Vertrag zur Auftragsverarbeitung (AV-Vertrag)

zwischen

Name, Firmierung und Anschrift des Auftraggebers sind dem Hauptauftrag zu entnehmen.

- Auftraggeber = Verantwortlicher -

und

HUBIT e.K., Lise-Meitner-Str. 2, 28359 Bremen

- Auftragnehmer = Auftragsverarbeiter -

Vorbemerkung

Zwischen den Parteien besteht oder wird zeitgleich ein (Haupt-)Vertrag über die Erbringung von Dienstleistungen geschlossen, die eine automatisierte Verarbeitung personenbezogener Daten konkret zum Gegenstand haben bzw. zwangsläufig mit sich bringen oder bei denen ein Zugriff auf personenbezogene Daten aus der unternehmerischen Sphäre des Auftraggebers zumindest nicht ausgeschlossen werden kann, wie es insbesondere bei der Prüfung und Wartung von automatisierten Verfahren oder Datenverarbeitungsanlagen der Fall ist.

Seit dem 25.05.2018 gelten in allen Mitgliedsstaaten der Europäischen Union die Regelungen der Europäischen Datenschutz-Grundverordnung (DSGVO) unmittelbar, in deren Art. 28 die Datenverarbeitung im Auftrag geregelt wird und insbesondere das Erfordernis konkreter Festlegungen in Bezug auf den Datenschutz im Rahmen eines Vertrags oder eines anderen Rechtsinstituts des Unionrechts oder des Rechts eines Mitgliedsstaats enthalten ist. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ordnet die Wartung und Fernzugriffe auf Systeme als Auftragsverarbeitung ein, wenn ein Zugriff auf personenbezogene Daten notwendig oder zumindest möglich ist.

Mit dem vorliegenden schriftlichen oder elektronischen Vertrag werden die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung im Auftrag nach Maßgabe der DSGVO im Einzelnen geregelt.

1. Gegenstand und Dauer des Auftrags

(1) Der zugrundeliegende Auftrag hat im Wesentlichen folgende Dienstleistungen zum Gegenstand:

☐ Webhosting

☐ Domainregistrierung

☐ HUBIT-Cloud:
Bereitstellen eines (virtuellen) Servers
Erstellung einer Datensicherung
Installation von Software-Updates
Benutzerverwaltung

☐ HUBIT Consent-Manager:
Bereitstellen einer Software für die Verwaltung von Einwilligungen auf der Webseite

☐ HUBIT PenTest:
Vorbereitung und Durchführung von Penetrationstests.

☐ HUBIT Webstat:
Bereitstellen eines (virtuellen) Servers
Erstellung einer Datensicherung
Installation von Software-Updates
Benutzerverwaltung

☐ HUBIT Mailexpress
Bereitstellen einer Plattform für den Versand von E-Mails.
Pflege von E-Mailverteillisten
Vorbereitung und Durchführung von Mailingaktionen
Erstellung einer Datensicherung
Installation von Software-Updates
Benutzerverwaltung

Wartung und Support

Im Übrigen wird auf die Leistungsbeschreibung des Hauptvertrags verwiesen.

(2) Die Laufzeit des vorliegenden Vertrags beginnt mit der Unterzeichnung durch beide Parteien und endet zeitgleich mit dem Hauptvertrag, ohne dass es eines gesonderten Beendigungstatbestandes bedarf. Im Hauptvertrag vereinbarte Kündigungsfristen bleiben unberührt.

(3) Der Auftraggeber kann (auch) den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen gesetzliche Datenschutzvorschriften oder Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

2. Konkretisierung des Auftragsinhalts

(1) Art der vom Hauptvertrag vorgesehenen Verarbeitung von personenbezogenen Daten:

Die unter Ziffer 1 beschrieben Aufgaben dienen nicht der Verarbeitung von Daten durch den Auftragnehmer. Sie dienen vielmehr der Bereitstellung und Pflege, der Systeme, die durch den Auftragnehmer für den Auftraggeber bereitgestellt werden.

Bei den unter Ziffer 1 beschriebenen Aufgaben kein eine Einsichtnahme von (personenbezogenen) Daten nicht in allen Fällen ausgeschlossen werden.

Der Auftragnehmer kann Datensicherungen vor Wartungsarbeiten oder auf Weisung des Auftraggebers abfertigen und auf seinen Systemen speichern.

Die unter Ziffer 1 genannten Gegenstände des Auftrags sind nur Gegenstand dieses Vertrags sofern sie durch den Auftraggeber beauftragt wurden.

(2) Hinsichtlich des Zwecks der Verarbeitung wird nach oben auf Ziffer 1. Abs. 1 dieses Vertrags sowie auf den Hauptvertrag verwiesen.

(3) Die Datenverarbeitung findet ausschließlich in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in einen Drittstaat bedarf der vorherigen Zustimmung des Auftraggebers. Die Verlagerung in einen Drittstaat darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind.

(4) Gegenstand der Verarbeitung sind folgende Arten / Kategorien personenbezogener Daten:

☐ 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)

☐ Gesundheitsdaten

☐ Gen-Daten

☐ biometrische Daten

☐ weitere Kategorien von Daten (bitte auflisten):

(5) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Kunden

☐ Interessenten

☐ Abonnenten

☐ Beschäftigte / Bewerber

☐ Lieferanten

☐ Handelsvertreter

☐ Ansprechpartner

☐ weitere Kategorien von Betroffenen (bitte auflisten):

3. Technische und -organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen (TOM) 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 und diesem als Anlage 1 beigefügt. 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 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO 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 durch Austausch der Anlage 1 zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

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.

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 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Der Ansprechpartner beim Auftragnehmer für Datenschutzfragen ist in Anlage 2 benannt.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO, die über das Vertragsende hinaus gilt. 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 anderweitigen Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (siehe Anlage 1).

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

e) 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.

f) 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.

g) 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.

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

6. Unterauftragsverhältnisse

(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 weitere Auftragsverarbeiter als Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der in Anlage 3 benannten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

b) Die generelle Auslagerung auf Unterauftragnehmer und/oder der Wechsel eines bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer dem Auftraggeber das konkrete Vorhaben eine angemessene Zeit vorab schriftlich oder in Textform mit allen relevanten Details anzeigt und
- der Auftraggeber gegenüber dem Auftragnehmer nicht bis zum Zeitpunkt der Übergabe der Daten schriftlich oder in Textform Einspruch gegen das konkrete Vorhaben erhebt und
- der Umsetzung eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zugrunde gelegt wird.

(1) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(2) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, was generell nur mit vorheriger Zustimmung des Auftraggebers gemäß Ziffer 2. Abs. 3 dieses Vertrags zulässig ist, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(3) Eine weitere Auslagerung durch den Unterauftragnehmer 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 DSGVO 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 DSGVO;

- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- 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) Im Falle der Unterbeauftragung erstrecken sich die Kontrollrechte übergreifend auf die gesamte Vertragskette, so dass Auftragnehmer und Unterauftragnehmer auch durch über dem jeweiligen Auftraggeber stehende Auftraggeber kontrolliert werden können.

(5) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer eine gesonderte Vergütung beanspruchen.

8. Mitwirkungspflicht des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen 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, Datenschutzvorfälle im Sinne einer Verletzung von gesetzlichen Datenschutzvorschriften oder Verstößen gegen vertragliche Vereinbarungen bzw. Weisungen des Auftraggebers 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 des Hauptvertrags enthalten und nicht auf eigenes Fehlverhalten des Auftragnehmers zurückzuführen sind, kann dieser eine gesonderte Vergütung beanspruchen. [

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können schriftlich, per Fax, per E-Mail oder mündlich erfolgen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftraggeber kann gegenüber dem Auftragnehmer weisungsberechtigte Personen benennen, wie auch der Auftragnehmer weisungsempfangsberechtigten Personen benennen kann. Die Benennung dieser Personen erfolgt gegebenenfalls in Anlage 2 anhand des Namens, der Funktionsbezeichnung oder der Zugehörigkeit zu einer Personengruppe (z.B. Abteilung). Änderungen und Ergänzungen sind durch Austausch der Anlage 2 zu dokumentieren.

(3) 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 des Hauptvertrags – 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.

Datum: siehe E-Mail- / Auftragsbestätigung

Anlage 1 - Technische und organisatorische Maßnahmen (TOM)

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

- Zutrittskontrolle

  Das Gebäude ist dauerhaft verriegelt und außerhalb der Arbeitszeiten verschlossen.

  Das Gebäude ist mit einer Einbruchmeldeanlage (EMA) gesichert. Die EMA alarmiert mittels

  - akustischem Alarm
  - optischem Signalgeber
  - Direktruf des Wachdienstes
  - Direktruf festgelegter Mitarbeiter des Unternehmens

  Es kommen Sicherheitsschlösser zum Einsatz. Es kommt eine elektronische Zutrittskontrolle zum Einsatz. Ein Schließsystem mit verschiedenen Schließkreisen wird genutzt. Schlüssel können nur bei Vorlage einer Sicherheitskarte nachgemacht werden. Schlüssel (auch elektronische) werden gegen Unterschrift ausgegeben.

  Büroräume und Fenster werden zum Arbeitsende verschlossen durch den letzten Mitarbeiter verschlossen.

  Es ist ein Serverraum vorhanden und fensterlos. Der Serverraum ist stets verschlossen. Nur ein eingeschränkter und schriftlich benannter Personenkreis hat Zutritt zum Serverraum.

  Der Zutritt zum Unternehmen ist unternehmensfremden Personen nur nach Einlass durch einen Mitarbeiter möglich. Besucher werden am Eingang bzw. Empfang persönlich abgeholt und im Unternehmen durchgehend begleitet. Besucher werden grundsätzlich in einem Besprechungsraum empfangen. Besucher haben zu Räumen mit Datenverarbeitungsanlagen (kurz: DVA) nur dann Zutritt, wenn sie ständig beaufsichtigt werden und personenbezogene Daten nicht offen einsehbar sind.

- Zugangskontrolle

  Das Unternehmensnetzwerk ist mittels Firewall gesichert.

  Der Zugang zum Firmennetzwerk erfolgt ausschließlich mittels VPN. Der VPN-Zugang wird gesichert mittels Benutzer-Authentifikation.

  Jede DVA, mit der personenbezogene Daten verarbeitet werden, ist mittels einer Benutzerauthentifizierung auf Betriebssystemebene geschützt. Zusätzlich kommen software-spezifischen Authentifizierungen zum Einsatz.

  Jeder Benutzer hat seine persönlichen Zugangsdaten. Es gibt eine Passwort-Richtlinie, die die Ansprüche an Komplexität und Länge sowie das Änderungsintervall des Passwortes definiert.

  Die Passwort-Vorgaben werden durch eine im Betriebssystem implementierte Passwortrichtlinie durchgesetzt. Es wird eine Passworthistorie angelegt, so dass die letzten 3 Passwörter nicht erneut genutzt werden können.

  Beim Verlassen des Arbeitsplatzes ist die DVA manuell zu sperren (passwortgeschützter Sperrbildschirm).

  Zugänge von Mitarbeitern, die zeitweise oder endgültig nicht im Unternehmen beschäftigt sind, werden gesperrt bzw. gelöscht.

- Zugriffskontrolle

  Anhand der Benutzerauthentifizierung des Betriebssystems werden die Benutzer bestimmten Gruppen zugeordnet.

  Die Zugriffsfreigabe auf Ordner und Dokumente erfolgt durch den *Administrator* mittels ADS (Active Directory Service).

  Es wird ein betriebliches WLAN bereitgestellt. Der WLAN-Schlüssel ist nur einem eingeschränkten Personenkreis bekannt.

  Für Besucher wird ein Gast-WLAN bereitgestellt. Das Gast-WLAN ist mit einem Netzwerkschlüssel geschützt. Das Gast-WLAN ist virtuell vom Firmennetzwerk getrennt. Besucher erhalten einen zeitlich begrenzten Zugang zum Gast-WLAN.

  Es wird Fernwartung durch den Auftragnehmer beim Auftraggeber durchgeführt. Es kommen technische Maßnahmen zum Einsatz, wodurch die jeweilige Fernwartungsverbindung nur mit Einwilligung des Auftraggebers hergestellt werden kann. Der Auftraggeber kann jederzeit die Fernwartungsverbindung trennen. Der Aufbau einer Fernwartungsverbindung erfolgt ausschließlich über in Deutschland beheimatete Verbindungsserver.

  Es wird Fernwartung beim Auftragnehmer durch seine Auftragnehmer durchgeführt. Es kommen technische Maßnahmen zum Einsatz, wodurch die jeweilige Fernwartungsverbindung nur mit Einwilligung des Auftragnehmers hergestellt werden kann. Der Auftragnehmer kann jederzeit die Fernwartungsverbindung trennen.

- Trennungskontrolle

  Die Datentrennung erfolgt durch

  - separate Hardware
  - serverinterne Infrastruktur
  - softwarespezifische Lösungen
  - Ablage in unterschiedlichen Datei-Ordnern
  - Ablage von Papierdokumenten in unterschiedlichen Akten

  Es wird gewährleistet, dass die Daten von verschiedenen Auftraggebern oder unterschiedlichen Zwecken dienende Daten streng voneinander getrennt sind.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) / Anonymisierung
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

  Die Pseudonomisierung und Anonymisierung von Daten erfolgt im Umfang der Weisungen des Auftraggebers.

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

- Weitergabe- / Transportkontrolle

  Festplatten von Notebooks / Netbooks o.ä., auf denen Daten des Auftraggebers verarbeitet werden, sind verschlüsselt.

  Mobile Datenträger (USB-Sticks, externe Festplatten etc.), auf denen Daten des Auftraggebers gespeichert werden, sind verschlüsselt.

  Die Übermittlung von Daten erfolgt verschlüsselt oder/und passwortgeschützt.

  VPN-Verbindungen sind verschlüsselt.

  Daten werden per Email verschlüsselt oder/und passwortgeschützt übermittelt bzw. werden schützenswerte Informationen in einem verschlüsselten Anhang versendet.

  Papiere mit personenbezogenen Daten oder Unternehmensgeheimnissen des Auftraggebers werden mittels handelsüblichen Schreddern zerkleinert. Die Schredder haben folgende Sicherheitsstufe gemäß DIN 66399: P3

  Papiere mit personenbezogenen Daten oder Unternehmensgeheimnissen des Auftraggebers werden in verschlossenen Behältern gesammelt und durch einen Dienstleister mindestens mit der folgenden Sicherheitsstufe gemäß DIN 66399 vernichtet: P3

  Elektronische Datenträger werden low-level-formatiert durch mehrfaches Überschreiben (Wiping) und / oder mechanisch zerstört.

- Eingabekontrolle

  Die Verarbeitung von Daten des Auftraggebers wird mit Zeitstempel protokolliert.

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

- Verfügbarkeitskontrolle

  Betriebssysteme werden automatisch oder manuell aktualisiert.

  Jeder Server ist mit einer Schutzsoftware gegen Schadprogramme (z.B. Computerviren, Trojaner, Ransomware) ausgestattet, die sich mindestens täglich automatisch aktualisiert.

  Jeder Arbeitsplatzrechner, Notebook etc. ist mit einer Schutzsoftware gegen Schadprogramme (z.B. Computerviren, Trojaner, Ransomware) ausgestattet, die sich mindestens täglich automatisch aktualisiert.

  Eine unterbrechungsfreie Stromversorgung (USV) ist installiert. Die USV fängt Spannungsspitzen ab. Bei Stromausfall signalisiert die USV den angeschlossenen Geräten den Stromausfall. Die Geräte werden sodann automatisch heruntergefahren.

  In dem Serverraum verlaufen keine offen verlegten Wasserrohre.

  Vor dem Serverraum befindet sich ein für elektrische Anlagen geeigneter Feuerlöscher.

  Die Server werden mittels Klimaanlage gekühlt.

  Es bestehen mehrere Internetverbindungen. Die Internetverbindungen werden von unterschiedlichen Providern bereitgestellt.

  Die Systeme verfügen über redundante Speichereinheiten.

  Es erfolgt eine automatische Datensicherung in folgendem Turnus: täglich

  Die Datensicherung wird mit einem automatisierten Monitoring überwacht.

Die Datensicherung wird in einem anderen Gebäude gelagert.

Ein etwaiger Transport des Sicherungsmediums erfolgt durch eine sorgfältig ausgewählte Transportperson.

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

  Stichprobenartig wird die Datensicherung manuell geprüft, ob die zu sichernden Daten tatsächlich auf dem Sicherungsmedium gespeichert wurden. Die Stichprobe wird dokumentiert.

  Stichprobenartig wird das Wiederherstellen von Daten aus der Datensicherung getestet.
  Die Stichprobe wird dokumentiert.

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

   - Datenschutz-Management;

     Es existiert ein schriftliches Regelwerk (z.B. Datenschutz-Konzept, Datenschutz-Ordnung und/oder Richtlinien, ggf. Betriebsvereinbarungen) in dem Abläufe, Zuständigkeiten und Vertretungsfälle mit dem Ziel der Gewährleistung und kontinuierlichen Verbesserung des Datenschutzes niedergelegt sind.

     Beschäftigte werden zu Beginn des Arbeitsverhältnisses schriftlich zur Vertraulichkeit verpflichtet.

     Beschäftigte werden mindestens jährlich zum Datenschutz geschult. Die Schulungsteilnahme wird dokumentiert.

     Es sind Prozesse zur Wahrung der Betroffenenrechte etabliert.

   - Auftragskontrolle

     Im Verhältnis zu etwaigen Unterauftragnehmern ist der Auftragnehmer selbst Auftraggeber und prüft als Verantwortlicher deren technische und organisatorische Maßnahmen gemäß der EU DSGVO.

     Der Auftragnehmer prüft, ob beim Unterauftragnehmer ein betrieblicher Datenschutzbeauftragter bestellt ist. Besteht hierfür die gesetzliche Verpflichtung und wird dieser nicht nachgekommen, darf kein Unterauftrag zur Auftragsdatenverarbeitung geschlossen werden.

     Die Auftragskontrolle erfolgt mindestens jährlich und wird dokumentiert.

Technische und organisatorische Maßnahmen im Rechenzentrum

Folgende technische und organisatorische Maßnahmen (TOM) gemäß EU Datenschutz Grundverordnung sind grundlegend für die Datenverarbeitung im genutzten Rechenzentrum (Webhosting, Serverhousing). Ergänzende Maßnahmen und / oder Abweichungen sind gegebenenfalls im jeweiligen Verfahren beschrieben.

1 Vertraulichkeit und Integrität

1.1 Verschlüsselung

Datenübertragungen per SSL, HHTPS, SSH
VPN-Zugänge sind personalisiert.

1.2 Zutrittskontrolle

Alarmanlage
Chipkarten- / Transponder-Schließsystem mit PIN-Code (2-Faktor-Authentifizierung)
Videoüberwachung der Zugänge
Personenkontrolle beim Pförtner / Empfang
Protokollierung der Besucher
Tragepflicht von Berechtigungsausweisen

1.3 Zugangskontrolle

Festlegung und Review von Benutzerrechten
Passwortrichtlinie
Verschlüsselung der Datensicherungssysteme
Sperren externer Schnittstellen
Einsatz von Intrusion Detection System
Einsatz Anti-Viren-Software
Einsatz redundanter Hardware-Firewall

1.4 Zugriffskontrolle

Berechtigungskonzept
Verwaltung der Rechte durch Systemadministrator
Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
Sichere Aufbewahrung on Datenträgern
physische Löschung von Datenträgern vor der Wiederverwendung
Einsatz eines zertifizierten Dienstleister für Aktenvernichtung

1.5 Eingabekontrolle

Protokollierung von Eingaben, Änderung und Löschung von Daten

1.6 Auftragskontrolle

Schriftliche Weisungen von Auftraggebern
Verpflichtung der Mitarbeiter auf Vertraulichkeit (Datengeheimnis)
Sicherstellung der Vernichtung von Daten

2 Verfügbarkeit

Unterbrechungsfreie Stromversorgung
Klimatisierte Serverräume
Überwachung von Temperatur und Feuchtigkeit
Brandmeldeanlage (BMA)
Feuerlöschgeräte
Alarmierung bei unberechtigtem Zutritt oder nicht ordnungsgemäß verschlossenen Türen
Erstellen, Pflege und Test eines Recovery-Konzepts
Erstellen eines Notfallplans
Aufbewahrung von Datensicherungen an einem sicheren und ausgelagerten Ort
Serverräume über Wassergrenze

3 Besondere Datenschutzmaßnahmen

Interne Verhaltensregeln
Risikoanalyse
Wiederanlaufkonzept
Zertifizierung gem. ISO 27001 (Information Security Management System)
Zertifizierung gem. ISO 9001 (Qualitätsmanagement)
Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Anlage 2 - Kontaktpersonen

1. Ansprechpartner für Datenschutzfragen beim Auftragnehmer, falls kein DSB – Ziffer 5. b) AV-Vertrag

Vorname Name	Haye Hösel
Abteilung / Funktion	Inhaber / Geschäftsführer
Rufnummer	0421-33114300
Emailadresse	info@hubit-internet.de

2. Optional: Weisungsempfangsberechtigte Person(en) beim Auftragnehmer – Ziffer 9. Abs. 2 AV-Vertrag

Vorname(n) Name(n)	
und/oder Funktion(en)	Geschäftsführung
und/oder Abteilung(en)	
Rufnummer(n)	0421-33114300
Emailadresse(n)	info@hubit-internet.de

Anlage 3 - Unterauftragnehmer

Der Auftragnehmer bedient sich im Zuge der Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen eines oder mehrerer Dritter als Subunternehmer. Es handelt dabei sich konkret um folgende(s) Unternehmen:

Unternehmen	Anschrift	Aufgabe
STRATO AG	Otto-Ostrowski-Straße 7, 10249 Berlin	Rechenzentrum
Plutex GmbH	Hermann-Ritter-Str. 108 28197 Bremen	Rechenzentrum
IONOS SE	Elgendorfer Str. 57 56410 Montabaur	Rechenzentrum
NETWAYS GmbH	Deutschherrnstr. 15-19 90429 Nürnberg	Rechenzentrum
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Rechenzentrum
netcup GmbH	Daimlerstraße 25 76185 Karlsruhe	Rchenzentrum
LOGABIT GmbH	Agnes-Pockels-Bogen 1 80992 München	Rechenzentrum
Bremen Briteline GmbH	Wiener Str. 5 28359 Bremen	Rechenzentrum
Variomedia AG	August-Bebel-Straße 68 14482 Potsdam	