

Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO

Diese Vereinbarung wird getroffen

zwischen dem Verantwortlichen

- nachfolgend **Auftraggeber** -

und dem Auftragsverarbeiter

Dr. Josef Raabe Verlags-GmbH, Rotebühlstr. 77, 70178 Stuttgart, vertreten durch Herrn Dr. Sebastian Hild, Rotebühlstr. 77, 70178 Stuttgart

- nachfolgend **Auftragnehmer** -

- nachfolgend zusammen die **Vertragspartner** -



1. Inhalt, Geltungsbereich, Begriffsbestimmungen

- 1.1 Dieser Vertrag über die Auftragsverarbeitung personenbezogener Daten (im Folgenden „**Vereinbarung**“) regelt die Rechte und die Pflichten von Auftraggeber und -nehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- 1.2 Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.
- 1.3 „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- 1.4 „Verarbeitung“ meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
- 1.5 „Verantwortlicher“ ist diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
- 1.6 „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- 1.7 Die in dieser Vereinbarung verwendeten Begriffe sind entsprechend ihrer Definition in der EU-Datenschutz-Grundverordnung (im Folgenden „**DS-GVO**“) zu verstehen.

2. Gegenstand und Dauer der Verarbeitung

- 2.1 Der Auftragnehmer stellt dem Auftraggeber die App „Büffelbiest“ zur Verfügung. Dabei handelt es sich um eine Lernplattform, in der Lehrer:innen Lehrereinheiten konzipieren und ihren Schüler:innen zur Verfügung stellen sowie zur Bearbeitung zuweisen können.
- 2.2 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des bestehenden Vertragsverhältnisses und tritt mit Unterzeichnung durch beide Vertragspartner in Kraft. Sie endet, sobald die App „Büffelbiest“ nicht mehr durch den Auftragnehmer bereitgestellt wird oder werden kann.
- 2.3 Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Art und Zweck der Verarbeitung

- 3.1 Die Verarbeitung dient dem Zweck der Bereitstellung aller Inhalte und Services der App „Büffelbiest“.
- 3.2 Bei der Nutzung von „Büffelbiest“ werden folgende Arten von personenbezogenen Daten erhoben und verarbeitet:
 - Personenstammdaten (z.B. Vor- und Nachname der Lehrer:innen)
 - (berufliche) E-Mail-Adresse der Nutzer:innen
 - Schulzugehörigkeit
 - Leistungsdaten der Schüler:innen (Lernfortschritt, Abschlussrate von Lerneinheiten, ...)
 - Technische Daten (z.B. IP-Adresse, IMEI, ...)
- 3.3 Von der Verarbeitung betroffen sind alle Nutzer:innen von „Büffelbiest“, dabei handelt es sich vor allem um Lehrende und Schüler:innen.

4. Dokumentierte Weisung

- 4.1 Der Auftragnehmer darf Daten nur im Rahmen des Auftrags und nach Weisungen des Auftraggebers verarbeiten.
- 4.2 Der Auftraggeber ist als Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit und nach Beendigung dieser Vereinbarung Weisungen an den Auftragnehmer erteilen.
- 4.3 Jede Weisung des Auftraggebers bedarf mindestens der Textform (z.B. Brief, Fax, E-Mail, SMS, Chatnachricht) und muss nachvollziehbar dokumentiert werden. Es muss stets nachvollzogen werden können, wann von wem eine Weisung an den Auftragnehmer erteilt wurde. Der Auftragnehmer hat nur Weisungen in Schrift- oder Textform zu befolgen.
- 4.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

5. Vertraulichkeit

- 5.1 Der Auftragnehmer gewährleistet und versichert, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- 5.2 Der Auftragnehmer erbringt auf Anfrage den Nachweis über die Verpflichtung auf Vertraulichkeit.
- 5.3 Soweit der Auftragnehmer in Berührung kommt mit personenbezogenen Daten, die Rückschlüsse auf Eigenschaften, Umstände, Informationen oder Geschehnisse, die dem Amtsträgergeheimnis unterliegen oder unterliegen könnten, zulassen, verpflichtet er sich, diese vertraulich zu behandeln.

6. Technisch-organisatorische Maßnahmen des Auftragnehmers

- 6.1 Der Auftraggeber arbeitet nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
- 6.2 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat der Auftragnehmer geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem gegebenenfalls Folgendes ein:
 - a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
 - b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
 - c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
 - d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- 6.3 Bei der Beurteilung des angemessenen Schutzniveaus hat der Auftragnehmer die Risiken berücksichtigt, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
- 6.4 Der Auftragnehmer unternimmt Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

- 6.5 Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten hat der Auftragnehmer geeignete technisch-organisatorische Maßnahmen getroffen. Ergänzend hierzu gilt die **Anlage 1 „Beschreibung der technisch organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO“**. Die darin beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das von dem Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll.
- 6.6 Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, wozu auch herstellerseitige Softwareupdates zählen, solange das hier vereinbarte Sicherheitsniveau nicht unterschritten wird.
Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen.

7. Einschaltung von weiteren Auftragsverarbeitern

- 7.1 Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zur Einschaltung weiterer Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 DS-GVO.
- 7.2 Bei Abschluss dieser Vereinbarung hat der Auftraggeber der Inanspruchnahme der in **Anlage 2 „Weitere Auftragsverarbeiter“** bezeichneten weiteren Auftragsverarbeitern sowie der Verarbeitung von personenbezogenen Daten durch diese zugestimmt.
- 7.3 Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen begründeten Einspruch im Laufe von 14 Tagen zu erheben. Sind die durch den Auftraggeber vorgebrachten Gründe berechtigt, darf der Auftragnehmer die beabsichtigte Änderung nicht vollziehen. Der Bestand der weiteren Auftragsverarbeiter bleibt davon unberührt. Es bleibt der Auftragnehmerin unbenommen, weitere beabsichtigte Änderungen, deren Vollzug sich ebenfalls nach dieser Klausel richtet, vorzuschlagen. Dem Auftraggeber entsteht kein gesondertes Kündigungsrecht durch den Einspruch in eine beabsichtigte Änderung.
- 7.4 Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser Vereinbarung dem weiteren Auftragsverarbeiter zu übertragen. Dies gilt insbesondere für die zwischen den Vertragspartnern festgelegten Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit.

8. Rechte der Betroffenen

- 8.1 Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen.
- 8.2 Der Auftragnehmer trifft insbesondere geeignete technische und organisatorische Maßnahmen, um dem Auftraggeber die Erfüllung seiner Pflichten gegenüber den Betroffenen zu ermöglichen.

9. Unterstützung des Auftraggebers

- 9.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit der Verarbeitung personenbezogener Daten sowie zu etwa bestehenden Melde- und Benachrichtigungspflichten, durchzuführenden Datenschutz-Folgeabschätzungen und notwendigen vorherigen Konsultationen der Aufsichtsbehörde.
- 9.2 Der Auftragnehmer stellt ein angemessenes Schutzniveau durch technische und organisatorische Maßnahmen sicher, welche 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.

- 9.3 Der Auftragnehmer ist verpflichtet, eine Verletzung des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Meldeverpflichtung aus Art. 33 DS-GVO und stellt ihm die etwa benötigten Informationen unverzüglich zur Verfügung.
- 9.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen aus Art. 34 DS-GVO und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
- 9.5 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwa durchzuführender Datenschutz-Folgeabschätzungen gem. Art. 35 DS-GVO.
- 9.6 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwa notwendiger vorheriger Konsultationen der Aufsichtsbehörde.

10. Vergütungsregelungen

- 10.1 Der Auftragnehmer darf dem Auftraggeber Aufwendungen in Rechnung stellen, die ihm durch seine Inanspruchnahme auf Grundlage dieses Vertrags und Erfüllung seiner Pflichten aus diesem Vertrag entstanden sind. Dies gilt nicht, wenn der Auftragnehmer aufgrund der zugrundeliegenden schuldrechtlichen Vereinbarung oder aufgrund einer Pflichtverletzung vertraglich oder gesetzlich verpflichtet ist.
- 10.2 Der Aufwand ist in Höhe der zwischen den Vertragspartnern vereinbarten Stundensätze zu vergüten. Sind keine Stundensätze vereinbart, kann der Auftragnehmer eine angemessene Vergütung verlangen.

11. Abschluss der Erbringung der Verarbeitungsleistungen

- 11.1 Nach Beendigung des bestehenden Vertragsverhältnisses und des jeweiligen Einzelauftrags hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auf Verlangen auszuhändigen.
- 11.2 Die Datenträger des Auftragnehmers sind danach auf Verlangen physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist – auf Verlangen des Auftraggebers – in geeigneter Weise zu dokumentieren.

12. Kontrollrechte des Auftraggebers

- 12.1 Der Auftraggeber hat das Recht, sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen. Hierfür kann er insbesondere Selbstauskünfte des Auftragnehmers einholen und sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, begrenzt auf einmal jährlich, persönlich überzeugen oder einen Dritten hiermit beauftragen.
- 12.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist insbesondere verpflichtet, die Umsetzung von angemessenen technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis über solche Maßnahmen, die nicht nur den konkreten Einzelauftrag betreffen, kann erfolgen durch:
 - a) die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO;
 - b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DS-GVO;
 - c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

13. Berichtigung, Einschränkung und Löschung von Daten

- 13.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, einschränken oder löschen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.
- 13.2 Falls vereinbart, sind das Vorhandensein eines datenschutzkonformen Löschkonzepts, die Datenportabilität sowie die Umsetzung der Rechte auf Berichtigung und Löschung („Recht auf Vergessenwerden“) vom Auftragnehmer sicherzustellen.

14. Datenschutzbeauftragter

Der Auftragnehmer ist gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet. Dieser Verpflichtung ist er nachgekommen. Die Kontaktdaten des Datenschutzbeauftragten sind:

Datenschutzbeauftragter der Dr. Josef Raabe Verlags-GmbH
Rotebühlstraße 77
70178 Stuttgart

E-Mail: datenschutzbeauftragter@raabe.de

15. Dokumentationspflichten des Auftragnehmers

- 15.1 Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag für den Auftraggeber durchgeführten Tätigkeiten der Verarbeitung. Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
- 15.2 Der Auftraggeber oder der Auftragnehmer sowie gegebenenfalls der Vertreter des Auftraggebers oder des Auftragnehmers stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

16. Informationspflichten, Schriftformklausel, Rechtswahl

- 16.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.
- 16.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- 16.3 Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftragnehmers.

Ort und Datum

Stuttgart, den 05.05.2023

Ort und Datum

Für den Auftraggeber



Für den Auftragnehmer

Anlage 1

Beschreibung der technisch organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO

Der Auftragnehmer hat unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen die im Folgenden aufgeführten geeigneten technischen und organisatorischen Maßnahmen in die Verarbeitungstätigkeit miteinbezogen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der geltenden DS-GVO erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

1. Vertraulichkeit (Art. 32 Abs. 1 b) DS-GVO)

1.1 Zutrittskontrolle

Die Verhinderung des Zutritts nicht berechtigter Personen in das Gebäude sowie einzelner abgesicherter Bereiche innerhalb des Gebäudes wird durch folgende Maßnahmen gewährleistet:

- Das Betriebsgebäude ist in unterschiedliche Zutrittsbereiche eingeteilt
- Besucher melden sich am Empfang und werden vom Ansprechpartner abgeholt
- Der Zutritt zu sämtlichen Datenverarbeitungsanlagen ist Unbefugten vollständig verwehrt
- Der Zutritt jeglicher Personen (auch Mitarbeiter) muss durch autorisiertes Personal im Voraus genehmigt werden und wird durch eine Personenkontrolle überprüft
- Sämtliche Zugänge und Räumlichkeiten der Datenverarbeitungsanlagen werden durch Kameras überwacht und durch elektronische Schließsysteme kontrolliert
- Jeglicher Zutritt wird protokolliert

1.2 Zugangskontrolle

Ein ausreichender Schutz der IT-Systeme des wird gewährleistet durch:

- Zugang zu den Datenverarbeitungsanlagen erhält ausschließlich autorisiertes und fachlich qualifiziertes Personal
- Der Zugang erfolgt über eine Benutzerkennung und Eingabe eines Passwortes
- Die Passwörter entsprechen einem technisch sicheren Niveau und sind durch interne Richtlinien geregelt
- Die Anmeldungen werden protokolliert

1.3 Zugriffskontrolle

Systeme, die von unterschiedlichen Benutzern verwendet werden, werden durch Zugriffskontrollen abgesichert. Dabei handelt es sich um einen allgemeinen Zugriffsschutz rund um Server und Netzwerk:

- Der Zugriff auf die Datenverarbeitungssysteme ist durch eine Nutzer- und Rechteverwaltung abgesichert. Es ist einzelnen Mitarbeitern nur möglich die für ihre Aufgaben erforderlichen Daten einzusehen, zu nutzen, zu verarbeiten oder zu löschen
- Die Zugriffe auf die Datenverarbeitungssysteme werden geloggt
- Beim Verlassen des Arbeitsplatzes erfolgt eine Sperrung durch Bildschirmschoner, Freigabe nur durch Eingabe des Passwortes
- Jeder Mitarbeiter wird entsprechend zur Vertraulichkeit und der Einhaltung des Datenschutzes bei Aufnahme seiner Tätigkeit verpflichtet. Ein Verstoß hätte die fristlose Kündigung, sowie eine Strafanzeige zur Folge. Betroffene Auftraggeber würden in so einem Fall selbstverständlich über den Vorfall informiert

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Konzept zur logischen (virtuellen) Mandantentrennung
- Logische Trennung von Mitarbeiter- und Kundendaten

1.5 Pseudonymisierung (Art. 32 Abs. 1 a) DS-GVO; Art. 25 Abs. 1 DS-GVO)

Gewährleistung der Pseudonymisierung der personenbezogenen Daten, sodass diese nicht mehr einer spezifischen betroffenen Person zugeordnet werden können:

- Verschlüsselte Datenübertragung (verschlüsselte Internetverbindungen mittels TLS/SSL)
- Personenbezogene Daten werden soweit möglich pseudonymisiert/anonymisiert

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

2.1 Weitergabekontrolle

Diese Maßnahmen dienen dem Schutz vor unberechtigten Zugriffen auf Daten bei der elektronischen Übertragung:

- Der Auftragnehmer überträgt von sich aus personenbezogene Daten ausschließlich elektronisch über verschlüsselte Datenverbindungen, so dass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können
- Nicht mehr benötigte oder defekte Datenträger werden durch ein zertifiziertes Unternehmen entsorgt

2.2 Eingabekontrolle

Maßnahmen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Die Eingabe, Änderung oder Löschung personenbezogener Daten wird mit der Kennung des zuständigen Mitarbeiters geloggt

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

3.1 Verfügbarkeitskontrolle

Zur Sicherung geschäftskritischer Daten wird ein umfassendes Sicherheitskonzept eingesetzt, welches vor zufälliger oder mutwilliger Zerstörung schützt:

- Sämtliche Daten sind soweit technisch möglich im Rahmen der Ausfallsicherheit vor zufälligem Verlust oder Zerstörung geschützt.
- Hierzu kommen u.a. RAID Systeme, Ersatzhardware, Überspannungsschutz, USV-Anlagen, Notstromaggregat, Löschanlage zum Einsatz
- Weitergehend werden Backups bereitgehalten

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 c) DS-GVO)

Um Datenverlust zu vermeiden ist eine umfangreiche Datensicherungsstrategie entwickelt worden:

- Regelmäßige und dokumentierte Datenwiederherstellungen
- IT-Notfallpläne und Wiederanlaufpläne

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

4.1 Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Eindeutige Vertragsgestaltung
- Formalisiertes Auftragsmanagement
- Bestellung eines Datenschutzbeauftragten

4.2 Datenschutzmanagement; Incident-Response-Management

- Managementsystem zum Datenschutz und der Informationssicherheit
- Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen
- Durchführung regelmäßiger IT-Schwachstellenanalysen
- Durchführung regelmäßiger interner Audits
- Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen

4.3 Datenschutzfreundliche Voreinstellungen

- Die standardisierten Voreinstellungen wurden im datenschutzfreundlichen Sinne getroffen

Anlage 2 – Weitere Auftragsverarbeiter

Firma, Anschrift	Dienstleistung	Drittlandübermittlung / geeignete Garantien?
Mittwald CM Service GmbH & Co. KG Königsberger Straße 4-6 32339 Espelkamp	- Hosting	- Keine Drittlandübermittlung - AVV abgeschlossen
Slim brand interactive GmbH Ferdinand-Walbrecht-Str. 4 30163 Hannover	- Weiterentwicklung, Pflege und Betrieb der App	- Keine Drittlandübermittlung - AVV abgeschlossen

