Stand: 04.09.2026

Vertrag über die Auftragsverarbeitung

(remberg Software)

1. Vertragsgegenstand, Definitionen und Rangordnung

1.1 Dieser Vertrag über die Auftragsverarbeitung (nachfolgend „**AV-Vertrag**“ genannt) regelt die datenschutzrechtlichen Rechte und Pflichten gem. Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (nachfolgend „**DSGVO**“ genannt), soweit im Rahmen der Leistungserbringung gemäß Angebot, Bestellung, Bestellschein, oder Leistungsbeschreibung und AGB (nachfolgend gemeinsam „**Hauptvertrag**“ genannt) der Auftragnehmer (als Auftragsverarbeiterin i.S.v. Art. 4 Nr. 8 DSGVO) personenbezogene Daten im Auftrag des Auftraggebers (als Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO) verarbeitet. Als Verantwortlicher trägt der Auftraggeber die alleinige Verantwortung für die Rechtmäßigkeit der Übermittlung der personenbezogenen Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung.

1.2 Die Definitionen des Hauptvertrages gelten für den AV-Vertrag (einschließlich Anlagen) entsprechend, mit der folgenden Maßgabe: Der Kunde wird auch als „**Auftraggeber**“ und remberg auch als „**Auftragnehmer**“ bezeichnet. Soweit im AV-Vertrag die Begriffe „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) verwendet werden, wird die Definition der Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1.3 Bei Widersprüchen oder Unklarheiten zwischen den Bestimmungen des Hauptteils des AV-Vertrages und den Bestimmungen der Anlagen zum AV-Vertrag gehen die Bestimmungen des Hauptteils des AV-Vertrages vor. Bei Widersprüchen oder Unklarheiten zwischen den Bestimmungen des AV-Vertrages und den Bestimmungen des Hauptvertrages gehen die Bestimmungen des AV-Vertrages vor, soweit es sich um datenschutzrechtliche Themen handelt.

2. Beschreibung der Datenverarbeitung und Laufzeit

2.1 Die Einzelheiten der Datenverarbeitung, insbesondere die Zwecke, für die die personenbezogenen Daten im Auftrag des Auftraggebers verarbeitet werden, und die Kategorien personenbezogener Daten, sind in **Anlage 1** zu diesem Vertrag aufgeführt. Die Einzelheiten der Leistungserbringung sind im Hauptvertrag geregelt.

2.2 Die Laufzeit des AV-Vertrages entspricht der Laufzeit des Hauptvertrages. Der AV-Vertrag endet automatisch mit Beendigung des Hauptvertrages.

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten. Die technischen und organisatorischen Maßnahmen sind in **Anlage 2** spezifiziert. Der Auftraggeber hat die technischen und organisatorischen Maßnahmen in **Anlage 2** geprüft und erachtet diese unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung als angemessen i.S.d. Art. 32 DSGVO.

3.2 Soweit eine Überprüfung durch den Auftraggeber einen Anpassungsbedarf der in **Anlage 2** aufgeführten technischen und organisatorischen Maßnahmen ergibt, werden sich die Parteien einvernehmlich über eine Anpassung der technischen und organisatorischen Maßnahmen mit geeigneten Mitteln verständigen.

3.3 Die in **Anlage 2** aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer ist berechtigt, andere adäquate Maßnahmen umzusetzen, wobei das Sicherheitsniveau der in **Anlage 2** aufgeführten technischen und organisatorischen Maßnahmen nicht unterschritten werden darf. Wesentliche Änderungen sind dem Auftraggeber schriftlich mitzuteilen (Textform ausreichend).

4. Weisungsrecht des Auftraggebers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich gemäß den Weisungen des Auftraggebers, es sei denn, der Auftragnehmer ist gesetzlich zu einer anderen Verarbeitung verpflichtet; in diesem Fall unterrichtet der Auftragnehmer den Auftraggeber vor der Verarbeitung über diese gesetzliche Verpflichtung, es sei denn, das betreffende Recht verbietet eine solche Unterrichtung aufgrund eines wichtigen öffentlichen Interesses.

4.2 Die Weisungen des Auftraggebers richten sich nach (a) den Bestimmungen des Hauptvertrages, (b) dem AV-Vertrag sowie (c) sonstigen Weisungen des Auftraggebers zur Erbringung der vertraglichen Leistungen nach den Bestimmungen des Hauptvertrages, die jeweils schriftlich zu dokumentieren sind (Textform ausreichend). Der Auftraggeber wird mündliche Weisungen unverzüglich schriftlich oder in Textform bestätigen.

4.3 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Auffassung ist, dass eine Weisung gegen geltendes Datenschutzrecht verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der Weisung solange auszusetzen, bis der Auftraggeber die Weisung bestätigt oder abgeändert hat.

5. Betroffenenrechte

5.1 Der Auftraggeber ist als verantwortliche Stelle für die Wahrung der Betroffenenrechte verantwortlich (Art. 15 ff. DSGVO). Der Auftragnehmer informiert den Auftraggeber, wenn betroffene Personen ihre Betroffenenrechte im Zusammenhang mit der Datenverarbeitung gegenüber dem Auftragnehmer geltend machen.

5.2 Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung und Umsetzung von Betroffenenrechten. Dabei wird der Auftragnehmer Betroffenenrechte nicht eigenmächtig, sondern nur auf dokumentierte Weisung des Auftraggebers erfüllen. Für die Unterstützung des Auftraggebers bei der Erfüllung von Betroffenenrechten kann der Auftragnehmer eine angemessene Vergütung verlangen.

5.3 Soweit dies im Rahmen der Funktionalitäten der im Rahmen der Leistungserbringung zur Verfügung gestellten Systeme möglich ist, wird der Auftraggeber personenbezogene Daten selbst beauskunften, berichtigen, löschen oder einschränken.

6. Meldungen von Sicherheitsverletzungen

6.1 Der Auftragnehmer gestaltet die Datenverarbeitung, seine Betriebsabläufe und die damit verbundenen Prozesse, Systeme und Einrichtungen so, dass der Auftragnehmer mögliche Verletzungen des Schutzes personenbezogener Daten erfassen, erkennen und melden kann.

6.2 Der Auftragnehmer benachrichtigt den Auftraggeber unverzüglich, wenn eine Verletzung des Schutzes personenbezogener Daten i.S.d. Art. 4 Nr. 12 DSGVO vorliegt, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten geführt hat.

6.3 Die Benachrichtigung durch den Auftragnehmer erfolgt in einer Weise, die es dem Auftraggeber ermöglicht, seinen gesetzlichen Verpflichtungen, insbesondere gemäß Art. 33 und 34 DSGVO, nachzukommen. Der Auftragnehmer dokumentiert die relevanten Informationen und stellt sie dem Auftraggeber für weitere Maßnahmen zur Verfügung.

7. Pflichten des Auftragnehmers

7.1 Zur Wahrung der Vertraulichkeit setzt der Auftragnehmer bei der Verarbeitung personenbezogener Daten nur Personen ein, die auf die Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die mit den für sie relevanten Datenschutzbestimmungen vertraut gemacht wurden.

7.2 Der Auftragnehmer unterstützt den Auftraggeber in dem nach der Art der Datenverarbeitung erforderlichen und angemessenen Umfang bei der Sicherstellung der Einhaltung der gesetzlichen Pflichten, insbesondere bei der Durchführung von Datenschutzfolgeabschätzungen gem. Art. 35 DSGVO und bei erforderlichen Konsultationen mit den zuständigen Aufsichtsbehörden gem. Art. 36 DSGVO.

7.3 Der Datenschutzbeauftragte des Auftragnehmers ist unter folgenden Kontaktdaten erreichbar:

DataCo GmbH
Dachauer Straße 65
80335 München
Deutschland

+49 89 7400 45840
www.dataguard.de

7.4 Der Auftragnehmer wird den Auftraggeber unverzüglich über Maßnahmen und Überprüfungen einer Aufsichtsbehörde oder sonstige behördliche Anfragen im Zusammenhang mit der Datenverarbeitung unterrichten. Soweit der Auftraggeber seinerseits Maßnahmen und Überprüfungen einer Aufsichtsbehörde ausgesetzt ist, wird der Auftragnehmer den Auftraggeber im erforderlichen und zumutbaren Umfang bei der Beantwortung unterstützen und ihm in diesem Zusammenhang alle relevanten Informationen zur Verfügung stellen. Für die Unterstützung des Auftraggebers kann der Auftragnehmer eine angemessene Vergütung verlangen.

7.5 Der Auftragnehmer überprüft regelmäßig seine internen Prozesse sowie die technischen und organisatorischen Maßnahmen (vgl. Anlage 2), um sicherzustellen, dass die Datenverarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen (a) der anwendbaren datenschutzrechtlichen Bestimmungen sowie (b) den Bestimmungen des AV-Vertrages erfolgt.

7.6 Der Auftragnehmer verarbeitet personenbezogene Daten sowohl (a) innerhalb der Europäischen Union (nachstehend „**EU**“ genannt) bzw. den Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (nachstehend „**EWR**“ genannt) als auch (b) außerhalb der EU bzw. des EWR. Eine Datenverarbeitung außerhalb der EU bzw. des EWR erfolgt durch den Auftragnehmer nur dann, wenn die besonderen Schutzbestimmungen der Art. 44 ff. DSGVO erfüllt sind, um ein angemessenes Datenschutzniveau sicherzustellen (z.B. angemessenes Datenschutzniveau auf Grundlage eines Angemessenheitsbeschlusses der Europäischen

Kommission gem. Art. 45 DSGVO und/oder durch den Abschluss von EU-Standardvertragsklauseln gem. Art. 46 Abs. 2 lit. c und d in Verbindung mit Art. 47 DSGVO).

8. Unterauftragsverarbeitung

8.1 Eine Auftragsdatenverarbeitung im Sinne dieser Ziffer 8 liegt vor, wenn der Auftragnehmer im Rahmen der Leistungserbringung nach Maßgabe des Hauptvertrages andere Auftragnehmer (nachfolgend „**Unterauftragsverarbeiter**" genannt) ganz oder teilweise mit der Verarbeitung personenbezogener Daten beauftragt. Hiervon nicht erfasst sind etwaige Nebenleistungen, die der Auftragnehmer in Anspruch nimmt (z.B. Telekommunikations-, Transport-, Reinigungs- oder Bewachungsleistungen). Der Auftragnehmer trifft jedoch auch bei der Auslagerung von Nebenleistungen angemessene vertragliche Regelungen und Kontrollmaßnahmen, um den Datenschutz und die Datensicherheit zu gewährleisten.

8.2 Die derzeit vom Auftragnehmer eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt. Der Auftraggeber hat die in **Anlage 3** aufgeführten Unterauftragsverarbeiter zur Kenntnis genommen und stimmt dem Einsatz dieser Unterauftragsverarbeiter im Rahmen der Leistungserbringung zu.

8.3 Die Beauftragung neuer bzw. die Änderung bestehender Unterauftragsverarbeiter gemäß **Anlage 3** ist zulässig, wenn der Auftragnehmer dem Auftraggeber den Einsatz des Unterauftragsverarbeiters vorher schriftlich (Textform ausreichend) mitteilt und der Auftraggeber nicht innerhalb einer angemessenen Frist, die dreißig (30) Tage nicht überschreiten darf, widerspricht, wobei ein Widerspruch des Auftraggebers stets nur aus wichtigem Grund möglich ist. Erfolgt kein Widerspruch, gilt die Beauftragung oder Änderung des Unterauftragsverarbeiters als vom Auftraggeber genehmigt. Soweit ein Widerspruch des Auftraggebers aus wichtigem Grund vorliegt und die Parteien keine einvernehmliche Lösung hinsichtlich des betroffenen Unterauftragsverarbeiters erzielen, kann der Auftragnehmer nach seiner Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer unzumutbar ist - die Leistung gegenüber dem Auftraggeber innerhalb von zwei (2) Wochen nach Zugang des Widerspruchs fristlos zum Quartalsende kündigen. Im Falle der Kündigung ist die Leistung bis zum Vertragsende ohne die beabsichtigte Änderung zu erbringen.

8.4 Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf nur erfolgen, wenn der Auftragnehmer mit dem Unterauftragsverarbeiter eine Vereinbarung gem. Art. 28 DSGVO abgeschlossen hat, die mit den Regelungen dieses AV-Vertrages grundsätzlich vergleichbare Datenschutzbestimmungen enthält. Insbesondere stellt der Auftragnehmer sicher,

dass ausreichende Garantien für die Umsetzung der technischen und organisatorischen Maßnahmen bestehen.

8.5 Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU bzw. des EWR, gilt Ziffer 7.6 entsprechend.

8.6 Der Auftragnehmer bleibt dem Auftraggeber gegenüber für die Erfüllung der Verpflichtungen des beauftragten Unterauftragsverarbeiters verantwortlich.

9. Kontrollrechte des Auftraggebers

9.1 Der Auftraggeber ist berechtigt, die Einhaltung (a) der anwendbaren datenschutzrechtlichen Bestimmungen sowie (b) der Bestimmungen des AV-Vertrages, insbesondere hinsichtlich der technischen und organisatorischen Maßnahmen, zu überprüfen. Nach Maßgabe dieser Ziffer 9 wird der Auftragnehmer dem Auftraggeber in seinem Verantwortungsbereich alle zum Nachweis der Einhaltung der anwendbaren datenschutzrechtlichen Bestimmungen erforderlichen Auskünfte erteilen und Kontrollen der Datenverarbeitung im Rahmen der nachfolgenden Datenverarbeitung ermöglichen und unterstützen.

9.2 Soweit im Einzelfall die Überprüfung (a) der Einhaltung der anwendbaren datenschutzrechtlichen Bestimmungen oder (b) der Bestimmungen des AV-Vertrages erforderlich ist, hat der Auftraggeber das Recht, nach Abstimmung mit dem Auftragnehmer entsprechende Überprüfungen in den jeweiligen Betriebsstätten des Auftragnehmers, in denen die Datenverarbeitung erfolgt, selbst oder durch im Einzelfall zu bestimmende, geeignete und zur Verschwiegenheit verpflichtete Prüfer durchzuführen oder durchführen zu lassen. Die Überprüfung ist auf die Verarbeitung personenbezogener Daten zu beschränken und ohne vermeidbare Störung des Auftragnehmers durchzuführen. Der Auftragnehmer ist berechtigt, der Auswahl des Prüfers aus wichtigem Grund (z.B. Unzuverlässigkeit oder Wettbewerbsverhältnis zum Auftragnehmer) zu widersprechen. Außer bei Vorliegen dringender, sachlich gerechtfertigter Gründe, die vom Auftraggeber entsprechend zu dokumentieren sind, werden Überprüfungen in den Geschäftsräumen des Auftragnehmers nach angemessener Vorankündigung von mind. einem (1) Monat während der normalen Geschäftszeiten des Auftragnehmers und höchstens alle zwölf (12) Monate durchgeführt. Für die Unterstützung bei der Durchführung der Überprüfung kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Aufwand für eine Überprüfung ist für den Auftraggeber grundsätzlich auf einen (1) Tag pro Kalenderjahr begrenzt.

9.3 Die Parteien gehen übereinstimmend davon aus, dass Überprüfungen des Auftraggebers und die Erteilung von Auskünften und Nachweisen durch den Auftragnehmer in erster Linie in der Weise erfolgen, dass der Auftragnehmer dem Auftraggeber aktuelle Testate, Berichte oder

Berichtsauszüge unabhängiger Dritter (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutz- oder Qualitätsauditoren) oder entsprechende Zertifizierungen durch IT-Sicherheits- oder Datenschutzaudit vorlegt.

10. Löschung von personenbezogenen Daten und Rückgabe von Datenträgern

10.1 Ohne Wissen des Auftraggebers werden keine Kopien oder Duplikate von personenbezogenen Daten angefertigt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Mit Beendigung des AV-Vertrages (oder vorher nach entsprechender Weisung des Auftraggebers) hat der Auftragnehmer alle in seinem Besitz befindlichen personenbezogenen Daten an den Auftraggeber herauszugeben oder nach Wahl des Auftraggebers datenschutzgerecht zu vernichten, soweit der Auftragnehmer nicht aufgrund gesetzlicher Vorschriften zur weiteren Speicherung der Daten verpflichtet ist. Die Löschung bzw. Vernichtung ist dem Auftraggeber in Textform zu bestätigen.

10.3 Die Parteien vereinbaren, dass mit Beendigung des Hauptvertrages eine automatische Löschung der Daten gemäß Ziffer 10.2 erfolgt, es sei denn, der Auftraggeber fordert ab Zugang der Kündigung bis spätestens 14 Tage vor der Beendigung des Hauptvertrages beim Auftragnehmer die Herausgabe seiner Daten an. Die Bestätigungsfrist gemäß Ziffer 10.2 gilt entsprechend.

11. Schlussbestimmungen

11.1 Änderungen und Ergänzungen des AV-Vertrages bedürfen der Schriftform (Textform mit elektronischer Signatur ausreichend). Dies gilt auch für den Verzicht auf das Schriftformerfordernis. Soweit Änderungen des AV-Vertrages erforderlich sind oder werden, um den Anforderungen des geltenden Datenschutzrechts zu genügen, werden sich die Parteien rechtzeitig hierüber verständigen.

11.2 Sollten eine oder mehrere Bestimmungen des AV-Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die Parteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung gemeinsam durch eine wirksame zu ersetzen, die dem von den Parteien Gewollten wirtschaftlich am nächsten kommt. Entsprechendes gilt für etwaige Lücken des AV-Vertrages. Die Parteien sind sich darüber einig, dass diese Regelung keine bloße Beweislastumkehr darstellt, sondern vielmehr § 139 BGB ausdrücklich abbedungen wird.

11.3 Der AV-Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

Anlage 1 – Beschreibung der Auftragsverarbeitung

1. Art der Verarbeitung

Die Auftragsverarbeitung erfolgt zu folgenden Zwecken:

- Erheben*, Erfassen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleichen oder Verknüpfen, Einschränken, Löschen oder Vernichten von personenbezogenen Daten im Zusammenhang mit der Bereitstellung, dem Betrieb, der Betreuung und der Wartung der remberg Anything-Relationship-Management (XRM) Software für den Auftraggeber und seine Nutzer nach Maßgabe der Bestimmungen des Hauptvertrages*

2. Kategorien personenbezogener Daten, die verarbeitet werden

Die Auftragsverarbeitung umfasst folgende Datenkategorien:

- *Personalstammdaten (insb. Name, E-Mail-Adresse, Telefonnummer)*
- *Firmendaten (insb. Firmenname, Webseite, Adresse, Land, IP-Adresse)*
- *Kommunikationsdaten (insb. Protokolle der Nutzung der Software sowie getätigter Änderungen an Daten)*
- *Vertragsabrechnungs- und Zahlungsdaten*

3. Verarbeitete sensible Daten (falls zutreffend)

Die Auftragsverarbeitung umfasst folgende sensible Daten (Art. 9 DSGVO)

- *N/A*

4. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Die Auftragsverarbeitung betrifft die folgenden Kategorien betroffener Personen:

- *Mitarbeiter – freie und angestellte – des Auftraggebers oder falls zutreffend, eines mit ihm verbundenen Unternehmens*
- *Ehemalige Mitarbeiter – freie und angestellte – des Auftraggebers oder falls zutreffend, eines mit ihm verbundenen Unternehmens*
- *Mitarbeiter – freie und angestellte – der Kunden des Auftraggebers*
- *Mitarbeiter – freie und angestellte – der Interessenten des Auftraggebers*

5. Dauer *der Verarbeitung*

Die Auftragsverarbeitung hat folgenden Zeitraum:

- *Die Datenverarbeitung erfolgt für die Dauer des Hauptvertrages*

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

- **Zutrittskontrolle**

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

  Die Verarbeitung erfolgt in den Rechenzentren von Amazon Web Services. AWS ist für die physische Sicherheit verantwortlich. Zu den Maßnahmen gehören u.a. 24/7 Sicherheitsdienst, biometrische Zugangskontrollen, Videoüberwachung und strikte Zutrittsprotokollierung. Die Einhaltung wird durch SOC- und ISO-Zertifikate belegt.

  Zu unseren eigenen Geschäftsräumen gilt:

  - Alarmanlage
  - Elektrische Türöffner
  - Schlüsselregelung
  - Sorgfältige Auswahl von Reinigungspersonal
  - Regelung in Bezug auf Datenschutz mit Reinigungspersonal
  - Gäste sind stetig in Begleitung von Mitarbeitern
  - Protokollierung von Besuchern
  - Anweisung, Fenster und Türen außerhalb der Arbeitszeit zu schließen

- **Zugangskontrolle**

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

  - Zuordnung von Benutzerrechten

- Passwortvergabe & Authentifizierung mit Benutzername / Passwort
- Einsatz von Multi-Faktor-Authentifizierung
- Einsatz von Anti-Viren Software
- Automatische Desktopsperre
- BIOS-Schutz (separates Passwort)
- Einsatz eines VPN bei Remote-Zugriffen
- Firewall
- Mobile Device Management
- Schlüsselregelung
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Verschlüsselung von mobilen Endgeräten
- Verschlüsselung von mobilen Datenträgern
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Richtlinie zum Datenschutz und / oder Sicherheit
- Richtlinie zur IT-Sicherheit
- Richtlinie „Sicheres Passwort“
- Anleitung „Manuelle Desktopsperre“
- Verwaltung von Benutzerberechtigungen
- Vergabe rollenbasierter Benutzerberechtigungen („Need to Know“)

- Mobile Device Policy
- Richtlinie „Clean desk“
- Richtlinie „Löschen / Vernichten“
- Sorgfältige Auswahl von Reinigungspersonal

- **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.

  - Einsatz von Berechtigungskonzepten
  - Verwaltung der Rechte durch Systemadministratoren
  - Sichere Aufbewahrung von Datenträgern
  - Es existiert eine strenge Passwortrichtlinie inkl. Passwortlänge
  - Anzahl der Administratoren auf das “Notwendigste” reduziert.
  - Bedarfsgerechte Zugriffsrechte
  - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  - Datenschutzkonformer Aktenschredder (gem. ISO/IEC 21964; mind. Stufe 4, cross cut)
  - Gesicherte Schnittstellen (USB, Firewire, Netzwerk, etc.)
  - Physische und datenschutzkonforme Löschung von Datenträgern

- **Trennung**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Getrennte Ordnerstrukturen (Auftragsverarbeitung)
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)
- Festlegung von Datenbankrechten
- Steuerung über Berechtigungskonzept

2. Integrität

- **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.

  - Dokumentenmanagement
  - Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
  - Manuelle oder automatisierte Kontrolle der Protokolle
  - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
  - Klare Zuständigkeiten für Löschungen
  - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
  - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

- **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.

  - E-Mail-Verschlüsselung
  - Bereitstellung über verschlüsselte Verbindungen wie z.B. SSL-Verschlüsselung (SFTP, HTTPS)
  - Einrichtung von Standleitungen bzw. VPN-Tunneln (Virtual Private Network)
  - Nutzung von Signaturverfahren, wie elektronischer Signatur
  - Protokollierung von Zugriffen und Abrufen
  - Regelung für eine datenschutzgerechte Vernichtung von Daten
  - Regelung zur Vermeidung der Erstellung physischer Datenkopien

3. Verfügbarkeit und Belastbarkeit

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

Da unsere Dienste auf Amazon Web Services (AWS) gehostet werden, wird die physische Verfügbarkeit und Belastbarkeit der Infrastruktur vollständig durch AWS sichergestellt. AWS setzt modernste Redundanzkonzepte ein, darunter unterbrechungsfreie Stromversorgung (USV), Notstromaggregate und redundante Netzwerkanbindungen über räumlich getrennte Verfügbarkeitszonen hinweg, was regelmäßig nach ISO 27001 und SOC 2 auditiert wird. Dies wird ergänzt durch automatisierte Backup-Strategien, kontinuierliches Monitoring der Systemleistung sowie den Einsatz von Skalierungsmechanismen (z. B. Auto-Scaling), um die Stabilität und

Erreichbarkeit der Anwendungen auch bei hohen Lastspitzen oder Hardwareausfällen zu garantieren.

- Klimaanlage in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- Feuer- und Rauchmeldeanlagen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellung eines Backup- & Recovery-Konzepts
- Testen von Datenwiederherstellung
- Kontrolle des Sicherungsvorgangs
- Existenz eines Notfallplans

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Datenschutz-Maßnahmen**

  Maßnahmen, die gewährleisten, dass die getroffenen technischen und organisatorischen Maßnahmen noch wirksam sind. Dies muss regelmäßig stattfinden.

  - Mind. Jährliche Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen
  - Sicherheitszertifizierung nach ISO 27001
  - Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet, …)
  - Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
  - Organisation kommt Informationspflichten nach Art. 13 und 14 DSGVO nach
  - Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

- **Incident-Response-Management**

  Maßnahmen, die bei der Reaktion auf Sicherheitsverletzungen unterstützen.

  - Einsatz von Firewall(s) und regelmäßige Aktualisierung
  - Einsatz von Spamfilter(n) und regelmäßige Aktualisierung
  - Einsatz von Virenscanner(n) und regelmäßige Aktualisierung
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - Dokumentierter Meldeprozess von Datenpannen und Sicherheitsvorfällen
  - Dokumentierter Prozess zum Umgang mit Sicherheitsvorfällen
  - Dokumentation von Datenpannen und Sicherheitsvorfällen
  - Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

- **Datenschutzfreundliche Voreinstellungen**

  Maßnahmen zur Datenvermeidung und Datensparsamkeit.

  - Beschränkung der Verarbeitung auf für den Zweck erforderliche personenbezogene Daten
  - Einfache Ausübung des Widerrufsrechts von Betroffenen durch technische Maßnahmen
  - Schulung/Sensibilisierung der Mitarbeiter
  - Richtlinie zur Entwicklung von Apps/Tools etc.

- **Technische und Organisatorische Maßnahmen für Telearbeit**

  Maßnahmen, die gewährleisten, dass die Verarbeitung von personenbezogenen Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. im Rahmen von Telearbeit, Heimarbeit, Homeoffice, mobilem Arbeiten) unter Einhaltung eines angemessenen Datenschutzniveaus erfolgt.

- Anmeldeverfahren mit Nutzernamen und Passwort
- Automatische Desktopsperre
- Anleitung „Manuelle Desktopsperre“
- Mobile Device Policy
- Richtlinie zum Datenschutz im Homeoffice, etc.
- Vorgabe „Clean desk“ auch für Arbeit im Homeoffice / bei Telearbeit etc.
- Vorgabe „Sicheres Passwort“ speziell auch für Arbeit im Homeoffice / bei Telearbeit etc.
- Vorgabe der Vermeidung von Ausdrucken in Papierform
- Vorgabe Telefonate mit Personenbezug ohne Mithören Dritter zu führen
- Vorgabe Daten möglichst nicht lokal oder auf mobilen Speichermedien zu sichern

Für weitere Informationen dazu, welche technischen und organisatorischen Maßnahmen unsere Unterauftragsverarbeiter treffen, siehe bitte die referenzierten Datenschutzinformationen in **Anlage 3**.

Anlage 3 – Unterauftragsverarbeiter

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten (Unterauftragsverarbeiter).

Die aktuelle Liste von Unterauftragsverarbeitern ist hier zu finden: remberg.com/de/unterauftragnehmer