Vertrag über Auftragsverarbeitung (AVV)

zwischen

Unternehmen: …….

Anschrift: …….

…….

im Folgenden Verantwortlicher genannt

und

OAS AG

Caroline-Herschel-Straße 1

28359 Bremen

im Folgenden Auftragsverarbeiter genannt

OAS AG

TechnologiePark Bremen
Caroline-Herschel-Straße 1
D-28359 Bremen
+49 421 2206-0
info@oas.de
www.oas.de

Vorstand: Kerstin Schwimmbeck (CEO),
Uwe Heidbreder, Paul Ulrich Höcker, Christian Kaiser
Aufsichtsrat: Dr. Patrick Wendisch (Vorsitzender)
Sitz der Gesellschaft: Bremen
Registergericht: Bremen HRB 22006
USt-IdNr.: DE114425032

Die Sparkasse Bremen AG
IBAN DE78 2905 0101 0001 0294 53 | BIC SBREDE22XXX
Commerzbank AG
IBAN DE59 2904 0090 0123 0010 00 | BIC COBADEFFXXX
Bremische Volksbank Weser-Wümme eG
IBAN DE06 2919 0024 0091 7249 00 | BIC GENODEF1HB1

1. Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die im Anhang 1 aufgeführten Datenverarbeitungen durch. Darin werden Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien verarbeiteter Daten und betroffener Personen beschrieben.

2. Weisungen der Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für in Anhang 1 aufgeführte Zwecke bzw. nur auf Grund dokumentierter Weisungen des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der Union oder eines Mitgliedstaats verstößt.

(3) Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

3. Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft mindestens die im Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.

(2) Die in Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter die Anpassungen dem Verantwortlichen unaufgefordert mit.

4. Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der erhaltenen

personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz und teilt dessen Kontaktdaten im Anhang 1 mit. Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über den Wechsel des Datenschutzbeauftragten.

(4) Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundes-republik Deutschland, in einem Mitgliedstaat der Europäischen Union oder inner-halb des Europäischen Wirtschaftsraums. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen dokumentierten Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind.

5. Unterstützungspflichten des Auftragsverarbeiters

(1) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden und bei Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

(2) Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungs-pflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

(3) Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann.

6. Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens drei Wochen im Voraus in Textform über alle beabsichtigten Beauftragungen von Unterauftragsverarbeitern, damit der Verantwortliche vor der Beauftragung Einwände erheben kann. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Wahrnehmung seines Einspruchsrechts zu entscheiden mit der Unterrichtung über die geplante Beauftragung zur Verfügung. Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 6 Abs. 2 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

(2) Ein Zugriff auf personenbezogene Daten durch Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber dem Unterauftragsverarbeiter gelten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf

Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen vollumfänglich dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhaltet, die Einhaltung der Regelungen der Artikel 44 ff. DSGVO sicher, indem – sofern erforderlich - geeignete Garantien gemäß Artikel 46 DSGVO getroffen werden.

(4) Der Auftragsverarbeiter verpflichtet sich in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, mit dem Unterauftragsverarbeiter Standardvertragsklauseln nach Art. 46 DSGVO zu schließen, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

(5) Im Falle des § 6 Abs. 4 führt der Auftragsverarbeiter eine Prüfung nach den Klauseln 14 und 15 der Standardvertragsklauseln durch und stellt diese dem Verantwortlichen unaufgefordert zur Verfügung. Kommen Auftragsverarbeiter oder Verantwortlicher zu dem Ergebnis, dass weitere Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. Der Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

7. Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragsverarbeiters berücksichtigen.

(2) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt.

(3) Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

8. Mitzuteilende Verstöße

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

9. Beendigung des Auftrags

(1) Mit Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, dies gilt auch für etwaige Sicherungskopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen. Die Löschung hat der Auftragsverarbeiter dem Verantwortlichen in Textform anzuzeigen.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

(3) Der Auftragsverarbeiter kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Verantwortliche auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragsverarbeiter den Verantwortlichen darüber in Kenntnis gesetzt hat.

10. Beitritt zum Vertrag

Diesem Vertrag können mit Zustimmung aller Parteien über eine Beitrittserklärung jederzeit weitere Parteien als Verantwortliche oder als Auftragsverarbeiter beitreten. Zusätzlich zur Beitrittserklärung sind – soweit erforderlich – die Anhänge 1 bis 3 auszufüllen. Ab dem Zeitpunkt des Beitritts gelten die beitretenden Parteien als Vertragsparteien dieses Vertrags mit den entsprechend ihrer Bezeichnung bestehenden Rechten und Pflichten.

11. Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(3) Im Falle eines Widerspruchs zwischen diesen Vertragsklauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Ort, Datum…….. ……..

Verantwortlicher

Ort, Datum ……. ……..

Auftragsverarbeiter

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Der Auftragsverarbeiter erbringt für den Verantwortlichen Dienstleistungen, IT-Administration, Fernwartung für die bei dem Verantwortlichen eingesetzte Software, u. a. Logistiklösung, Wägedatenverarbeitung, Prozessleit- und Dokumentenmanagementsysteme sowie kaufmännische Softwarelösungen.
Art und Zweck der Verarbeitung	Im Rahmen der Dienstleistungen und dem technischen Support hat der Auftragsverarbeiter Zugriff auf personenbezogene Daten des Verantwortlichen. Die Tätigkeit dient der Gewährleistung und Erhaltung des ordnungsgemäßen Betriebs der vorab aufgeführten Systeme und Lösungen sowie der Fehlerbehebung, dem Support und der internen IT-Organisation.
Art der personenbezogenen Daten	Der Auftragsverarbeiter hat Zugriff auf: Nutzungsdaten, Bestandsdaten, Personalstammdaten, Zeiterfassungsdaten, Telekommunikationsdaten, Bild- und Videodaten, Logfiles sowie sonstige Kundendaten.
Kategorien betroffener Personen	Von der Datenverarbeitung sind alle Personen betroffen, die in einem Programm, z. B. Personalwesen, Rechnungswesen, Warenwirtschaft und Dokumenten-Management-System erfasst werden sowie Nutzer der Programme des Verantwortlichen. Das sind insbesondere ▪ Mitarbeiter des Verantwortlichen, ▪ Freiberufler, ▪ Geschäftskunden, ▪ sonstige externe Personen. Außerdem sind alle Personen betroffen, auf deren E-Mails der Auftragsverarbeiter im Rahmen des Supports Zugriff hat und der Personenkreis, der im E-Mail-Kontakt mit dem Verantwortlichen steht.
Dauer der Verarbeitung	Entspricht der Dauer des Hauptvertrages bzw. des Auftrags vom …….

Datenschutz-beauftragte/r des Verantwortlichen	Bitte Kontaktdaten eintragen oder „Der Verantwortliche hat keinen Datenschutzbeauftragten bestellt.“
Datenschutz-beauftragte/r des Auftragsverarbeiters	datenschutz nord GmbH Konsul-Smidt-Straße 88 28217 Bremen Web: www.datenschutz-nord-gruppe.de office@datenschutz-nord-gruppe.de

Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

- **ENTFÄLLT –**

Anhang 3: Technisch-organisatorische Maßnahmen der OAS AG

Siehe Anlage „Datenschutz - Technisch organisatorische Maßnahmen“

Datenschutz – Technisch organisatorische Maßnahmen

Inhaltsverzeichnis

1. Ziel und Zweck 2
2. Geltungsbereich 2
3. Zuständigkeiten 2
4. Begriffe 2
5. Abläufe und Regelungen 3
   5.1. Zugangskontrolle 3
   5.2. Datenträgerkontrolle 3
   5.3. Speicherkontrolle 3
   5.4. Benutzerkontrolle 4
   5.5. Zugriffskontrolle 4
   5.6. Übertragungskontrolle 4
   5.7. Eingabekontrolle 5
   5.8. Transportkontrolle 5
   5.9. Wiederherstellbarkeit 5
   5.10. Zuverlässigkeit 5
   5.11. Datenintegrität 5
   5.12. Auftragskontrolle 6
   5.13. Verfügbarkeitskontrolle 6
   5.14. Trennbarkeit 6
   5.15. Sonstige Maßnahmen gem. Art. 32 Abs. 1 lit b, c, d DSGVO 6
6. Dokumentation 7
7. Mitgeltende Unterlagen 7
8. Änderungshistorie 7

© OAS AG

Erstellt:	02.01.2025	**Geprüft:**	02.01.2025	**Freigegeben:**	02.01.2025
M. Pott		S. Häusler		C. Lienau	

1. Ziel und Zweck

Mit dieser Verfahrensanweisung legen wir die technisch organisatorischen Maßnahmen fest, die wir zum Schutze aller unserer Daten, speziell aber der personenbezogenen Daten nach DSGVO, getroffen haben.

2. Geltungsbereich

Der Geltungsbereich dieser Verfahrensanweisung erstreckt sich auf alle Mitarbeiter[1] der OAS AG und der zugehörigen Tochterunternehmen.

3. Zuständigkeiten

Die technischen und organisatorischen Maßnahmen werden von der Leitung IT und dem Datenschutzbeauftragten festgelegt. Die Umsetzung erfolgt durch IT-intern und den Datenschutzkoordinator.

4. Begriffe

DSGVO	Datenschutzgrundverordnung

© OAS AG

[1] Auf die Verwendung von Doppelformen oder andere Kennzeichnungen für weibliche und männliche Personen wird verzichtet, um die Lesbarkeit und Übersichtlichkeit zu wahren. Mit allen im Text verwendeten Personenbezeichnungen sind stets beide Geschlechter gemeint.

5. Abläufe und Regelungen

5.1. Zugangskontrolle

- Zu den üblichen Bürozeiten existiert ein ständig besetzter Empfangsbereich zum Gebäude.
- Das Gebäude ist mittels einer Einbruchmeldeanlage (EMA) alarmgesichert.
- Beim Auslösen der EMA wird ein beauftragter Wachdienst informiert.
- Das Gebäude ist mit einem elektronischen Schließsystem ausgestattet (RFID und PIN).
- Zutrittsregelung: Abholung und Begleitung von betriebsfremden Personen am Eingang.
- Der Serverraum ist mittels Einbruchmeldeanlage geschützt
- Die Zutrittsrechte werden personifiziert vergeben
- Die Zutritte werden protokolliert und 90 Tage gespeichert.

5.2. Datenträgerkontrolle

- Verschlüsselung beim Transfer personenbezogener Daten per
    - Verschlüsselter Datei als Mailanhang
    - VPN
    - https / TLS
    - Dateiaustausch per Cryptshare
- Entsorgung von nicht mehr benötigten Papierunterlagen in verschlossene Datentonnen, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden.
- Nicht mehr benötigte Datenträger werden vom Entsorger physisch zerstört.
- Auf Notebooks erfolgt eine Verschlüsselung der Festplatte.
- Smartphones verfügen über eine sog. Container Lösung, ein Bereich auf der Festplatte ist geschützt und aus der Ferne löschbar.
- Verbindliche Passwortparameter bei Notebooks: Hardware-Token (TPM) plus 6 Zeichen
- Die Verarbeitung von personenbezogen Daten auf eigenen privaten Geräten der Mitarbeiter (bring your own device) ist untersagt.

5.3. Speicherkontrolle

- Authentisierung der Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst.
- Verbindliche Passwortparameter: Minimum 8 Zeichen. Von diesen 8 Zeichen muss mindestens 1 Zeichen als Sonderzeichen hinterlegt sein. Außerdem sind Zahlen, Buchstaben (klein/groß) und Sonderzeichen zu mischen, Gültigkeitsdauer max. 90 Tage.
- Verwaltung der Rechte durch Systemadministratoren.

© OAS AG

5.4. Benutzerkontrolle

- Sofern nichts Abweichendes angegeben ist, gilt für passwortgeschützte Anwendungen gemäß IT-Richtlinie immer: Die Länge muss mindestens 8 Zeichen betragen. Von diesen 8 Zeichen mindestens 1 Sonderzeichen, jeweils 1 Groß- und Kleinbuchstabe und eine Ziffer, die bunt gemischt aneinandergereiht werden.
- Verschlüsselung beim Transfer personenbezogener Daten
- Schutz vor unbefugten Datenzugriffen mittels stets aktualisiertem Virenschutz, Anti-Spyware und Spamfilter
- Regelmäßige Updates der Firewall.
- Authentifikation mit Benutzername/Passwort
- Sperrung ausscheidender Mitarbeiter

5.5. Zugriffskontrolle

- Verwaltung der Rechte durch Systemadministratoren.
- Authentisierung der Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst.
- Sperrung des Bildschirms nach längstens 15 Minuten Inaktivität.
- Begrenzung von erfolglosen Anmeldeversuchen (5); die Zugänge bleiben für 60 Minuten gesperrt.
- Authentisierung bei Fernzugängen mit VPN-Zertifikat und Benutzerkennung inkl. Passwort und Multikfaktor.
- Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen (5), die Zugänge bleiben für 5 Minuten gesperrt.
- Schutz vor unbefugten Datenzugriffen mittels stets aktualisiertem Virenschutz, Anti-Spyware und Spamfilter
- Regelmäßige Updates der Firewall.

5.6. Übertragungskontrolle

- Verschlüsselung beim Transfer personenbezogener Daten per
    - Verschlüsselter Datei als Mailanhang
    - VPN
    - https / TLS
    - Dateiaustausch per Cryptshare

© OAS AG

5.7. Eingabekontrolle

- Verwaltung der Rechte durch Systemadministratoren.
- Authentisierung der Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst.
- Authentifikation mit Benutzername/Passwort

5.8. Transportkontrolle

- Verschlüsselung beim Transfer personenbezogener Daten per
  - Verschlüsselter Datei als Mailanhang
  - VPN
  - https / TLS
  - Dateiaustausch per Cryptshare
- Verschlüsselung der Backups

5.9. Wiederherstellbarkeit

- Tägliche Speicherung des Datenbestandes
- Speicherung auf Sicherungsbändern und Festplatten
- Externe Lagerung der Sicherungsbänder
- Speicherung der Backups in einem externen Rechenzentrum
- Verschlüsselung der Backups
- Der Aufbewahrungsort der Backups befindet sich in einem vom primären Server aus betrachtet getrennten Brandabschnitt.

5.10. Zuverlässigkeit

- Schutz vor unbefugten Datenzugriffen mittels stets aktualisiertem Virenschutz, Anti-Spyware und Spamfilter.
- Behebung von Fehlfunktionen und Ausfällen durch die interne IT.

5.11. Datenintegrität

- Tägliche Speicherung des Datenbestandes
- Speicherung auf Sicherungsbändern und Festplatten
- Externe Lagerung der Sicherungsbänder
- Speicherung der Backups in einem externen Rechenzentrum
- Verschlüsselung der Backups

© OAS AG

- Der Aufbewahrungsort der Backups befindet sich in einem vom primären Server aus betrachtet getrennten Brandabschnitt.

5.12. Auftragskontrolle

- Auftragskontrolle: Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen, z. B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters.

5.13. Verfügbarkeitskontrolle

- Rauchmelder
- Anschluss des Serverraums an eine Brandmeldezentrale
- Löschsystem (CO2-Löscher)
- Klimatisierung
- Unterbrechungsfreie Stromversorgung (USV)
- Regelmäßige Tests der technischen Sicherungsmaßnahmen
- Tägliche Speicherung des Datenbestandes
- Speicherung auf Sicherungsbändern und Festplatten
- Speicherung der Backups in einem externen Rechenzentrum
- Verschlüsselung der Backups
- Der Aufbewahrungsort der Backups befindet sich in einem vom primären Server aus betrachtet getrennten Brandabschnitt.

5.14. Trennbarkeit

- Datenbank-Segregation, wenn dies erforderlich ist.
- Mandantentrennung, wenn dies erforderlich ist.

5.15. Sonstige Maßnahmen gem. Art. 32 Abs. 1 lit b, c, d DSGVO

- Gemeinsam mit dem externen Datenschutzbeauftragten der OAS AG werden die technischen und organisatorischen Maßnahmen dokumentiert, regelmäßig geprüft und bewertet sowie ggf. angepasst.
- Die OAS AG setzt ein Datenschutzmanagementtool zur Dokumentation ein. U. a. werden hier das Verzeichnis für Verarbeitungstätigkeiten, bei denen wir Verantwortlicher sind, Datenschutzverstöße und Betroffenenanfragen geführt.
- Verarbeitungstätigkeiten, bei denen wir Auftragsverarbeiter sind, werden im ERP-System dokumentiert.
- Eine dokumentierte Richtlinie zum Vorgehen bei Datenschutzverstößen ist vorhanden.

© OAS AG
Revision A 02.01.2025

- Mitarbeiter der OAS AG, die personenbezogene Daten verarbeiten, werden auf die Vertraulichkeit verpflichtet und regelmäßig im Datenschutz geschult.

6. Dokumentation

Die Dokumentation der Maßnahmen erfolgt in Form von Protokollen und Listen im Bereich der IT-intern bzw. im Datenschutzmanagementtool.

7. Mitgeltende Unterlagen

Interne Anweisungen von IT-intern
Jährliche Bewertung des Datenschutzbeauftragten

8. Änderungshistorie

Version	Datum	Änderungsgrund
A	02.01.2025	Integration in QM-System, Überarbeitung, MFA für VPN

© OAS AG