Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO

Zwischen der Firma

Expocloud GmbH
Eupener Straße 332
52076 Aachen

- nachfolgend „Auftragnehmer“ genannt –

und der Firma

_____ **(Firmenname)**

_____ **(Straße & Hausnummer)**

_____ **(Postleitzahl & Ort)**

- nachfolgende „Auftraggeber“ genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Der Gegenstand des Auftrags ergibt sich aus den gebuchten Software-Abonnements und deren Leistungsbeschreibung (in der jeweils aktuellen Fassung), auf die hier verwiesen wird.

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: …… (Definition der Aufgaben)

(2) Dauer

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Software-Abbonements.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ 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 6 Wochen gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☒ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in den Leistungsbeschreibungen der gebuchten Software-Abbonements (in der jeweils aktuellen Fassung).

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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☒ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

☐ wird hergestellt durch sonstige Maßnahmen: ..... (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

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

☒ Personenstammdaten

☒ Kommunikationsdaten (z.B. Telefon, E-Mail)

☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☒ Kundenhistorie

☒ Vertragsabrechnungs- und Zahlungsdaten

☒ Planungs- und Steuerungsdaten

☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☒ Interessenten
- ☒ Abonnenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☒ Handelsvertreter
- ☒ Ansprechpartner

Die Verarbeitung betrifft alle in Expocloud registrierten Benutzer.

3. Technisch-organisatorische Maßnahmen (Anlage 1)

(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. Artt. 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 [Einzelheiten in Anlage 1].

(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

(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 Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 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.

☒ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr Dr. Schadowski: Ralf W., Schadowski, ADDAG GmbH & Co. KG, 0049-(0)241-44688-0, info@addag.de bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Artt. 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.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) 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.

h) 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.

i) 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.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse (Anlage 2)

(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.

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

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der in Anlage 2 benannten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO.

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers

sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(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.

(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.

(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);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(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.
(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).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

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

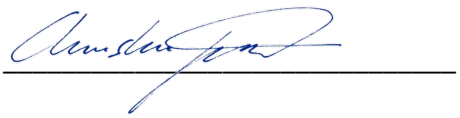
(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(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 der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Für den Auftraggeber:	**Für den Auftragnehmer:**
Name und Funktion:	Dr. Christian Coppeneur-Gülz, CEO:
_____	
Ort, Datum, Unterschrift:	Ort, Datum, Unterschrift:
_____	Aachen, den 05.12.2019

Anlage TOM – Technisch-organisatorische Maßnahmen

Diese stellt der Auftragnehmer dem Auftraggeber in freier Form zur Prüfung zur Verfügung

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

- Zutrittskontrolle
  - Der Zutritt zum Gebäude in Monschau ist nur zur Arbeitszeit zwischen 08 und 18 Uhr möglich. Die Schlüssel können bei Bedarf nach Eintragung in eine Liste von ausgewählten Mitarbeitern abgeholt werden.
  - Der Zutritt zum Serverraum in Monschau wird über die Ausgabe und Protokollierung des Schlüssels geregelt. Dieser liegt bei der Geschäftsleitung und muss bei Bedarf abgeholt werden.
  - Kunden und Besucher erhalten am Empfang einen Besucherausweis.
    Das Firmengelände ist videoüberwacht.
- Zugangskontrolle
  - Der Zugang zu den Systemen ist nur für autorisierte Benutzer möglich. Die Autorisierung erfolgt über sichere Passwörter (min. acht Stellen lang und bestehend aus Buchstaben, Zahlen und Sonderzeichen) und Microsofts Zwei-Faktor-Authentifizierung
  - Auf jedem Gerät ist eine Virenschutzsoftware aktiv
  - Nach 10 Minuten Inaktivität durch den Benutzer wird automatisch der Bildschirm gesperrt. Bei Verlassen des Arbeitsplatzes ist die Sperre manuell zu aktivieren.
  - Auf den Systemen eine Festplattenverschlüsselung eingerichtet.
  - Das interne Netzwerk der WWM ist an allen Standorten durch eine Firewall gesichert. Die Standorte sind dabei mit einer verschlüsselten Site-To-Site-VPN-Verbindung verbunden.
- Zugriffskontrolle
  - Der Zugriff auf personenbezogene Daten erfolgt lediglich von dazu autorisierten Benutzern, die Berechtigungen hierzu werden auf Basis von Active-Directory vergeben.
  - Die Rechtevergabe ist dabei maximal drei Systemadministratoren möglich.
  - Datensätze können nur von den vorgesehenen Nutzern gelesen, kopiert, geändert oder entfernt werden.
  - Das Kopieren von personenbezogenen Daten auf externe Datenträger ist nicht gestattet.
  - Jeder Arbeitsplatz ist mit einem verschließbaren Rollcontainer ausgestattet, in dem nach Arbeitsende jegliche Unterlagen und Geräte einzuschließen sind.
  - Der entfernte Zugriff zur Remoteverwaltung der Geräte wird per TLS mit einem 2048-Bit-RSA-Schlüssel verschlüsselt
- Trennungskontrolle
  - Alle projektrelevanten Daten werden in Abhängigkeit des myWWM Vertragscodes gespeichert und stehen nur für Analysen nach Vorgabe des Verantwortlichen zur Verfügung.
- Pseudonymisierung
  - Die zweckmäßige Verarbeitung erfolgt intern über eindeutig vergebene Identifikationsnummern. Ein Personenbezug kann nicht direkt aus dem System abgelesen werden.
    Erst zur Auftragserfüllung wird ein Personenbezug zu einem Datensatz hergestellt.

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

- Weitergabekontrolle
  Die Daten werden in Microsoft Dynamics NAV verarbeitet. Dabei steuert die Software die Integrität der Datensätze und bietet eine Funktion zur Integritätsprüfung an.
  Die Übertragung der Daten zwischen dem Browser des Bestellers und dem System, auf dem die Verarbeitung erfolgt, ist durch ein SSL-Zertifikat mit hybrider Verschlüsselung geschützt.
- Eingabekontrolle
  Das zertifizierte ERP-System Microsoft NAV verfügt über eine Protokollierung von Änderungen an personenbezogenen Daten. Dabei wird der Inhalt vor und nach der Änderung, sowie der verantwortliche Mitarbeiter und der Zeitpunkt protokolliert.
  Die Protokolldaten werden für 3 Jahre gespeichert.

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

- Verfügbarkeitskontrolle
  Zentrale Backup-Server stehen zum Speichern von Backup-Daten zur Verfügung. Das RAID-1-Festplattensystem reduziert die Wahrscheinlichkeit eines Datenverlustes.
  Alle Backups werden zusätzlich in Microsoft Azure gesichert.

  Die unterbrechungsfreie Stromversorgung (USV) wird durch eine 15-minütige Batterieka-pazität garantiert. Sämtliche USV-Anlagen sind dabei redundant ausgelegt.

  Die Server werden kontinuierlich mit Sicherheitsupdates versehen.

  Die direkte freie Kühlung sorgt für eine umweltschonende Kühlung der IT-Hardware. Die Klimatisierung erfolgt über den Doppelboden.

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

- Incident-Response-Management
  - Monitoring von Datenanpassungen
  - Kameraüberwachung des Firmengeländes
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
  - Manuelle Löschung nach gesetzlicher Vorgabe
  - Manuelle Löschung auf Anforderung
- Auftragskontrolle
  - Auswahl eines Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
  - Auftragnehmer hat Datenschutzbeauftragten bestellt
  - Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Anlage Unterauftragnehmer

1 Microsoft Deutschland GmbH

1.1 Unternehmen

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München
Deutschland

1.2 Leistungen

Hosting

1.3 Datum AV (DSGVO §28)

30.8.2018

2 Hubspot GmbH

2.1 Unternehmen

Hubspot GmbH
Unter den Linden 26
10117 Berlin
Deutschland

2.2 Leistungen

CRM-Software
Ticket-System

2.3 Datum AV (DSGVO §28)

25.5.2018

3 aConTech Enterprise IT-Solutions GmbH

3.1 Unternehmen

aConTech Enterprise IT-Solutions GmbH
Mohnweg 9
90768 Fürth
Deutschland

3.2 Leistungen

IT-Support

3.3 Datum AV (DSGVO §28)

30.08.2018