Institut für
Datenschutz und
Datensicherheit

Vertrag zur Auftragsverarbeitung

zwischen

Verantwortlicher (Firma)
Straße, Hausnummer
PLZ, Ort
Deutschland

als Verantwortlicher (hier bezeichnet als „**Auftraggeber**“)

und

Weise Software GmbH
Bamberger Str. 4 - 6
01187 Dresden
Deutschland

als Auftragsverarbeiter (hier bezeichnet als „**Auftragnehmer**“)

1. Allgemeines

1.1. Im Rahmen der Leistungserbringung verarbeitet der Auftragnehmer (im Wartungsfall ggf.) personenbezogene Daten für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften ist („Auftraggeber-Daten“). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 und Art. 28 (DSGVO).

1.2. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Laufzeit und Kündigung des Vertrags

2.1. Die Dauer der Verarbeitung entspricht der Laufzeit der Leistungserbringung, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Aufbewahrung bzw. Speicherung der Auftraggeber-Daten besteht.

2.2. Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung gemäß der Leistungserbringung.

3. Gegenstand des Auftrags

3.1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers. Der Auftraggeber bleibt Verantwortlicher im Sinne des Art. 4 Nr.7 DSGVO.

3.2. Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.

3.3. Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine Ausnahme nach Art. 49 DSGVO vorliegt.

4. Weisungsbefugnisse des Auftraggebers

4.1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten ausschließlich gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen zur Leistungserbringung festgelegt und dokumentiert. Einzelweisungen, die von diesen Festlegungen abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers. Die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber ist in diesem Fall gesondert zu vereinbaren.

4.3. Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, oder kann der Auftragnehmer darlegen, dass eine Verarbeitung gemäß Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, teilt er dies dem Auftraggeber unverzüglich mit und ist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber und einer Klärung der Haftung zwischen den Parteien auszusetzen.

5. Pflichten und Verantwortlichkeiten des Auftraggebers

5.1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

5.2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

5.3. Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

5.4. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5.5. Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

5.6. Der Auftraggeber sensibilisiert seine mit der Verarbeitung betrauten Mitarbeiter dahingehend, vor etwaigen Wartungsmaßnahmen durch den Auftragnehmer Dokumente und sonstige Prozesse (z.B. nicht den Auftrag betreffende Software), bei denen der Zugriff des Auftragnehmers auf personenbezogene Daten nicht ausgeschlossen werden kann, nach Möglichkeit zu vermeiden.

6. Maßnahmen zur Sicherheit der Verarbeitung

6.1. Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

6.2. Der Auftragnehmer bestätigt, einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt zu haben. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Datenschutzbeauftragte des Auftragnehmers kann unter der E-Mail-Adresse weise-software@ifdds.eu, oder unter der Telefonnummer +49 351 27 57 90 57 erreicht werden.

6.3. Der Auftragnehmer hat alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere die in **Anlage 2** aufgeführten Maßnahmen zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme getroffen. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen und mindestens dasselbe mit Vertragsschluss festgelegte Datenschutzniveau eingehalten wird.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus

Anlage 3. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

7.2. Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, die Leistungserbringung und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

7.3. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist und dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

7.4. Unter Einhaltung der Anforderungen der Ziffer 3.3 dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird.

8. Rechte der betroffenen Personen

8.1. Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich.

8.2. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.3. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

8.4. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.5. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.6. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1. Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber unverzüglich über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten unterstützen.

9.2. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO, sowie beim zur Verfügung stellen der Informationen für die Einhaltung der in den Art. 32 DSGVO genannten Pflichten unterstützen.

9.3. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

9.4. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

9.5. Zur Durchführung von Inspektionen nach Ziffer 9.4 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten nach rechtzeitiger Vorankündigung gemäß Ziffer 9.7 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.

9.6. Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

9.7. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

9.8. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 9 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

9.9. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach ISO 27001 – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

10. Datenlöschung

10.1. Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren und dem Auftraggeber auf dessen Nachfrage schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10.2. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

11. Haftung

11.1. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

11.2. Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

12. Schlussbestimmungen

12.1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

12.2. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, gehen die Regelungen dieses Vertrags vor.

12.3. Es gilt deutsches Recht.

12.4. Diese Vereinbarung umfasst die folgenden Anlagen, die Bestandteil des Vertrages sind:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Subauftragnehmer

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Gilt im Falle der Leistungserbringung „Wartungsmaßnahmen“

Angaben zur Datenverarbeitung	
Zweck der Verarbeitung	Im Rahmen einer Leistungsvereinbarung kann es notwendig sein, dass der Auftragnehmer Zugriff auf das System des Auftraggebers erhält, um für den ordnungsgemäßen Betrieb Sorge zu tragen. Im Rahmen der Tätigkeiten des Auftragnehmers ist nicht ausgeschlossen, dass der Auftragnehmer dabei auch Zugriff auf personenbezogene Daten des Auftraggebers erhält.
Art und Umfang der Verarbeitungsprozesse	(flüchtige) Speicherung, Offenlegung durch Übermittlung (durch Auftraggeber)
Kategorien der personenbezogenen Daten	• Ggf. Name, Vorname (Ansprechpartner oder Kunde von Auftraggeber) • Darüber hinaus ist nicht ausgeschlossen, dass weitere personenbezogene Daten zur Kenntnis gelangen (z.B. aufgrund geöffneter Dokumente auf dem Client).
Kategorien von Betroffenen	• Ggf. Ansprechpartner oder Kunde von Auftraggeber • Darüber hinaus ist nicht ausgeschlossen, dass weitere Personenkategorien zur Kenntnis gelangen (z.B. aufgrund geöffneter Dokumente auf dem Client).
Dauer der Speicherung der personenbezogenen Daten	Die Löschung erfolgt systemseitig unmittelbar nach der jeweiligen Wartung.

Gilt im Falle der Leistungserbringung „Brandschutznachweis“

Angaben zur Datenverarbeitung	
Zweck der Verarbeitung	
Art und Umfang der Verarbeitungsprozesse	
Kategorien der personenbezogenen Daten	• Login Daten (Benutzername, Passwort gehasht, mit Salt) • IP-Adresse des Nutzers • Name, Vorname • Titel

	• Firma • Firmenanschrift • Kontaktdaten (Telefon, Fax, E-Mail, Mobil) • Berufsbezeichnung • Listennr. / Mitgliedsnummer • Webseite • Anrede
Kategorien von Betroffenen	• Mitarbeiter des Auftraggebers • Bauherr • Aufsteller des Brandschutznachweises

Anlage 2: Technische und organisatorische Maßnahmen

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. a DSGVO

1.1. Zutrittskontrolle

- Alarmanlage
- Chipkarten / Transpondersysteme
- Manuelles Schließsystem
- Sicherheitsschlösser
- Türen mit Knauf Außenseite
- Videoüberwachung der Eingänge
- Schlüsselregelung
- Empfang
- Besucher in Begleitung durch Mitarbeiter
- Sorgfalt bei Auswahl des Wachpersonals
- Sorgfalt bei Auswahl Reinigungsdienste

1.2. Zugangskontrolle

- Login mit Benutzername + Passwort (Passwort-Policy gemäß NIST-Richtlinien)
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Firewall
- Verwalten von Benutzerberechtigungen für die firmeninterne Kundendatenbank

1.3. Zugriffskontrolle

- Aktenvernichter
- Externer Vernichter von DVD-Datenträgern
- Einsatz Berechtigungskonzepte in Bezug auf die firmeninterne Kundendatenbank
- Datenschutztresor
- Verwaltung Benutzerrechte durch Administratoren

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen

2.2. Eingabekontrolle

- Protokollierung bestimmter Systemereignisse

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

- Rauchmeldeanlage im Serverraum
- Serverraum klimatisiert
- Schutzsteckdosenleisten Serverraum
- Datenschutztresor
- Alarmmeldung bei unberechtigtem Zutritt zu Serverraum

- Backup & Recovery-Konzept
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten
- Regelmäßiger Sicherheitscheck des Netzes
- Virenschutzsystem

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

- Bestellung externer Datenschutzbeauftragter
- Regelmäßige Sensibilisierung der Mitarbeiter
- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

4.2. Auftragskontrolle

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere in Bezug auf Datenschutz und Datensicherheit)

Anlage 3: Subauftragnehmer

Gilt im Falle der Leistungserbringung „Wartungsmaßnahmen“

Subauftragnehmer	Anschrift	Leistungen	Drittlandübermittlungen	Rechtsgrundlage bei Drittlandübermittlung
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen Deutschland	• Software zur Fernwartung	nein	-

Gilt im Falle der Leistungserbringung „Brandschutznachweis“

Subauftragnehmer	Anschrift	Leistungen	Drittlandübermittlungen	Rechtsgrundlage bei Drittlandübermittlung
keine		•		