Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

[Stand: September 2018]

zwischen

_____

_____

_____

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

weclapp GmbH
Frauenbergstraße 31-33
35039 Marburg

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DS-GVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Dieser Vertrag gilt ab dem 25.05.2018 und enthält nach dem Willen der Parteien den Vertrag im Sinne des Art. 28 Datenschutz-Grundverordnung (DS-GVO).

(3) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird dafür die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DS-GVO zugrunde gelegt. Eine Verarbeitung personenbezogener Daten umfasst insbesondere das Erheben, die Speicherung, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Sperrung, Löschung oder sonstige Nutzung von Daten.

2. Gegenstand und Dauer des Auftrags sowie Auftragsinhalt

(1) Der Auftragnehmer erbringt für den Auftraggeber verschiedene Leistungen im Rahmen des „Cloud-Dienstleistungsvertrages“. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten und Rechte des Auftraggebers und des Auftragnehmers im Zusammenhang mit der Verarbeitung der personenbezogenen Daten des Auftraggebers durch den Auftragnehmer.

(2) Die Dauer dieses Vertrages entspricht der Dauer des Cloud-Dienstleistungsvertrages.

(3) Art und Zweck der Datenverarbeitung richten sich nach den getroffenen Vereinbarungen bzw. nach den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser zugestimmt hat (mind. in Textform).

(4) Die von der Datenverarbeitung betroffenen Datenarten sind:

(ggf. durch Auftraggeber anzupassen)

- ☐ Kommunikationsdaten (z. B. Telefon, E-Mail)
- ☐ Zahlungsdaten (z. B. IBAN)
- ☐ Kundendaten
- ☐ Nutzerdaten (z. B. Name)
- ☐ Bankdaten
- ☐ Mitarbeiterdaten
- ☐
- ☐
- ☐
- ☐

(5) Die von der Datenverarbeitung Betroffenen sind:

(ggf. durch Auftraggeber anzupassen)

- ☐ Mitarbeiter
- ☐ Kunden
- ☐ Interessenten
- ☐ Lieferanten
- ☐ Bewerber
- ☐ Ansprechpartner
- ☐ Dritte
- ☐
- ☐
- ☐
- ☐

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Der Auftraggeber hat das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Die Weisungen müssen schriftlich (mind. Textform) erfolgen.

(2) Erteilt der Auftraggeber ergänzende Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, ist der Auftragnehmer berechtigt, eine Vergütung für den Mehraufwand zu verlangen.

(3) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden, muss dies mind. in Textform erfolgen. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer unverzüglich mind. in Textform mitteilen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(5) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DS-GVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer führt die Datenverarbeitung im Auftrag nur in Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums durch. 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.

(2) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen Datenschutzvorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DS-GVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(4) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten mitzuteilen, die im Zuge der Verarbeitung von Daten des Auftraggebers erfolgt. Der Auftragnehmer wird den Auftraggeber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DS-GVO gegenüber dem Auftragnehmer tätig wird und dies eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betrifft.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzung und vorherige Konsultation. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DS-GVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen.

(6) Der Auftragnehmer kann für die Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, eine Vergütung verlangen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten nach Art. 37 DS-GVO bestellt hat.

(2) Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

(3) Die Kontaktdaten des Datenschutzbeauftragten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt. Auf Anforderung teilt der Auftragnehmer dem Auftraggeber den Namen und die Kontaktdaten des Datenschutzbeauftragten mit.

6. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet. Der Auftraggeber stimmt der Beauftragung des nachfolgenden Unterauftragnehmers zu:

Unterauftragnehmer	Leistung
ProfitBricks GmbH Greifswalder Straße 207 10405 Berlin	Erbringung von Rechenzentrumsleistungen in Form IaaS Cloud Computing.

Dem Auftragnehmer wird die allgemeine Genehmigung erteilt, weitere Unterauftragnehmer zur Verarbeitung der Daten des Auftraggebers einzusetzen oder den bestehenden Unterauftragnehmer zu wechseln, vorausgesetzt, der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung eines Unterauftragnehmers und der Auftraggeber erhebt gegenüber dem Auftragnehmer keinen Einspruch (mind. in Textform) bis zum Zeitpunkt der Übergabe der Daten.

(2) Der Einspruch ist nur zulässig, wenn die Hinzuziehung oder Ersetzung eines Unterauftragnehmers eine nicht datenschutzkonforme Verarbeitung zur Folge hätte.

(3) Erhebt der Auftraggeber gegen die Hinzuziehung oder Ersetzung einen zulässigen Einspruch, ist der Auftragnehmer berechtigt, diesen Vertrag und den Cloud-Dienstleistungsvertrag fristlos zu kündigen.

(4) Der Vertrag mit dem Unterauftragnehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann. Der Auftragnehmer hat dem Unterauftragnehmer dieselben Verpflichtungen aufzuerlegen, die in diesem Vertrag gem. Art. 28 Abs. 3 DS-GVO festgelegt sind.

(5) Nicht als Unterauftragsverhältnisse sind Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Erfüllung der geschäftlichen Tätigkeit in Anspruch nimmt. Dazu zählen Reinigungsleistungen, Postdienste, Telekommunikationsleistungen und Bewachungsdienste. Der Auftragnehmer ist jedoch verpflichtet, auch bei diesen Diensten geeignete Vorkehrungen zum Schutz personenbezogener Daten zu treffen. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DS-GVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

7. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer ermöglicht dem Auftraggeber, sich insbesondere von der Einhaltung der technischen und organisatorischen Maßnahmen durch den Auftragnehmer zu überzeugen. Dazu kann der Auftraggeber Auskünfte einholen oder eine Vor-Ort-Kontrolle durchführen. Der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen kann durch den Auftragnehmer auch erbracht werden durch Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, IT-Sicherheitsabteilung oder

Datenschutzbeauftragter), Zertifizierung nach einem geeigneten Zertifizierungsverfahren gemäß Art. 42 DS-GVO oder geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit. Auftragnehmer und Auftraggeber sind sich darüber einig, dass der Nachweis zudem erbracht werden kann durch sonstige Nachweise, die wahrscheinlich machen, dass der Auftragnehmer seine Tätigkeiten unter Einhaltung der Vorgaben der DS-GVO sorgfältig und gewissenhaft erbringt.

(2) Der Auftraggeber kann nach Vereinbarung eines Termins die Kontrolle am Sitz des Auftragnehmers zu den Geschäftszeiten des Auftragnehmers vornehmen. Der Auftragnehmer wird den Auftraggeber bei der Durchführung von Kontrollen unterstützen und an der vollständigen und zügigen Abwicklung der Kontrolle mitwirken. Der Auftragnehmer wird dem Auftraggeber hierzu erforderliche Auskünfte erteilen und die Umsetzung der technischen und organisatorischen Maßnahmen nachweisen, soweit dies für die Durchführung der Kontrolle erforderlich ist.

(3) Der Auftragnehmer ist berechtigt, für die Ermöglichung der Kontrolle eine Vergütung zu verlangen.

8. Verpflichtung auf Vertraulichkeit

(1) Der Auftragnehmer erklärt, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit deren Anwendung vertraut ist.

(2) Der Auftragnehmer gewährleistet, dass die mit der Verarbeitung der personenbezogenen Daten befassten Mitarbeiter auf das Datengeheimnis bzw. auf die Vertraulichkeit verpflichtet worden sind und mit den für sie maßgeblichen Bestimmungen zum Datenschutz vertraut gemacht wurden.

9. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-22 DS-GVO zu bearbeiten, zu unterstützen. Der Auftragnehmer wird den Auftraggeber informieren, wenn Betroffene ihre Betroffenenrechte an den Auftragnehmer richten.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten (insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung) durch den Auftraggeber erforderlich ist, wird der Auftragnehmer den Auftraggeber auf Anforderung (mind. in Textform) unterstützen.

(3) Der Auftragnehmer wird den Auftraggeber dabei unterstützen, Informationen bereitzustellen. Voraussetzung hierfür ist, dass der Auftraggeber den Auftragnehmer hierzu auffordert (mind. in Textform).

(4) Der Auftragnehmer kann für die Unterstützungshandlungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber eine Vergütung verlangen.

10. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DS-GVO.

(2) Der derzeit bestehende Stand der getroffenen technischen und organisatorischen Maßnahmen ist in **Anlage 1** dokumentiert und wird dem Auftraggeber zur Prüfung bereitgestellt.

(3) Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Der Auftragnehmer ist daher bei entsprechender Änderung berechtigt, die technischen und organisatorischen Maßnahmen anzupassen. Wesentliche Änderungen werden dokumentiert. Der Auftraggeber ist berechtigt, jederzeit eine aktuelle Fassung der technischen und organisatorischen Maßnahmen anzufordern.

11. Beendigung des Vertrages

(1) Nach Beendigung des Vertrages hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, wobei die Rückgabe nur für Unterlagen gilt, die in nicht elektronischer Form vorliegen.

(2) Der Auftraggeber ist verpflichtet, bis spätestens zum Beendigungszeitpunkt mitzuteilen (mind. in Textform), ob er die Rückgabe oder Löschung seiner personenbezogenen Daten wünscht. Geht bis zum Beendigungszeitpunkt keine Mitteilung beim Auftragnehmer ein, wird der Auftragnehmer alle Daten des Auftraggebers 14 Tage nach Beendigung des Vertrages löschen. Die Löschung ist in geeigneter Weise zu dokumentieren und dem Auftraggeber auf Anforderung (mind. Textform) zu bestätigen. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung bzw. Aufbewahrung der Daten bleiben unberührt.

(3) Wünscht der Auftraggeber die Rückübertragung seiner in der weclapp-Cloud verarbeiteten Daten, bedarf dies einer gesonderten Vereinbarung.

12. Zurückbehaltungsrecht

Es besteht Einigkeit darüber, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S. d. § 273 BGB bezüglich der verarbeiteten Daten ausgeschlossen wird.

13. Haftungsfreistellung im Falle des Art. 82 Abs. 4 DS-GVO

Werden Auftragnehmer oder Auftraggeber nach Art. 82 Abs. 4 DS-GVO von einer betroffenen Person in Haftung/ Anspruch genommen, stellen sie einander auf erstes Anfordern von allen Ansprüchen frei, die unter den in Art. 82 Abs. 2 DS-GVO festgelegten Bedingungen dem Anteil der jeweils anderen Partei an der Verantwortung für den Schaden entsprechen.

14. Aufhebung der „ADV“ nach § 11 BDSG

Haben Auftraggeber und Auftragnehmer zum Cloud-Dienstleistungsvertrag eine Auftragsdatenverarbeitungsvereinbarung (ADV) nach § 11 BDSG abgeschlossen, wird diese mit Abschluss dieses Vertrages zur Auftragsverarbeitung gemäß Art. 28 DS-GVO einvernehmlich aufgehoben.

15. Schlussbestimmungen

(1) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

(2) Für sämtliche Rechtsbeziehungen zwischen den Vertragspartnern gilt das für die Rechtsbeziehungen inländischer Parteien maßgebliche Recht der Bundesrepublik Deutschland unter Ausschluss der Bestimmungen des Internationalen Privatrechts.

(3) Gerichtsstand ist Marburg/Lahn. Ein etwaiger ausschließlicher Gerichtsstand bleibt hiervon unberührt.

_____, den _____	Marburg, den _____
Ort Datum	Ort Datum
_____	_____
- Auftraggeber -	- weclapp GmbH -

Anlage 1 Technische und organisatorische Maßnahmen zur Datensicherheit gem. Art. 32 Abs. 1 DS-GVO

I. Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

Für den elektronischen Transport der Daten setzt der Auftragnehmer Verschlüsselungsverfahren ein.

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

1. Zugangskontrolle und Zutrittskontrolle

Zutrittskontrolle

Standort Marburg

Die Betriebsareale am Standort Marburg sind in mehrere Sicherheitsbereiche untergliedert. Besucher müssen sich am Empfang identifizieren und werden nur in Begleitung zu ihren Ansprechpartnern in den jeweiligen Sicherheitsbereichen geführt. Der Zutritt zu den Sicherheitsbereichen wird durch ein automatisches Zugangskontrollsystem geschützt. Die Ausgabe der Schlüssel für die Sicherheitsbereiche wird zentral verwaltet, überwacht und die Zutrittsberechtigungen gem. Rollenkonzept und darauf aufbauenden Nutzerrechten vergeben. Die Autorisierung von berechtigtem Personal an dem Zugangskontrollsystem erfolgt über ein Chipkarten- /Transponder-Schließsystem. Der Zutritt zu besonders kritischen Systemen, wie dem Serverraum, ist nur eingeschränktem Personal möglich. Die Zutrittsbereiche sind durch Alarmanlage abgesichert. Es erfolgen Alarmmeldungen in mehreren sicherheitsrelevanten Abstufungen bei unberechtigten Zutritten zu den Serverräumen, in der höchsten Kritikalitätsstufe zur nächsten Polizeistation. Innerhalb der Bereiche werden Bewegungsmelder eingesetzt. Es erfolgt eine sorgfältige Auswahl von Wach- und Reinigungspersonal.

Standort Kitzingen

Der Zutritt zum Standort Kitzingen ist durch ein elektronisches Zugangssystem geschützt. Der Zutritt ist nur für Mitarbeiter mit einem elektronischen Key möglich. Das Betreten der Räumlichkeiten wird durch das elektronische Zugangssystem protokolliert. Rollenkonzepte und Nutzerrechte sind zentral für alle Mitarbeiter für alle Standorte geregelt. Die oben beschriebenen Maßnahmen für den Standort Marburg treffen deshalb auf den Standort Kitzingen zu.

Zugangskontrolle

Die Datenverarbeitungssysteme werden insbesondere durch Anti-Viren-Software, Firewall-Systeme (Hardware/Software) und Proxy-Server geschützt. Die Verwaltung der Sicherheitssoftware wird regelmäßig sichergestellt und erfolgt nur durch autorisiertes Personal. Die Autorisierung des Personals wird durch zugeordnete Benutzerrechte bzw. Benutzerprofile sichergestellt. Über diese Profile

kann eine Authentifizierung an den jeweiligen IT-Systemen durch Benutzername / Passwort erfolgen. Zugriffe auf Datenverarbeitungssysteme erfolgen über gesicherte Verbindungen (u.a. VPN-Technologie).

2. Zugriffskontrolle

Die Rechtevergabe wird gemäß Berechtigungskonzept umgesetzt und die Verwaltung obliegt den Systemadministratoren. Grundsätzlich wird die Anzahl der Administratoren nur auf das „Notwendigste“ reduziert. Um den Zugriff auf Daten nur autorisiertem Personal zu ermöglichen, werden Datenträger und Daten verschlüsselt und der Zugriff über die Nutzerrechte reguliert. Eine Passwortrichtlinie verpflichtet Mitarbeiter organisatorisch sowie technisch angemessene Passwörter zu wählen und regelmäßige Wechsel durchzuführen. Der Zugriff auf Systeme und Anwendungen erfolgt passwortgestützt und ist rechtegebunden - jeder Mitarbeiter kann im Rahmen seines Tätigkeitsbereiches nur auf die notwendigen Funktionen zum Verrichten seiner Tätigkeiten zugreifen. Der Auftragnehmer verfolgt den Grundsatz, möglichst wenige Drucksachen zu erzeugen. Bei der Entsorgung werden Aktenvernichter eingesetzt. Datenträger werden in Sicherheitsbereichen mit Zugriffsbeschränkung aufbewahrt und verschlossen. Eine ordnungsgemäße Vernichtung von Datenträgern erfolgt durch einen Dienstleister. Die Vernichtung erfolgt protokolliert und überwacht. Der unrechtmäßige Zugriff auf Systeme oder auf die Datenintegrität über Sicherheitslücken in Programmen wird durch regelmäßige Scans der Netzwerkinfrastruktur und umgehende Behebung gefundener Probleme verhindert. Sowohl externe als auch interne Zugriffe werden so erkannt und deren Auswirkungen minimiert.

3. Trennungskontrolle

Der Auftragnehmer kommt den Anforderungen des DS-GVO nach, zu unterschiedlichen Zwecken erhobene Daten getrennt zu verarbeiten. Diese Anforderung wird durch eine organisationsbezogene Funktionstrennung und die Verwaltung von Sicherheitsbereichen verdeutlicht; auch innerhalb der Abteilungen wird dieses Prinzip weitestgehend erfüllt. Daten, die für unterschiedliche Mandanten erhoben wurden, werden separat verwaltet und getrennt verarbeitet. Um das sicherzustellen, wurde ein umfangreiches Berechtigungskonzept erstellt, auf dem auch die Datenbankrechte basieren. Eine softwareseitige logische Mandanten-Trennung erfolgt und wird sichergestellt. Testumgebungen werden vom Produktivsystem unabhängig verwaltet – eine Überführung von Kundendaten in dieses Testsystem erfolgt nicht und wird technisch verhindert.

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

1. Weitergabekontrolle

Der elektronische Datenaustausch wird durch Sicherungssysteme überwacht. Das unbefugte Entfernen von Datenträgern im Unternehmen wird durch Sicherheitsbereiche eingeschränkt. Für die jeweiligen Bereiche sind Richtlinien erlassen, die ein unberechtigtes Entfernen von Datenträgern verhindern. Zudem sind die Datenträger verschlüsselt. Ausrangierte Datenträger werden in abgeschlossenen Containern verwahrt und gemäß Vorgabe vernichtet. Die Umsetzung erfolgt durch ein 4-Augen-Prinzip. Außerdem erfolgt eine Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts. Beim physischen Transport von Datenträgern werden sichere Transportbehälter eingesetzt.

2. Eingabekontrolle

Durch die restriktive Vergabe von Rechten wird die Eingabe, Änderung oder Entfernung von personenbezogenen Daten in Datenverarbeitungssystemen eingeschränkt. Die Eingabe, Änderung und Entfernung von Daten durch den jeweiligen Nutzer wird protokolliert und ist nachvollziehbar. Es existiert eine Liste, aus der sich ergibt, mit welchen Applikationen Daten eingegeben, geändert und gelöscht werden können. Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt auf Basis eines Berechtigungskonzepts.

IV. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b. DS-GVO) sowie rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Um zufällige Zerstörung oder Verlust im Rahmen der auftragsbezogenen Verarbeitung von Daten einzuschränken, wurde ein Backup- & Recoverykonzept erstellt, implementiert und die Wiederherstellung regelmäßig getestet. Die Datensicherungen werden an einem sicheren, ausgelagerten Ort verwahrt. Um auch bei Störungen im Stromnetz den regelmäßigen und sicheren Betrieb der Systeme zu gewährleisten, wird eine unterbrechungsfreie Stromversorgung (USV) in Verbindung mit einer Netz-Ersatz-Anlage (NEA) eingesetzt. Der Serverraum wird durch unterschiedliche Überwachungs- und Meldesysteme abgesichert, wie insbesondere Geräte zur Überwachung von Temperatur und Feuchtigkeit sowie Feuer- und Rauchmeldeanlagen. Maßnahmen zur Risikoverminderung, wie das organisierte Platzieren von Feuerlöschern und die Installation von Brandschutzklappen sind selbstverständlich. Die regelmäßige Wartung der Melde- und Steuerungssysteme erfolgt in definierten Intervallen. Die Räumlichkeiten wurden zielgerichtet erstellt und erfüllen gängige Sicherheitsanforderungen. Dabei wurde darauf geachtet, besonders schützenswerte Bereiche in isolierten Zonen zu platzieren und gegen Störfälle abzusichern. Dafür wurde ein Notfallkonzept entworfen und die notwendigen diesbezüglichen Maßnahmen implementiert.

V. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)

1. Auftragskontrolle

Der Auftragnehmer verarbeitet die eingereichten Daten gemäß dem geschlossenen Vertrag und achtet dabei die gesetzlichen Vorschriften und per Vertrag definierten Anforderungen im Rahmen der Weisungen des Auftraggebers. Dadurch wird die Weitergabe der Daten an unbefugte Dritte vertraglich ausgeschlossen und der Weisungsrahmen festgelegt.

Bei Unteraufträgen werden bei der Festlegung vor allem auch die Pflichtinhalte des Art. 28 DS-GVO berücksichtigt. Der Auftragnehmer ermöglicht dem Auftraggeber eine Prüfung der Dokumentation der „technisch / organisatorischen Maßnahmen“ oder falls erforderlich, eine vor Ort Besichtigung der Datenverarbeitungsanlagen. Eine mögliche Überprüfung des Auftragnehmers sowie seiner, im Rahmen der Datenverarbeitung durchgeführten Tätigkeiten, wird durch den Auftragnehmer dadurch ermöglicht und unterstützt.

2. Datenschutz-Management

Die Beschäftigten des Auftragnehmers werden regelmäßig über die Anforderungen des Datenschutzes unterrichtet.

Alle Mitarbeiter des Auftragnehmers werden auf das Datengeheimnis bzw. zur Wahrung der Vertraulichkeit verpflichtet. Dies wird auf einem sog. Laufzettel dokumentiert.

Es wurde ein Datenschutzbeauftragter benannt, der in sämtliche Fragestellungen zum Schutz personenbezogener Daten eingebunden wird. Der Datenschutzbeauftragte überwacht die Einhaltung der Vorgaben des Datenschutzes und wird durch Datenschutzkoordinatoren unterstützt.

3. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Dem Grundsatz Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen wird durch viele Maßnahmen Rechnung getragen. So dient eine Zwei-Wege-Authentifizierung dazu, dass sich unbefugte Personen nicht unerlaubt Zugang zum Account des Auftraggebers verschaffen. Dem Auftraggeber ist es möglich, Berechtigungen auf Daten und Softwareanwendungen flexibel zu setzen, indem etwa Lese- und Schreibrechte vergeben werden können. Die Möglichkeit zur Löschung von Daten ist abhängig von der zugeteilten Berechtigung. Pflichtfelder sind auf ein Minimum beschränkt.