ANLAGE ZUR RECHNUNG

Auftragsverarbeitung

zwischen

Kunde

Geschäftsansässig siehe Rechnung

- nachstehend auch der „*Auftraggeber*“ genannt -

und

Cosinuss GmbH

mit Sitz in München

Geschäftsanschrift: Kistlerhofstraße 60, 81379 München

- nachstehend „*Auftragnehmer*“ oder „*cosinuss°“* genannt -

- *Auftraggeber* und *Auftragnehmer* nachstehend gemeinsam die „*Parteien*“ genannt -

Vorbemerkung

1.

cosinuss° ist ein Technologieunternehmen, das sich auf die mobile Echtzeit-Überwachung mehrerer Vitalparameter spezialisiert hat. Hierfür entwickelt das Unternehmen eigene In-Ear Sensoren, Mini-Computer, Algorithmen und Software.
Dabei liegt der Fokus stark auf professionellen Anwendungen im Gesundheitswesen, in der Arbeitssicherheit sowie im Hochleistungssport.

Der Auftraggeber hat eine Lizenz zur Nutzung der cosinuss° Technologie zur kontinuierlichen Erfassung, Übertragung und zur Verfügungstellung von Vitalparameter sowie dazu nötige Geräte von cosinuss° erworben.

Falls es keine abweichende Vereinbarung zur Auftragsverarbeitung gibt, gilt diese Standardvereinbarung was folgt:

1. **Allgemeine Bestimmungen und Vertragsgegenstand**

Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragnehmer (Art. 28 DSGVO). Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber. Die Auftragsdetails entnehmen Sie der **Anlage 1**.

2. Vertragslaufzeit und Kündigung

Die Laufzeit des vorliegenden Vertrags richtet sich nach der Laufzeit der gekauften Lizenz. Findet nach Ablauf der Lizenz weiterhin eine Auftragsverarbeitung statt, gilt dieser Vertrag für die betreffenden Verarbeitungsvorgänge fort. Eine ordentliche, von der Lizenz unabhängige Kündigung des vorliegenden Vertrags ist unzulässig. Das Recht zur außerordentlichen fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

Der Auftragnehmer darf Daten nur im Rahmen der zweckmäßigen Bestimmung wie in der Beschreibung des Systems erläutert und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten, insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation.

3.1

Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

3.2

Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass der Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

3.3

Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z. B. per E-Mail) zu erteilen. Mündliche Weisungen sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt.

3.4

Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1

Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen.

4.2

Die Ergebnisse der Kontrollen und Weisungen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragnehmers

5.1

Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z. B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2

Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags dokumentiert. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben von Art. 32 DSGVO ausgewählt. Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen.

7. Unterstützungspflichten des Auftragnehmers

Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Auftragnehmer zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

Der Auftragnehmer ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 3 beigefügt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

8.1

Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des / der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des / der Subunternehmer(s) als genehmigt. Im Falle eines Widerspruchs dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und / oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden

Verdachtsmomente sind dem Widerspruch beizufügen.

8.2

Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und / oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8.3

Sämtliche Verträge zwischen dem Auftragnehmer und dem Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8.4

Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragnehmers

Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.1

Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragnehmer dem Ersuchen des Betroffenen ohne Weisung / Zustimmung des Auftraggebers nachkommen.

9.2

Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine rechtliche oder vertragliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z. B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. Der Auftragnehmer verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen.

12. Haftung

Der Auftragnehmer haftet ggü. dem Auftraggeber im Innenverhältnis nicht, wenn die haftungsauslösende Datenverarbeitung / Maßnahme in Folge einer Weisung des Auftraggebers durchgeführt wurde. Das gleiche gilt für Maßnahmen, die mit dem Auftraggeber abgestimmt wurden (z. B. TOMs nach Art. 32 DSGVO). Als Abstimmung gilt es auch, wenn eine Regelung in diesem Vertrag auf Verlangen des Auftraggebers eingefügt wurde.

12.1

Der Auftraggeber hat dafür zu sorgen, dass die originäre Erhebung der im Auftrag verarbeiteten Daten rechtmäßig erfolgt. Insbesondere hat er die ggf. erforderlichen Einwilligungen vollständig und korrekt einzuholen. Sofern der Auftragnehmer im Außenverhältnis wegen eines Verstoßes gegen diese Pflicht in Anspruch genommen wird, haftet der Auftraggeber ihr gegenüber im Innenverhältnis und stellt sie vom ggf. entstandenen Schaden frei.

12.2

Im Übrigen bleiben die gesetzlichen Haftungsregelungen (insb. Art. 82 DSGVO) unberührt.

13. Schlussbestimmungen

Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

13.1

Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

13.2

Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

13.3

Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

13.4

Vorbehaltlich abweichender Vereinbarungen kann der Auftragnehmer eine zusätzliche Vergütung für Mehraufwendungen verlangen, die ihm durch die Weisungen und Kontrollmaßnahmen des Auftraggebers oder bei der Durchführung der Unterstützungspflichten entstehen.

13.5

Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist der Sitz des Auftragnehmers Gerichtsstand für alle Streitigkeiten aus diesem Vertrag, sofern insoweit hierfür ein ausschließlicher Gerichtsstand nicht begründet wird.

Solange es keine andere schriftliche Vereinbarung gibt, gilt diese Standardvereinbarung zur Auftragsverarbeitung mit dem Kauf des cosinuss° Systems als abgeschlossen.

Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

cosinuss° bietet mobile und im-Ohr tragbare Sensoren zur Erfassung von Vitalparametern, stationäre Gateway Geräte zum Empfang und Weiterleitung der erfassten Daten und eine Server-basierte Web-Applikation an um die Daten zu visualisieren und zu managen. Mit diesen Komponenten zusammen ermöglicht cosinuss° die kontinuierliche Erfassung, Verarbeitung und den Zugang zu Vitaldaten von Individuen aus der Ferne (im Folgenden "Remote Vital Signs Monitoring Solution" genannt). cosinuss° stellt damit eine Ende-zu-Ende-Lösung zur Verfügung, die es Personen/Institutionen ermöglicht, Vitaldaten einer ausgewählten Gruppe von Personen (im Folgenden "Datensubjekte" genannt) aus der Ferne und unter mobilen Bedingungen zu überwachen.

1.
Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

Meta data	**Description**
Sensor Device (with accompanied firmware)	- MAC address - Unique Device Identification (UDI) - Firmware version - Bluetooth Device Name - Cap size
Gateway Device (with accompanied firmware)	- MAC address - Unique Device Identification (UDI) - Software version

Server
(with accompanied software)
	- Record id (data file id)
	- Person pseudonym
	  - Create time
	  - Modified time
	  - Status (Active or disabled)
	- Timestamp record start
	- Timestamp record end
	- Timestamp upload to server
	- Record duration
	- Record time zone
	- Server logs

Device Battery	Battery Level (%)
Quality data	
Quality Index	Fit of sensor indicating quality of measurement
Perfusion Index	Indication of the pulse strength (%)
RAW data	
PPG green	Raw Photoplethysmogram from Green LED
PPG red/infrared	Raw Photoplethysmogram from Red/Infrared LED
PPG ambient	Raw Photoplethysmogram LED turned off
Acceleration / Position	Information about X,Y, Z axis orientation

Temperature	Raw sensor temperature
Primary Vital signs	**Calculated from RAW data**
Core Body Temperature	Core Body Temperature (°C)
Heart Rate	Beats per Minute (bpm)
Respiration Rate	Breaths per Minute (1/min)
Arterial Oxygen Saturation	Blood Oxygen (%)
Server Score	**Calculated from processed Data**
Deviation Score (DS)	Deviation Thresholds on Vital Signs

3.

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

3.1 Patienten des Auftraggebers

3.2 Studienteilnehmer

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt.

Folgende Maßnahmen werden gewährleistet:

1.

Auftragskontrolle (organisatorisch)

1. 1. Auftragnehmer Weisung - Schriftliche Weisungen an den Auftragnehmer.

2.

Datenschutz-Management (organisatorisch)

2. 1. Sensibilisierung - Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich.

2. 2. Schulung/Verpflichtung - Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet Datenschutzbeauftragter: Dr. Johannes Kreuzer, CEO

3.

Datenschutz-Management (technisch)

3. 1. Prüfung technische Schutzmaßnahmen - Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt.

4.

Eingabekontrolle (technisch)

4. 1. Führung von Zugriffsberechtigungen

4. 2. Protokollierung von Eingabe, Veränderungen oder Löschungen pers. Daten

4. 3. Dokumentenmanagementsystem

5.

Transport- und Weitergabekontrolle

5. 1. Vorgabe von verbindlichen oder möglichen Speicherorten für Daten

5. 2. Dokumentation der Zugriffs- und Übermittlungsprogramme

5. 3. Interne Verifizierungsanforderungen - (Vier-Augen Prinzip)

5. 4. Authentifizierung der berechtigten Personen

5. 5. Sicherung des Übertragungs- oder Transportweges

6.

Transport- und Weitergabekontrolle (technisch)

6. 1. Signaturverfahren - Nutzung von Signaturverfahren

6. 2. Protokollierung der Zugriffe und Abrufe - Protokollierung der Zugriffe und Abrufe

6. 3. Einsatz kryptografischer Verfahren (Verschlüsselung)

6. 4. Virtual Private Networks

7.

Trennungskontrolle

7. 1. Trennung von Daten, die unter einem Alias (Pseudonym) gespeichert wurden von den Originaldaten

7. 2. Klare innerbetriebliche Vorgaben für Datenerhebung und Verarbeitung

7. 3. Dokumentation der verwendeten Datenbanken

8.

Trennungskontrolle (technisch)

8. 1. Physikalische Trennung (Systeme/Datenbanken/Datenträger)

8. 2. Berechtigungskonzept - Steuerung über Berechtigungskonzept

8. 3. Verzicht auf integrierte Datenspeicherung

8. 4. Einrichtung logischer Datenbanken

9.

Verfügbarkeitskontrolle (organisatorisch)

9. 1. Notfallmanagement - Notfallplan vorhanden. Schulung der Mitarbeiter

9. 2. Backupkonzept - Backup & Recovery-Konzept vorhanden

9. 3. Durchführung einer Risiko- und Schwachstellenanalyse für den gesamten Datenverarbeitungs-bereich

9. 4. Vorhandensein ausreichender Personalressourcen in der Datenverarbeitung

10.

Verfügbarkeitskontrolle (technisch)

10. 1. Festplattenspiegelung - RAID System / Festplattenspiegelung
Regelmäßige Datensicherung

10. 2. Kontrolle der Datensicherung durch testweises Zurückspielen von Daten

10. 3. Funktionstrennung zwischen Fachabteilung und DV

10. 4. Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in bestehenden Verfahren
10. 5. Einsatz der Fernwartung
10. 6. Unterbrechungsfreie Stromversorgung
10. 7. Virenschutz
10. 8. Firewall

11.

Zugangskontrolle (organisatorisch)

11. 1. Zweckmäßiger und/oder zeitlich beschränkter Zugang zu Endgeräten und der Identifikationsmerkmale
11. 2. Zugangsberechtigungen - Für Angestellte, einschließlich der jeweiligen Dokumentation
11. 3. Zugangsberechtigung nur für bestimmte Einzelpersonen
11. 4. Überprüfungs-, Korrektur- und Kontrollsysteme
11. 5. Regeln und Vorschriften für Dritte - z.B. IT-Dienstleister
11. 6. Prozesse für die Überprüfung und den Release von Programmen
11. 7. Protokollierung von Vorfällen - Überwachung von Einbruchsversuchen
11. 8. Passwort-Richtlinien - regelmäßige Änderung, Mindestlänge, Komplexität
11. 9. Organisation von Dateien - Regelungen über die Organisation von Dateien
11. 10. Differenzierte Zugangsregeln - Teilweise Blockierung
11. 11. Benutzernamen und Passwörter
11. 12. Sichere Verwahrung der personenbezogenen Identifikationsmedien

12.

Zugangskontrolle (technisch)

12. 1. Virenschutz - Einsatz von Anti-Viren-Software
12. 2. Verschlüsselung von Daten im Fall der Online-Übertragung
12. 3. Schutz des Übertragungskanals vor unberechtigtem Zugang
12. 4. Firewall - Einsatz einer Firewall
12. 5. Automatische Desktopsperre
12. 6. Abschottung interner Netze gegen Zugriffe von außen

13.

Zugriffskontrolle/Pseudonymisierung (organisatorisch)

13. 1. Systemtrennung - Trennung von Produktiv- und Testumgebung
13. 2. Sicherung der Bereiche, in denen sich Datenträger befinden
13. 3. Kontrolle der Entfernung von Datenträgern

13. 4. Einsatz Berechtigungskonzepte

13. 5. Differenzierte Zugriffsregelungen - z. B. partielle Sperrung, genaue Nutzerrollen oder Profile

13. 6. Autorisierter Zugriff - Zugriff nur für dafür autorisiertes Personal

13. 7. Administratoren - Minimale Anzahl an Administratoren mit besonderen Zugriffsberechtigungen

14.

Zugriffskontrolle/Pseudonymisierung (technisch)

14. 1. Vernichtung von Datenträgern - Unwiderrufliche Vernichtung von nicht mehr benötigten Datenträgern

14. 2. Sichere Löschung - Sichere Löschung von Datenträgern durch Einsatz von spezieller Software

14. 3. Schutzmaßnahmen für die Dateneingabe in den Speicher und für das Lesen, die Sperrung und Löschung von gespeicherten Daten.

14. 4. Pseudonymisierung und Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System

14. 5. Protokollierung - Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

14. 6. Physische Löschung von Datenträgern wenn notwendig.

14. 7. Nutzung von Verschlüsselung für sicherheitskritische Dateien.

14. 8. Endgeräte mit Zugriffsbenutzerschlüssel oder Benutzercode

14. 9. Nutzung eines Aktenschredders

14. 10. Abschottung interner Netze

15.

Zutrittskontrolle

15. 1. Sicherung der dezentralisierten Datenverarbeitungsanlagen und der Arbeitsplatzrechner

15. 2. Schutz und Einschränkung von Zutrittswegen

15. 3. Closed shops - Bestimmte Sicherheitsbereiche mit eigenen Zutrittskontrollen

15. 4. Bauliche Maßnahmen - Zäune, Überwachungskameras, verschlossene Türen, Tore und Fenster etc.

16.

Zutrittskontrolle (organisatorisch)

16. 1. Zutrittskonzept / Besucherregelung

16. 2. Vertrauenswürdiges Wachpersonal

16. 3. Schlüsselregelung - Vergabe policy, Quittierung

16. 4. Abholung betriebsfremder Personen durch Mitarbeiter

16. 5. Ausgabe von besucherausweisen

17.

Zutrittskontrolle (technisch)

17. 1. Videoüberwachung - Videoüberwachung der Eingänge

17. 2. Verschließbarkeit von Eingängen zu Datenverarbeitungseinrichtungen - Räume, Gehäuse, Computer-Hardware und ähnliche Geräte

17. 3. Verwendung von Sicherheitstüren

17. 4. Sicherheitsschlösser - Verwendung von Sicherheitsschlössern in Türen

17. 5. Gebäudeschachtsicherung - Security Officer

17. 6. Elektronisches Schließsystem

17. 7. Sicherung des Gebäudes oder Eingängen mittels einer Alarmanlage

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

Unternehmensname und Anschrift	Ort der Leistungserbringung
Hetzner Online GmbH Industriestraße 25, 91710 Gunzenhausen Deutschland Zertifikat: DIN ISO/IEC 27001	Falkenstein, Deutschland Nürnberg, Deutschland