiterleiten.

(2) Sofern der Leistungsumfang ein Löschungskonzept beinhaltet, das Recht auf Löschung der Daten, Datenkorrektur, Datenübertragbarkeit und Auskünfte gemäß den dokumentierten Weisungen des Auftraggebers werden von oculavis sichergestellt.

IV. Technische und organisatorische Maßnahmen

Der Auftragnehmer hat eine Sicherheit gemäß Art. 28 Abs.. 3 lit. c, 32 GDPR, insbesondere in Verbindung mit Art. 5 Abs.. 1, Abs. 2 DS-GVO und muss die Erfüllung dieser Anforderungen nachweisen können. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Datensicherheitsmaßnahmen und Maßnahmen zur Gewährleistung eines risikoadäquaten Schutzniveaus im Hinblick auf die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und der Zweck der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne des Art. 32 Abs.. 1 DS-GVO zu berücksichtigen.

Den vollständigen Text der technischen und organisatorischen Sicherheitsmaßnahmen (TOMs) von oculavis zum Schutz der Kundendaten finden Sie hier https://oculavis.de/de/downloads/TOMs_DE.pdf. Diese Maßnahmen sind Grundlage der Dienstleistungsvereinbarung. Ergibt sich bei der Prüfung/Auditierung durch den Kunden ein Anpassungsbedarf, so wird dieser einvernehmlich umgesetzt.

Die folgende Tabelle enthält Informationen über wichtige Sicherheitsmaßnahmen, z. B. in Bezug auf Backups, Aufbewahrung, Verschlüsselungsmethoden und andere wenige Themen. Um einen detaillierten Blick auf das vollständige Dokument zu werfen, besuchen Sie bitte https://oculavis.de/de/downloads/TOMs_DE.pdf

Technische und organisatorische Sicherheitsmaßnahmen (TOMs)	**Nachweis von technischen und organisatorischen Sicherheitsmaßnahmen**
Maßnahmen zur Pseudonymisierung und Verschlüsselung von Daten	Die Datenbanken, in denen Kundendaten gespeichert werden, sind mit AES-256 verschlüsselt. Backups werden ebenfalls verschlüsselt (AES-256). Die Kundendaten werden bei der Übertragung verschlüsselt (DTLS 1.2, SRTP, HTTPS, TLS 1.2).

Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit von Verarbeitungssystemen und -diensten	Es werden regelmäßig Sicherungskopien der Kundendaten erstellt. Die gesicherten Kundendaten werden aufbewahrt (die Aufbewahrungsfrist beträgt in der Regel 90 Tage) und während der Übertragung und im Ruhezustand mit dem fortgeschrittenen Verschlüsselungsstandard verschlüsselt. Es werden betriebliche Ausfallsicherheitsstrategien und Fähigkeitsergebnisse einbezogen, um einen Plan zur Aufrechterhaltung des Geschäftsbetriebs zu erstellen, zu dokumentieren, zu genehmigen, zu kommunizieren, anzuwenden, zu bewerten und zu pflegen. https://oculavis.de/de/downloads/TOMs_DE.pdf .
Maßnahmen zur Gewährleistung der Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen	Für weitere Informationen besuchen Sie bitte https://oculavis.de/de/downloads/TOMs_DE.pdf .
Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten	oculavis unterhält einen Sicherheitsrahmen auf der Grundlage von ISO 27001 Informationssicherheits-Managementsystem und die Wirksamkeit der TOMs wird regelmäßig (mindestens jährlich) geprüft und bewertet
Maßnahmen zur Identifizierung und Autorisierung der Nutzer	Um das Risiko der Datenexposition zu minimieren, folgt oculavis bei der Vergabe von Systemzugängen dem Prinzip des Least Privilege durch ein Zugriffskontrollmodell. Die Vergabe von Berechtigungen und Zugängen erfolgt nach dem Need-to-know-Prinzip unter Berücksichtigung der Sensibilität und Kritikalität der Datenverarbeitung sowie der Verantwortlichkeiten der Mitarbeiter im Unternehmen. Für weitere Informationen besuchen Sie bitte https://oculavis.de/de/downloads/TOMs_DE.pdf .
Maßnahmen zum Schutz der Daten bei der Übermittlung	Die Datenbanken, in denen Kundendaten gespeichert werden, sind mit AES-256 verschlüsselt. Backups werden ebenfalls verschlüsselt (AES-256). Die Kundendaten werden während der Übertragung verschlüsselt (DTLS 1.2, SRTP, HTTPS, TLS 1.2). Für weitere Informationen besuchen Sie bitte https://oculavis.de/de/downloads/TOMs_DE.pdf .
Maßnahmen zum Schutz der Daten während der Speicherung	Strikte Trennung von Test-/Entwicklungsdaten/-plattformen und Produktionsdaten/-plattformen. Nur die Administratorengruppe der Software hat Zugang zu den Kundeninstanzen (Produktionsumgebung) und

	nur für Sicherungs-, Aktualisierungs- oder Datenwiederherstellungszwecke Für weitere Informationen besuchen Sie bitte https://oculavis.de/de/downloads/TOMs_DE.pdf .
Maßnahmen zur Gewährleistung der physischen Sicherheit der Orte, an denen personenbezogene Daten verarbeitet werden	Für weitere Informationen besuchen Sie bitte https://oculavis.de/de/downloads/TOMs_DE.pdf .
Maßnahmen zur Sicherstellung der Ereignisprotokollierung	Sicherheitsrelevante Ereignisse werden innerhalb von Anwendungen und der zugrunde liegenden Infrastruktur ermittelt und überwacht. Es wird ein Prozess definiert und implementiert, um auf der Grundlage von sicherheitsrelevanten Ereignissen und den entsprechenden Metriken Warnungen an die verantwortlichen Akteure zu übermitteln Für weitere Informationen besuchen Sie bitte https://oculavis.de/de/downloads/TOMs_DE.pdf .
Maßnahmen zur internen IT- und IT-Sicherheitssteuerung und -verwaltung	Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird jährlich überprüft, bewertet und evaluiert. Auf Basis der ISO 27001 werden bei oculavis alle relevanten Normen, Vorschriften, rechtlichen/vertraglichen und gesetzlichen Anforderungen ermittelt und dokumentiert.
Maßnahmen zur Zertifizierung/Absicherung von Prozessen und Produkten	oculavis ist nach ISO 27001 zertifiziert.
Maßnahmen zur Gewährleistung der Datensparsamkeit	Die Daten werden nur für geschäftliche Zwecke erhoben. Die Art der erhobenen Daten finden Sie im Abschnitt „Einzelheiten der Verarbeitung“ des Datenverarbeitungsnachtrags. Die Anonymisierung von Gesichtern erfolgt auch bei mobilen Anwendungen für Personen, die nicht an dem Anruf beteiligt sind.
Maßnahmen zur Sicherung der Datenqualität	Die Datenbanken, in denen Kundendaten gespeichert werden, sind mit AES-256 verschlüsselt. Die Backups sind ebenfalls verschlüsselt (AES-256). Für weitere Informationen besuchen Sie bitte https://oculavis.de/de/downloads/TOMs_DE.pdf .
Maßnahmen zur Gewährleistung einer begrenzten Datenspeicherung	oculavis speichert personenbezogene Daten nur zur Abwicklung des Geschäftsbetriebes. Der Zugriff auf Kundendaten erfolgt nach Einwilligung des Kunden und nach dem Vier-Augen-Prinzip. Es ist ein Löschkonzept implementiert, das Aufbewahrungsfristen für personenbezogene Daten garantiert. Eine automatische oder halbautomatische Löschung von

	personenbezogenen Daten findet während der Vertragslaufzeit nicht statt. Bei Vertragsende erhält der Kunde die Möglichkeit, Daten aus seiner SW-Plattform SHARE zu speichern. Alle personenbezogenen Daten werden nach Ablauf der Aufbewahrungsfrist (in der Regel 90 Tage) oder auf Wunsch des Kunden kontrolliert gelöscht und/oder vernichtet. Logdateien werden nach 30 Tagen gelöscht.
Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung von Daten	Bei Vertragsende hat der Kunde die Möglichkeit, Daten von seiner SW-Plattform SHARE zu speichern. Alle personenbezogenen Daten werden nach Ablauf der Aufbewahrungsfrist (in der Regel 90 Tage) oder auf Wunsch des Kunden kontrolliert gelöscht und/oder vernichtet. Datenschutzanfragen können über privacy@oculavis.de

Die technischen und organisatorischen Maßnahmen sind dem technischen Fortschritt und der Weiterentwicklung unterworfen. In diesem Zusammenhang ist es dem Auftragnehmer gestattet, alternative angemessene Maßnahmen zu ergreifen, sofern diese alternativen Maßnahmen mindestens das Sicherheitsniveau aufrechterhalten, das durch die in den TOMs vereinbarten Maßnahmen gewährleistet wird.

V. Unterprozessoren

Unterauftragsverhältnisse im Sinne dieser Vorschrift sind solche Leistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Zusatzleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. als Telekommunikationsleistungen, Post-/Transportleistungen, Wartung und user services oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, durch geeignete und gesetzeskonforme vertragliche Vereinbarungen und Kontrollmaßnahmen den Datenschutz und die Datensicherheit der Daten des Auftraggebers auch bei Unterauftragsverarbeitern zu gewährleisten.

a) Der Auftragnehmer darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur mit vorheriger ausdrücklicher schriftlicher oder dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der hier genannten Unterauftragsverarbeiter *(*in Kürze verfügbar)* zu (gemäß Art. 28 Abs. 2-4 GDPR).
b) Meldungen und Änderungen von bestehenden Unterauftragsverarbeitern sind zulässig, soweit:

   - der Auftragnehmer den Auftraggeber schriftlich oder in Textform eine angemessene Frist, in der Regel 14 Tage im Voraus, über die Auslagerung an Unterauftragsverarbeiter informiert und
   - der Auftraggeber der geplanten Auslagerung nicht schriftlich oder in Textform gegenüber dem Auftragnehmer bis zum Zeitpunkt der Datenübermittlung widerspricht .
c) Rechte der betroffenen Personen:
   (1) eine vertragliche Vereinbarung im Sinne von Art. 28 Abs. 2-4 DSGVO angewendet wird. Der Auftragnehmer kontrolliert, dass die in dieser Vereinbarung festgelegten Datenschutzverpflichtungen auch gegenüber dem Unterauftragsverarbeiter im Verhältnis zwischen Auftraggeber und Auftragnehmer durchgesetzt werden, einschließlich eines Rechts des Auftraggebers, den/die Unterauftragsverarbeiter selbst oder durch unabhängige Prüfer zu überwachen und zu kontrollieren; der Auftragnehmer wird dem Auftraggeber auf schriftliche Anfrage Informationen über

den wesentlichen Inhalt des Vertrags mit dem Unterauftragsverarbeiter sowie Informationen über die Umsetzung der Datenschutzverpflichtungen im Rahmen des Unterauftragsverhältnisses zur Verfügung stellen. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragsverarbeiter ist nur zulässig, wenn alle Voraussetzungen für die Unterauftragsvergabe erfüllt sind.

(2) Erbringen die Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR, so hat der Auftragnehmer durch geeignete Maßnahmen sicherzustellen, dass dies datenschutzrechtlich zulässig ist. Das Gleiche gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(3) Jede weitere Auslagerung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Auftraggebers (zumindest in Textform).

(4) Alle vertraglichen Regelungen in der Vertragskette müssen auch den weiteren Unterauftragsverarbeitern auferlegt werden.

(5) Auftraggeber und Auftragnehmer, einschließlich des Rechts des Auftraggebers, den/die Unterauftragsverarbeiter selbst oder durch unabhängige Prüfer zu überwachen und zu kontrollieren; der Auftragnehmer wird dem Auftraggeber auf schriftliche Anfrage Informationen über den wesentlichen Inhalt der Vereinbarung mit dem Unterauftragsverarbeiter sowie Informationen über die Umsetzung der Datenschutzverpflichtungen im Rahmen des Unterauftragsverhältnisses zur Verfügung stellen.

VI. Qualitätssicherung und andere Verpflichtungen des Auftragnehmers

Neben der Einhaltung der Bestimmungen dieses Vertrages hat der Auftragnehmer die gesetzlichen Verpflichtungen gemäß Art. 28 bis 33 DSGVO; insoweit hat der Auftragnehmer insbesondere die Einhaltung der folgenden Anforderungen sicherzustellen:

a) Schriftliche Ernennung eines Datenschutzbeauftragten, der seine Aufgaben gemäß Artikel 38 und 39 DSGVO wahrnimmt. 38 und 39 DS-GVO wahrnimmt. Die Kontaktdaten des bestellten Datenschutzbeauftragten finden Sie hier: https://oculavis.de/en/imprint/. Der Auftragnehmer informiert den Auftraggeber unverzüglich über diesbezügliche Änderungen . Die Änderungen haben keinen Einfluss auf den laufenden Vertrag mit dem Auftraggeber.

b) **Vertraulichkeit der Verarbeitung:** Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs.. 3 Satz 2 lit. b, 29, 32 Abs. 4 GDPR. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Mitarbeiter ein, die zur Verschwiegenheit verpflichtet sind und die zuvor mit den für sie relevanten Datenschutzbestimmungen vertraut gemacht worden sind. Der Auftragnehmer und alle ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben, dürfen diese Daten nur nach den Weisungen des Auftraggebers einschließlich der in diesem Vertrag erteilten Ermächtigungen verarbeiten. Die Verschwiegenheitspflicht gilt auch nach Beendigung des Vertrages fort. Der Auftragnehmer wird seine Mitarbeiter regelmäßig im Datenschutz schulen und sie über ihre Pflichten aus dieser Vereinbarung angemessen informieren.

c) Die Durchführung und Einhaltung aller für dieses Abkommen erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs.. 3 Satz 2 lit. c, 32 DSGVO [Details in Anhang 1].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Unverzügliche Unterrichtung des Auftraggebers über Kontrollmaßnahmen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, wenn eine zuständige Behörde im Rahmen eines Verwaltungs- oder Strafverfahrens die Verarbeitung personenbezogener Daten bei der Abwicklung des Vertrags durch den Auftragnehmer untersucht.
f) Wenn der Auftraggeber selbst einer Kontrolle durch die Aufsichtsbehörde, einem Verwaltungs- oder Strafverfahren, der Haftung eines Betroffenen oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Abwicklung des Vertrages mit dem Auftragnehmer ausgesetzt ist, wird der Auftragnehmer ihn nach besten Kräften unterstützen.
g) Der Auftragnehmer muss die internen Prozesse sowie die technischen und organisatorischen Maßnahmen regelmäßig überwachen, um sicherzustellen, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen der geltenden Datenschutzvorschriften erfolgt und die Rechte der betroffenen Person geschützt werden.
h) Der Auftragnehmer führt regelmäßige Überprüfungen in Bezug auf die Erfüllung seiner vertraglichen Verpflichtungen aus diesem Vertrag durch, insbesondere die Einhaltung und ggf. Änderung von Bestimmungen und Maßnahmen, die zur Durchführung des Auftrags festgelegt wurden.

Der Auftragnehmer stellt sicher, dass die getroffenen technischen und organisatorischen Maßnahmen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages gegenüber dem Auftraggeber nachgewiesen werden können.

VII. Kontrollrechte des Auftraggebers

(1) In gegenseitigem Einvernehmen mit dem Auftragnehmer hat der Auftraggeber das Recht, bei Bedarf entweder persönlich oder durch beauftragte Prüfer oder Inspektoren Audits durchzuführen. Der Auftraggeber hat das Recht, sich von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in seinem Betrieb durch Stichproben zu überzeugen, die rechtzeitig anzukündigen sind. Der Auftragnehmer gewährt dem Auftraggeber oder dritten Auditoren des Auftraggebers Zutritt zu den Räumlichkeiten des Auftragnehmers für Inspektionen.
(2) Der Auftragnehmer stellt sicher, dass der Auftraggeber die Einhaltung der Verpflichtungen gemäß Art. 28 DSGVO BESTÄTIGEN KANN. Der Auftragnehmer verpflichtet sich, auf Anfrage die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber nachzuweisen. Der Auftragnehmer wird Kontrollen durch den Auftraggeber oder Dritte unterstützen, insbesondere durch kompetente Ansprechpartner und durch Bereitstellung von relevanten Informationen und Nachweisen auf Anfrage des Auftraggebers.
(3) Der Nachweis von Maßnahmen, die sich nicht nur auf diese spezielle Vereinbarung beziehen, kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder aktuelle Bescheinigungen, aktuelle Atteste, Zertifikate, Berichte oder Auszüge daraus von

unabhängigen Stellen (z.B. Wirtschaftsprüfer, Revisoren, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren). Das Recht des Auftraggebers zur Durchführung von Inspektionen bleibt unberührt.

(4) Der Auftragnehmer kann eine Vergütung für die Erleichterung der Kontrolltätigkeit des Auftraggebers verlangen.

VIII. Meldung von Verstößen durch den Auftragnehmer

1. Der Vertrag oder unterstützt den Kunden bei der Einhaltung der in den folgenden Artikeln festgelegten Verpflichtungen
   32 bis 36 der Datenschutz-Grundverordnung in Bezug auf die Sicherheit personenbezogener Daten, die Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Diese umfassen:

   a) Gewährleistung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die der Art und den Zwecken der Verarbeitung sowie der voraussichtlichen Wahrscheinlichkeit und Schwere einer potenziellen Verletzung von Rechten durch Sicherheitsverletzungen Rechnung tragen und die eine sofortige Feststellung relevanter Verletzungen ermöglichen.
   b) Die Verpflichtung, Verstöße gegen personenbezogene Daten dem Kunden unverzüglich, d. h. innerhalb von 24 Stunden zu melden.
   c) die Verpflichtung, den Kunden bei der Unterrichtung der betroffenen Person zu unterstützen und der betroffenen Person in diesem Zusammenhang unverzüglich alle relevanten Informationen zur Verfügung zu stellen.
   d) Unterstützung des Kunden bei seiner Datenschutz-Folgenabschätzung.
   e) Unterstützung des Kunden im Rahmen der vorherigen Konsultationen mit der Aufsichtsbehörde.
   f) Unverzügliche Unterrichtung des Kunden über alle Inspektionen, Kontrolltätigkeiten oder Maßnahmen der zuständigen Datenschutzbehörden in Bezug auf personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden.

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

IX. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer wird die vom Auftraggeber oder von Dritten, die im Auftrag des Auftraggebers handeln, zur Verfügung gestellten Daten ausschließlich für den Auftraggeber und nur im Rahmen dieses Vertrages und nach den dokumentierten Weisungen des Auftraggebers verarbeiten. Jede andere Verwendung dieser Daten, insbesondere für Zwecke des eigenen Geschäftsbetriebes oder für Zwecke Dritter, ist untersagt.

(2) Mündliche Anweisungen wie in der Vereinbarung, in dieser DPA, oder wie vom Kunden angewiesen oder
Endnutzer des Auftraggebers über die Dienste unverzüglich (zumindest in Textform) zu bestätigen.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der entsprechenden Weisung auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wird.

X. Löschung und Rückgabe von personenbezogenen Daten

(1) Ohne vorherige schriftliche Zustimmung des Kunden dürfen keine Kopien oder Duplikate der im Auftrag des Kunden verarbeiteten Daten angefertigt oder an Dritte weitergegeben werden. Dies gilt nicht für Sicherungskopien, da diese erforderlich sind, um eine angemessene Sicherheit der Datenverarbeitung zu gewährleisten.

(2) Bei Beendigung/Beendigung des Dienstleistungsvertrages - oder früher auf Verlangen des Auftraggebers - hat der Auftragnehmer alle in seinen Besitz gelangten Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datenbanken, die im Zusammenhang mit dem Vertragsverhältnis stehen, herauszugeben oder nach vorheriger Zustimmung datenschutzgerecht zu löschen. Das Gleiche gilt für Test- und Ausschussmaterial. Das Löschungsprotokoll ist auf Verlangen vorzulegen.

(3) Die Dokumentation, die nachweist, dass die Daten ordnungsgemäß und im Einklang mit dieser Vereinbarung verarbeitet wurden, wird vom Auftragnehmer über das Ende dieser Vereinbarung hinaus gemäß den einschlägigen Datenspeicherungsfristen aufbewahrt. Der Auftragnehmer kann diese Dokumentation nach Beendigung dieser Vereinbarung dem Auftraggeber aushändigen.