
Vertrag
über die Auftragsverarbeitung
gem. Art. 28 Datenschutzgrundverordnung (DS-GVO)

zwischen

vertreten durch

– Verantwortlicher –

nachstehend „**Auftraggeber**“ genannt

und

befine Solutions AG

Schwarzwaldstr. 151

79102 Freiburg

vertreten durch **Herr Oliver Kenk (CFO)**

– Auftragsverarbeiter –

nachstehend „**Auftragnehmer**“ genannt

gemeinsam im Folgenden auch

„**Vertragsparteien**“ genannt.

Inhaltsverzeichnis:

Präambel	3
1 Gegenstand und Dauer des Auftrags.....	3
2 Konkretisierung des Auftragsinhalts.....	4
3 Technisch-organisatorische Maßnahmen	5
4 Berichtigung, Einschränkung und Löschung von Daten	6
5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers	6
6 Unterauftragsverhältnisse	7
7 Kontrollrechte des Auftraggebers.....	8
8 Mitteilung bei Verstößen des Auftragnehmers.....	8
9 Weisungsbefugnis des Auftraggebers	9
Anlage 1 (Technisch- organisatorische Maßnahmen gem. DS-GVO)	10

Präambel

Zwischen dem Auftraggeber und dem Auftragnehmer besteht in tatsächlicher oder rechtlicher Hinsicht eine Zusammenarbeit über Leistungen im IT-Umfeld („Hauptvertrag“). Da es im Rahmen der Durchführung dieses Hauptvertrages zumindest nicht ausgeschlossen ist, dass der Auftragnehmer Zugriff auf oder Einsicht in personenbezogene Daten des Auftraggebers erhält, bedarf es einer Vereinbarung über die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (Auftragsverarbeitung).

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 S. 2 lit. a DS-GVO).

1 Gegenstand und Dauer des Auftrags

1.1. Gegenstand (Art. 28 Abs. 3 S. 1 DS-GVO)

- Der Gegenstand des Auftrags ergibt sich aus der beigefügten Leistungsvereinbarung, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

- Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
- ✓ Unterstützung bei Installation/Konfiguration der Software
 - ✓ Leisten eines Hotlinesupports während der Laufzeit des Hauptvertrags
 - ✓ Verschlüsselung, Übertragung und Speicherung von elektronischen Daten mittels Cryptshare, gemäß Produktbeschreibung

1.2. Dauer des Auftrags (Art. 28 Abs. 3 S. 1 DS-GVO)

- Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags

oder

- Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum

oder

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von zum gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2 Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten (Art. 28 Abs. 3 S. 1 DS-GVO)

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Hauptvertrag.

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus der beigefügten Leistungsvereinbarung

oder

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: ...

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

2.2. Art der Daten

Die Art der verwendeten personenbezogenen Daten ist in der beigefügten Leistungsvereinbarung konkret beschrieben.

oder

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

Personenstammdaten

Kommunikationsdaten (z.B. Telefon, E-Mail, IP-Adresse)

Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

Kundenhistorie

Vertragsabrechnungs- und Zahlungsdaten

Planungs- und Steuerungsdaten

-
- Auskunftangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
 - Im Rahmen der Supportleistung (Fernwartung oder persönlich vor Ort) kann gegebenenfalls, bestimmt durch das Kundenverhalten, Einblick in jede denkbare Form personenbezogener Daten kurzzeitig entstehen

2.3. Kategorien betroffener Personen

- Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der beigefügten Leistungsvereinbarung konkret beschrieben unter.

oder

- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
 - (Firmen-)Kunden
 - Interessenten
 - Abonnenten
 - Beschäftigte
 - Lieferanten
 - Handelsvertreter
 - Ansprechpartner
 - Mitarbeiter
 - Im Rahmen der Supportleistung (Fernwartung oder persönlich vor Ort) kann gegebenenfalls, bestimmt durch das Kundenverhalten, jede denkbare Person betroffen sein
 - ...

3 Technisch-organisatorische Maßnahmen

- 3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- 3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Die Einzelheiten sind in **Anlage 1** genannt.

-
- 3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4 Berichtigung, Einschränkung und Löschung von Daten

- 4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- 4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- 5.1 Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- a. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme über die Homepage des Unternehmens zur Verfügung gestellt. Ein Wechsel des Datenschutzbeauftragten wird über die Homepage bekannt gegeben.
 - b. Die jeweils aktuellen Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich unter folgendem Link hinterlegt: <https://www.befine-solutions.com/datenschutz.html>
- 5.2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- 5.3 Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO. Die Einzelheiten sind in Anlage 1 genannt.
- 5.4 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 5.5 Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- 5.6 Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- 5.7 Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- 5.8 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6 Unterauftragsverhältnisse

- 6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- 6.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
- Eine Unterbeauftragung ist unzulässig
- Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Nr.	Unterauftragnehmer (Firma, Anschrift)	Land	Leistung
1	Equinoxe GmbH Bismarckallee 9 79098 Freiburg i.Brg.	Deutschland	Hostingpartner für den Betrieb von Cryptshareservern (auch Demoserver)
2	TeamViewer GmbH	Deutschland	Fernwartungstool zur Einsichtnahme der Desktopoberfläche des Auftraggebers

- Die Hinzuziehung weiterer Unterauftragnehmer oder die Ersetzung bestehender Unterauftragnehmer sind zulässig, soweit:
- der Auftragnehmer eine solche Hinzuziehung oder Ersetzung dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
 - der Auftraggeber der Hinzuziehung oder Ersetzung nicht innerhalb von 14 Tagen nach Zugang der Information, jedoch nur aus wichtigem Grund, widerspricht.
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

-
- 6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- 6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- 6.5 Eine weitere Auslagerung durch den Unterauftragnehmer
- ist nicht gestattet;
 - bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
 - bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);
- 6.6 Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7 Kontrollrechte des Auftraggebers

- 7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- 7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen mit geeigneten Mitteln nachzuweisen.
- 7.3 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8 Mitteilung bei Verstößen des Auftragnehmers

- 8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
- a. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
 - b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
 - c. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
 - d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung

- e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- 8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9 Weisungsbefugnis des Auftraggebers

- 9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- 9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
- 9.3 Löschung und Rückgabe personenbezogener Daten
- 9.4 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- 9.5 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- 9.6 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Auftraggeber

Auftragnehmer

Name (in Blockbuchstaben)

befine Solutions AG

Name (in Blockbuchstaben)

Funktion / Titel

Oliver Kenk, CFO

Funktion / Titel

Ort, Datum

Freiburg, den

Ort, Datum

Unterschrift

Unterschrift

Anlage 1 (Technisch- organisatorische Maßnahmen gem. DS-GVO)

zum Vertrag über die Auftragsverarbeitung, zwischen

der

und der **befine Solutions AG** vom

1. Vertraulichkeit (Art. 32 Abs. 1 lit. B DS-GVO)

✓ Zutrittskontrolle

- Die Büroräumlichkeiten sind während und außerhalb der Geschäftszeiten verschlossen und sind nur von einem dafür berechtigten Personenkreis betretbar.
- Außerhalb der Geschäftszeiten sind die Büroräume alarmgesichert.
- Alle Außentüren sind nur mit einem Speziälschlüssel zu öffnen.
- Der Serverraum ist gesondert verriegelt und alarmgeschützt sowie nur von einem erforderlichen Personenkreis betretbar.
- Berechtigte Mitarbeiter erhalten Zugang gegen Vereinbarung einer gesonderten Schlüssel- und Token-Nutzungsvereinbarung, sowie nach Unterzeichnung einer Verschwiegenheitsverpflichtung.

✓ Zugangskontrolle

- Einsatz von Datenverschlüsselung
- Benutzeridentifikation und Passwortverfahren
- Einsatz einer Hardware-Firewall
- Einsatz von Anti-Viren-Software
- Einsatz von VPN-Technologie für den Fernzugriff
- Einsatz von Mobile Device Management
- Verwaltung von Benutzerberechtigungen
- Sorgfältigste Mitarbeiterauswahl bis hin zu Reinigungskräften

✓ Zugriffskontrolle

- Einsatz von Aktenvernichtern
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- Berechtigungskonzept und Zugriffsrechte, angepasst auf Verantwortungsbereiche sowie nach dem need-to-know Prinzip
- Passworrichtlinie
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Die Anzahl der Administratoren des Systems ist auf das Notwendigste beschränkt

✓ Trennungskontrolle

- Produktiv- und Testsystem sind voneinander getrennt
- Es befinden sich keine personenbezogenen Echt-Daten des Auftraggebers auf Entwicklungs- und Testsystemen
- Anwendung eines Berechtigungskonzepts mit unterschiedlichen Zugriffsrechten
- Die Speicherung personenbezogener und nicht-personenbezogener Daten erfolgt in separaten Datenbanken mit unterschiedlichen Zugriffsrechten

2. Integrität (Art. 32 Abs. 1 lit. B DS-GVO)

✓ Weitergabekontrolle

- Nutzung von VPN-Tunneln für den remote-Zugriff von Mitarbeitern auf die Daten
- Nutzung von E-Mail Verschlüsselung und verschlüsselte Dateiübertragung für die Kommunikation mit Kunden
- Im Rahmen des Cryptshare Supports werden personenbezogene Daten grundsätzlich nicht an Dritte weitergegeben.

✓ Eingabekontrolle

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DS-GVO)

✓ Verfügbarkeitskontrolle

- Der Serverraum befindet sich im Gebäude oberhalb der Hochwassergrenze
- Der Serverraum befindet sich nicht unter sanitären Anlagen
- Feuerlöschgeräte befinden sich im Serverraum
- Es existiert ein körperliches Datenbackup-System
- Es werden zwei Serversysteme parallel gefahren

✓ Rasche Wiederherstellbarkeit

- Eine Wiederherstellung bei Datenverlust kann auf Basis der vorhandenen Sicherungseinrichtungen innerhalb von ca. 24 Stunden erfolgen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DS-GVO; Art. 25 Abs 1 DS-GVO)

- ✓ Datenschutz-Management
 - Der Auftragnehmer verfügt über das gesetzlich vorgeschriebene Datenschutz-Management.
- ✓ Incident-Response-Management
 - Verhaltensregeln bei datenschutzrelevanten Ereignissen sind im Intranet des Auftragnehmers stets in aktueller Version veröffentlicht und allen Mitarbeitern zugänglich
- ✓ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
 - Das Unternehmen verfügt über Berechtigungs- und Zutrittskonzepte für den Zugang zu personenbezogenen Daten.
- ✓ Auftragskontrolle
 - Unterauftragnehmer werden unter besonderer Berücksichtigung der gesetzlichen Bestimmungen „Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag“ und somit der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt.
 - Die Erhebung, Verarbeitung und Löschung der Daten erfolgt streng gebunden an Auftrag und Einzelweisungen des Auftraggebers gem. der im Auftragsdatenverarbeitungsvertrag festgehaltenen Vereinbarungen

5. Pseudonymisierung (Art. 32 Abs. 1 lit. B DS-GVO)

- ✓ Personenbezogene Daten, die im Rahmen von Supporttätigkeiten erhoben werden oder anfallen werden durch geeignete technische Maßnahmen pseudonymisiert.
- ✓ Die Pseudonymisierung erfolgt in regelmäßigen Intervallen jeweils zeitnah nach Abschluss der Supporttätigkeiten.