Vertrag zur Auftragsverarbeitung gemäß

Art. 28 DS-GVO

zwischen

- Verantwortlicher - nachstehend **Auftraggeber** genannt -

und

ProntoWeb GmbH
Hörvelsinger Weg 35
89081 Ulm

- Auftragsverarbeiter - nachstehend **Auftragnehmer** genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- **Bereitstellung Softwarenutzung „DropanGo“ für den Auftraggeber**

Für den Auftraggeber stellt der Auftragnehmer Zugang zur Nutzung der Software „DropanGo“ über eine gehostete Plattform zur Verfügung.

In der Verantwortung seitens des Auftragnehmers als Inhaber der Plattform stehen folgende Punkte:

- Inhalte der Plattform selbst
- Funktionen der Plattform
- Verwaltung der Kundeninformationen zu Zwecken:

- Bereitstellung Plattformfunktionen
- Verwendung von Kundendaten zur Auswertung

Auf den zwischen den Parteien geschlossenen Hauptvertrag wird hierbei hinsichtlich des Umfangs der Leistungen des Auftragnehmers Bezug genommen.

(2) Dauer

Diese Vereinbarung beginnt mit Vertragsschluss. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

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

Siehe Beschreibung unter Ziffer 1.)

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. 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.

Das angemessene Schutzniveau in Deutschland wird hergestellt durch sonstige Maßnahmen: Interne Datenschutzrichtlinien (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

(2) Art der Daten

Der Gegenstand der Verarbeitung personenbezogener Daten ergibt sich aus der entsprechend **Anlage 1** aufgeführten Datenkategorien.

3. Technisch-organisatorische Maßnahmen

(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.

(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.

(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) Auf die in **Anlage 2** aufgeführten technisch-organisatorischen Maßnahmen wird hierbei Bezug genommen.

4. Berichtigung, Einschränkung und Löschung von Daten

(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.
(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:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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.

- 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.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 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.
- 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.
- 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Der Auftragnehmer ist 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. Dabei hat der Auftragnehmer insbesondere dafür Sorge zu tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers

beauftragen, Art. 28 Abs. 2 DSGVO. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt.
Zurzeit sind für den Auftragnehmer die in der **Anlage 3** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(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, insbesondere wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch Erfüllung der besonderen Voraussetzungen der Art. 44 ff. DS-GVO sicher (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

Im Einzelnen umfasst dies u.a.:

- Es werden mit jedem Unterauftragnehmer schriftliche Vereinbarungen geschlossen, die dem Unterauftragnehmer dieselben Pflichten wie im zwischen dem Auftragnehmer und dem Auftraggeber geschlossenen AV-Vertrag auferlegen und die die Vorgaben des Art. 28 Abs. 3 DSGVO einhalten.
- Der Verantwortliche ermächtigt hiermit den Auftragsverarbeiter, im Namen des Verantwortlichen eine Vereinbarung mit einem Unterauftragnehmer auf der Grundlage der aktuellen Fassung der SCC der Europäischen Kommission zu schließen
- Der Auftragsverarbeiter haftet gegenüber dem für die Verarbeitung Verantwortlichen dafür, dass der Unterauftragnehmer seinen Datenschutzpflichten nachkommt.

Der Auftragnehmer versichert, dass eine Datenverarbeitung ausschließlich in Europa durchgeführt wird.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem 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.
(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 nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B.Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8. Mitteilung bei Verstößen des Auftragnehmers

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-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(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.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) 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.
(2) 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.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

.....	.....	.....
Ort, Datum	Name Auftraggeber	Unterschrift Auftraggeber

.....	.....	.....
Ort, Datum	Name Auftragnehmer	Unterschrift Auftragnehmer

Anlage 1 - Datenkategorien DropanGo

Folgende Datenarten werden von Ansprechpartnern und Mitarbeitern des Kunden verarbeitet:

- Benutzer
- IP Adresse
- Typ/Version des Browsers
- Benutzername / Login Name
- Letzter Login
- Kontaktdaten (Telefon, E-Mail)
- Passwort-Hash

Erweiterte Daten, welche vom Benutzer über die Benutzerverwaltung/Stammdatenpflege erfasst werden können:

- Firmendaten
- Name
- Adresse
- Kontaktdaten
- Berechtigungen
- Lieferungsbeschreibungen
- Lieferungen und Lieferungszeiten

Anlage 2 – Technisch-organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit benannt, die der Auftragsverarbeiter eingerichtet hat und laufend aufrechterhält. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Verantwortlicher und Ansprechpartner für alle nachfolgenden Maßnahmen:
Herr Otto Figel

Inhaltsverzeichnis

1 Technisch-organisatorische Maßnahmen

1.1 Sicherung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die verhindern, dass Unbefugte personenbezogene Daten zur Kenntnis nehmen können.

1.1.1 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Folgende Maßnahmen sind umgesetzt:

Maßnahmen

• **Begleitung betriebsfremder Personen** Betriebsfremde (Besucher, Wartungspersonal) sind während der Anwesenheit im Gebäude
• **Sorgfältige Auswahl von Reinigungspersonal** Das Reinigungspersonal wird vor Vertragsschluss sorgfältig geprüft.
• **Schlüsselregelung/Schlüsselbuch** Die Ausgabe der Schlüssel wird in einer Liste vermerkt.
• **Sorgfältige Auswahl von Sicherheitspersonal** Die Sicherheitsfirma wird vor Vertragsschluss sorgfältig geprüft.
• **Sicherheitsschlösser vorhanden** Es werden Sicherheitsschlösser verwendet.
• **Wachdienst** Die Alarmanlage ist an einen Wachdienst angeschlossen
• **Personenkontrolle Pförtner/Empfang** Es erfolgt eine Personenkontrolle/ bzw. Anmeldung beim Empfang .. Ein alleiniges Eintreten in die Firma ist nicht möglich.
• **Manuelles Schließsystem** Die Büroräume sind mit einem Schlüsselsystem gesichert.
• **Protokollierung der Besucher** Alle Besucher der Firma werden in einem Kalender protokolliert.
• **Chipkarten/Transponder-Schließsystem** Der Zugang erfolgt über Chipkarten-/Transponderschließsystem. Die Ausgabe der Token und die Berechtigungen sind in einer Liste vermerkt.
• **Alarmanlage** Die Räumlichkeiten sind mit einer Alarmanlage gesichert.

1.1.2 Zugangangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **2-Faktor-Authentifzierung** Bei allen Anwendungen, welche die Funktion einer 2-Faktor-Authentifzierung unterstützen, ist dies im Einsatz.
• **Einsatz Firewall** Es wird eine aktuelle Firewall eingesetzt, diese wird automatisch aktualisiert.
• **WLAN für Gäste** Gäste erhalten lediglich per Gast-WLAN einen Zugang zum Internet (Passwort ist zeitlich limitiert gültig).
• **Passwörter verschlüsselt** Passwörter werden einwegverschlüsselt gespeichert und übertragen. Nach definierter Anzahl an Fehlversuchen (je nach System) wird der Zugang gesperrt.
• **Automatisches Sperren Arbeitsrechner** Nach 5 Minuten Inaktivität werden die Clients automatisch gesperrt.
• **Einsatz Anti-Viren-Software** Es wird eine aktuelle Anti-Viren-Software mit aktuellen Definitionen auf den Clients und Servern eingesetzt. Diese wird automatisch aktualisiert.
• **Berechtigungskonzept vorhanden**
• **Authentifikation mit Benutzer + Passwort** Jeder Zugang zu IT-Systemen erfolgt passwortgeschützt. Die Systeme sind restriktiv konfiguriert, nicht benötigte Dienste sind deaktiviert, Standardpasswörter wurden verboten.
• **Passwortrichtlinie vorhanden** Einsatz von Passwortrichtlinien für starke Passwörter in den Systemen mit Nutzerkennungen {Verhinderung der Auswahl schwacher Passwörter) vorhanden
• **Benutzerkennwörter** Regelmäßiger Wechsel von Benutzerkennwörtern
• **Backup-Datenträger: Zugang eingeschränkt** Die Backup-Datenträger werden in verschlossenen Bereichen aufbewahrt. Zugang zu den Backup-Datenträgern haben nur berechtigte Personen.
• **Zuweisung von Benutzerrechten** Die Zuweisung erfolgt ausschließlich funktions- und rollenbasiert.
• **Automatische Updates** Automatisches Einspielen von Sicherheitsupdates des Betriebssystems, der installierten Software
• **Standard-Authentifizierungsinformationen** Standard-Äuthentifizierungsinformationen in Softwareanwendungen des Herstellers werden nach der Installation geändert
• **Regelung zum Sperren von Passwörtern** Regelungen zum automatischen Sperren von Passwörtern nach einem Sicherheitsvorfall

1.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Protokollierung von Zugriffen auf Anwendungen**
• **Erstellen von Benutzerprofilen**
• **Berechtigungen durch Verzeichnisdienst (z.B. AD) zentral verwaltet** Die Zugriffsrechte werden durch die zentrale Vergabe von Zugriffsrechten durch den Verzeichnisdienst oder über Berechtigungseinstellungen innerhalb der Anwendungen sichergestellt.
• **Einsatz von Aktenvernichtern** Kleinere Mengen Papier, mit personenbezogenen Daten, werden ausschließlich durch einen Aktenvernichter vernichtet. Größere Mengen an Papier werden, sollte dies zutreffend sein, einem zertifizierten Aktenvernichter zur sicheren Vernichtung übergeben.
• **Anzahl der Administratoren ist auf ein Minimum begrenzt**
• **Handlungsempfehlungen im Falle eines Virenbefalls für User und Administratoren sind vorhanden**
• **Schutzmaßnahmen zur Sicherung bei Nutzung von eigenen Geräten durch Mitarbeiter (z. B. Fernlöschung oder -sperrung)**

1.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Logische Mandantentrennung (Software)** Alle Anwendungen, welche den Kunden zur Verfügung stehen· und somit personenbezogene Daten enthalten, verfügen über eine Mandantentrennung.
• **Festlegen von Datenbankrechten** Alle Systeme, mit denen personenbezogene Daten verarbeitet werden, sind mandantenfähig bzw. datenbankbasiert, so dass eine Trennung der Daten unterschiedlicher Mandanten möglich ist. Datenbankberechtigungen können dadurch Mandantenbezogen vergeben werden.
• **Versehen der Daten mit Zweckattributen** Daten werden mit Zweckattributen zur Selektion und Zuordnung abgelegt.
• **Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern**
• **Trennung von Produktiv- und Testumgebung**

1.2 Sicherung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben.

1.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Keine Weitergabe personenbezogener Daten an Dritte** Es werden keinerlei personenbezogene Daten an Dritte ohne Einwilligung oder vertragliche Grundlage weitergegeben.
• **Dokumentation der Empfänger von Daten und der Zeitspannen der** • **geplanten Überlassung bzw. vereinbarten Löschfristen** Löschkonzept
• **Bereitstellung über verschlüsselte Verbindungen wie sftp, https**
• **Protokollierung der Zugriffe und Abrufe**

1.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Übersicht der Anwendungen** Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
• **Berechtigungskonzept vorhanden** Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten af Basis eines Berechtigungskonzepts.

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

Maßnahmen, die gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

1.3.1 Verfügbarkeitskontrolle und Belastbarkeitskontrolle

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

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Backup- und Recovery-Konzept** Es erfolgt eine tägliche Datensicherung der Server, die eine Sicherung der Konfigurationsdateien einschließt.
• **Datensicherung**

Es erfolgen regelmäßige Datensicherungen für Unternehmensdaten in Cloudsystemen und externen Rechenzentren
• **Einsatz RAID-System/Festplattenspiegelung**
• **Notfallplan vorhanden** Ein IT-Notfallplan liegt vor
• **Funktion der Backups getestet** Das Funktionieren der Backups wird regelmäßig getestet.

1.3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei physischen oder technischen Zwischenfällen schnell wieder herstellbar sind.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Backup- und Recovery-Konzept** Es erfolgt eine tägliche Datensicherung der Server, die eine Sicherung der Konfigurationsdateien einschließt.

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

Maßnahmen, die gewährleisten, dass personenbezogene· Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

1.4.1 Wirksamkeitsevaluierung

Maßnahmen, die gewährleisten, dass die zuvor eingeführten Maßnahmen weiterhin umgesetzt und ihre Validität besitzen.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Sofortige Information der Geschäftsleitung** (Alarmierungskette vorhanden)
• **Datenschutz-Management-System** Software-Lösung für Datenschutzmanagement
• **Zentrale Dokumentation** Zentrale Dokumentation aller Verfahrens-weisen und Regelungen zum Datenschutz+ ITSicherheit für Mitarbeiter nach Bedarf/Berechtigung
• **Datenschutzfolgeabschätzung** Durchführung von DSFA bei Bedarf
• **Datenschutzbeauftragter (extern) bestellt**
• **Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener**

1.4.2 Umgang mit Datenschutzverletzungen

Maßnahmen, die gewährleisten, dass eventuelle Datenschutzverletzungen frühzeitig erkannt und _sichergestellt werden.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Regelmäßige Schulung Mitarbeiter zum Datenschutz** Es erfolgt mindestens einmal jährlich eine Schulung der Mitarbeiter zum Thema Datenschutz.
• **Datenschutz-Management-System** Software-Lösung für Datenschutzmanagement
• **Prozess Datenschutzvorfälle vorhanden** Meldung binnen 72 Stunden nach Erkennen an die zuständige Aufsichtsbehörde, Verantwortlichen bzw. Information der Betroffenen

1.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO}

Maßnahmen, die gewährleisten, dass Systeme bzw. Produkte, in denen personenbezogene Daten verarbeitet werden, so konzipiert sind, dass sie möglichst wenige personenbezogene Daten benötigen.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Datenminimierung erfolgt aktiv**

1.4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.

Folgende Maßnahmen sind zusätzlich zu den vorgenannten Kontrollen umgesetzt:

Maßnahmen

• **Auftragnehmer bzw. getroffene Sicherheitsmaßnahmen und entsprechende Dokumentation vorab geprüft** vor Vertragsabschluss werden die Dienstleister sorgfältig geprüft
• **Auftragnehmer bzw. dessen Beschäftigte auf das Datengeheimnis verpflichtet**
• **Auftragnehmer werden sorgfältig ausgewählt**
• **Sicherstellung der Vernichtung von Daten durch den Auftragnehmer nach vereinharter Löschfrist**
• **Auftragnehmer sowie ihre Tätigkeiten werden überprüft**

Anlage 3 – Unterauftragnehmer

1. **OVH GmbH**

   Christophstraße 19,
   50670 Köln
   Deutschland
   USt-IdNr.: DE245768940
   Handelsregister: Amtsgericht Saarbrücken - HRB 15369

2. **Contabo GmbH**

   Aschauer Straße 32a
   81549 München
   Deutschland
   Registergericht: AG München
   Registernummer: HRB 180722
   USt.-ID-Nr: DE267602842