Vertrag zur Datenschutzvereinbarung gemäß Art. 28 DS-GVO
[Stand: Januar 2019]

Vereinbarung

zwischen dem/der

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

intellior AG

Zettachring 12

D-70567 Stuttgart

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präamble

Dies Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien dies sich aus dem Softwarenutzungsvertrag (im Folgenden Leistungsvereinbarung) ergeben.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Bestellung des BPM|Free Hosting Paketes Bestellnummer: ..... vom ....., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der der möglichen Einsichtnahme (Verarbeitung) personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der oben genannten Leistungsvereinbarung. Sie umfasst insbesondere das Hosting und die Wartung der Anwendung Aeneis für den Auftraggeber.

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.

(2) Art der Daten

Die Art der verwendeten personenbezogenen Daten ist abhängig von den Anwendungsszenarien des Auftraggebers. In den meisten Anwendungsszenarien werden innerhalb der Anwendung Aeneis die folgenden personenbezogenen Daten verwaltet:

- Benutzername (oft Synchron mit Benutzername der Anmeldung an der Windows Domäne)
- Kennwort, wenn keine LDAP Authentifizierung verwendet wird
- Email-Adresse
- Vorname
- Nachname

Da es sich bei Aeneis um ein stark anpassbares Werkzeug zur Unternehmensmodellierung handelt können prinzipiell vom Auftraggeber weitere personenbezogene Daten in das Modell integriert werden.

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

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten bzw. Dienstleister
- Ansprechpartner
- Weitere Kategorien in Abhängigkeit der Nutzung des Systems Aeneis durch den Auftraggeber

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. 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, Daten Portabilität 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:

a) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt:
   Michael Weinmann, Tel.: 0173-763 29 62, E-Mail: michael.weinmann@dsb-office.de.
b) Die Wahrung der Vertraulichkeit gemäß Art. 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.
c) 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 [Einzelheiten in 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 Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer, siehe Anlage 2, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

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 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.

_____, den	_____	_____, den	_____
Ort	Datum	Ort	Datum

_____	_____
- Auftraggeber -	- Auftragnehmer/intellior AG -

Anlage 1 – Technisch-organisatorische Maßnahmen

Alle Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, sind verpflichtet, angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen.

Dieses Dokument enthält eine Übersicht über die bei der intellior AG gemäß Art. 32 EU-DSGVO hierzu umgesetzten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.

Die intellior AG überprüft die getroffenen technischen und organisatorischen Maßnahmen regelmäßig daraufhin, ob sie dem Stand der Technik und den organisatorischen Möglichkeiten entsprechen. Insoweit ist es der intellior AG gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei ist gewährleistet, dass das Sicherheitsniveau der in diesem Dokument festgelegten Maßnahmen nicht unterschritten wird.

Organisationskontrolle

Die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Maßnahmen sind:

- In einer Richtlinie sind die Vorgaben zum Umgang mit personenbezogenen Daten, die Regelungen zur Erfüllung der EU-DSGVO und der Nutzung von IT-Systemen verbindlich geregelt
- Die Intellior AG hat gemäß Art. 37 EU-DSGVO einen fachkundigen und unabhängigen betrieblichen Datenschutzbeauftragten bestellt.
  Kontaktdaten:
  Michael Weinmann, Sielminger Hauptstr. 52/1, 70794 Filderstadt,
  Tel: 0173-763 29 62, Mail: michael.weinmann@dsb-office.de
- Der Beauftragte für den Datenschutz führt ein Verzeichnis über die eingesetzten Verarbeitungstätigkeiten
- Alle Beschäftigte sind gemäß Art. 32, Abs. 4 auf das Datengeheimnis und darüber hinaus arbeitsvertraglich zum vertraulichen Umgang mit Betriebs- und Geschäftsgeheimnissen verpflichtet.
- Alle Beschäftigten werden im Zusammenhang mit der Verpflichtung auf das Datengeheimnis über die Themen Datenschutz und Datensicherheit informiert.
- Beschäftigte mit Zugang zu Vermittlungs- bzw. Telefonanlagen werden auf das Fernmeldegeheimnis nach §88 TKG verpflichtet und entsprechend unterwiesen
- Alle Mitarbeiter werden regelmäßig zu aktuellen Themen des Datenschutzes informiert.

- Die Mitarbeiter werden jährlich zu Themen des Datenschutzes geschult. Das Curriculum der Schulung plant der Beauftragte für den Datenschutz

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

- Zutrittskontrolle
    - Schließanlage mit dokumentierter Schlüsselverwaltung. Zutrittsberechtigungen werden nach einem definierten Verfahren eingeräumt
    - Eigenständige Zutrittsregelung für sensible Bereiche (IT-Serverraum, Personal, etc.)
    - Einbruchshemmung der Zugänge
    - Empfang u. Begleitung betriebsfremder Personen
- Besondere Maßnahmen der Zutrittskontrolle Hosting sind:
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenter-Park
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
- Zugangskontrolle
    - Authentifizierung der Benutzer mit Benutzername u. Kennwort
    - Berechtigungskonzept i.S. eines Rechte-/Rollenkonzeptes, Dokumentation der Rechteerteilung
    - Kennwortrichtlinien mit Mindestanforderungen
    - Bildschirmsperrung mit Kennwortsperre
    - Firewall (Hard- u. Software)
    - VPN-Technologie
- Besondere Maßnahmen der Zugangskontrolle , Cloud Server sind:
    - • Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem

Auftragnehmer nicht bekannt sind
• Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-FaktorAuthentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.

- Zugriffskontrolle
    - Anzahl der Administratoren auf das „Notwendigste“ reduziert
    - Trennung Admin-User von Standard-User des IT-Mitarbeiters
    - Berechtigungskonzept mit schriftlicher Dokumentation
    - Verwaltung der Zugriffsrechte durch Systemadministrator
- Besondere Maßnahmen der Zugriffskontrolle Hosting sind:
    - Protokollierung aller Zugriffe (lesen/schreiben) auf den Passwort-Safe
    - Rollenbasierte Administrationsrechte für VMware Umgebung
- Trennungskontrolle
    - Regelmäßig erfolgt keine Kopie der Daten von Auftraggeber in Systeme des Auftragnehmers. Wenn die Anfertigung von Kopien zur Fehlerbehebung notwendig wird erfolgt dies nur mit Zustimmung des Auftraggebers. Die Daten werden dann logisch von anderen Daten getrennt gehalten und nach Beendigung der Aufgabenerfüllung umgehend gelöscht.
    - Trennung von Produktiv- und Testsystemen (Virtualisierte Server, V-Lan)
- Besondere Maßnahmen Trennungsgebot Hosting sind:
    - Logische Trennung von Kundendaten im Storage-System
    - Trennung des Netzwerkverkehrs durch VLAN-Technologie
- Besondere Maßnahmen der Datenträgerkontrolle beim Hosting sind:
    - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
    - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert)

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

- Weitergabekontrolle
    - Einrichtungen von Standleitungen bzw. VPN-Tunneln
    - Beim physischen Transport sorgfältige Auswahl von Transportpersonal und Fahrzeug

- Sichere Aufbewahrung von Datenträgern
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399-1 ff)
- Verbot der Nutzung mobiler Datenträger für vertrauliche bzw. personenbezogene Daten
- Verschlüsselung von mobilen Geräten wie Notebooks
- Verschlüsselung der Inhalte von Mail-Kommunikation nach Kundenwunsch

- Besondere Maßnahmen der Weitergabekontrolle Hosting sind
  - Nutzung verschlüsselter Datenübertragung
- Besondere Maßnahmen der Eingabekontrolle Hosting sind:
  - Erfassung aller Änderungen durch den Kundendienst im Ticket-System

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

- Verfügbarkeitskontrolle
  - Unterbrechungsfreie Stromversorgung (USV)
  - Schutzsteckdosenleisten in Serverräumen
  - Feuerlöschgeräte vor Serverräumen
  - Serverräume nicht unter sanitären Anlagen
  - Überwachung der Server bzgl. Temperaturentwicklung
  - Ausreichende Klimatisierung
- Besondere Maßnahmen der Verfügbarkeitskontrolle Hosting sind
  - Backup- und Recovery-Konzept mit mind. täglicher Sicherung. Vorhalten der Sicherung für 1 Woche
  - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlagen
  - Dauerhaft aktiver DDoS-Schutz
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
  - Definierte Eskalationsketten mit vorgaben zur Informationsstrategie

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

- Datenschutz-Management
  - Gewährleistung der Nachhaltigkeit des Datenschutzes.

  - Dokumentation des Datenschutzes vorhanden mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf. Regelmäßige Überprüfung der Wirksamkeit erforderlicher Schutzmaßnahmen wird durchgeführt. Die Mitarbeiter sind geschult auf Vertraulichkeit und sind dem Datengeheimnis verpflichtet.
  - Der Auftragnehmer kommt den Informationspflichten nach Art. 13 und 14 DS-GVO nach.

- Incident-Response-Management
  - Unterstützung bei der Reaktion auf Sicherheitsverletzungen
  - Der Auftragnehmer setzt Firewall-, Netzwerk und Spamfiltersysteme in redundanter Form für Umgebungen des Auftragnehmers ein. Die Funktionsweise wird durch regelmäßige Kontrolle und Wartung sichergestellt.
  - Sicherheitsvorfälle werden dokumentiert und ein DSB mit einbezogen.

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
  - Privacy by design / Privacy by default
  - Es werden nicht mehr personenbezogene Daten erhoben, bearbeitet oder verwendet als für den jeweiligen Zweck erforderlich. Eine einfache Ausübung des Wiederrufrechts des Betroffenen ist möglich.

- Auftragskontrolle
  - Es ist eine weisungsgemäße Auftragsverarbeitung zu gewährleisten.
  - Alle Weisungen des Auftraggebers erfolgen schriftlich per E-Mail an unser Ticketsystem, wodurch eine lückenlose Nachvollziehbarkeit gewährleistet ist. Mündliche Absprachen werden im Ticketsystem protokolliert und dem Auftraggeber zur Kontrolle übersendet. Arbeitsanweisung werden durch Mitarbeiter des Auftragnehmers einer Plausibilitätsprüfung unterzogen.
  - Der Auftragnehmer gewährleistet zu jederzeit eine einfache Wahrnehmung der Kontrollrechte des Auftraggebers um das Schutzniveau regelmäßig zu überprüfen.
  - Es werden grundsätzlich keine weiteren Subunternehmer beauftragt, sofern nicht auf ausdrücklichen Wunsch des Auftraggebers.
  - Nach Beendigung des Vertrages werden alle Daten des Auftraggebers übergeben oder gelöscht.
  - Ein Löschkonzept kann auf Anfrage eingesehen werden.

Anlage 2 – Unterauftragnehmer

Unterauftragnehmer	Ort	Leistung
NETWAYS GmbH	Deutschherrnstr. 15-19 DE-90429 Nürnberg	Hosting Services
noris network AG	Thomas-Mann-Straße 16 - 20 DE-90471 Nürnberg	Hosting Services
Hetzner Online GmbH	Industriestr. 25 DE-91710 Gunzenhausen	Hosting Services
STRATO AG	Pascalstraße 10 DE-10587 Berlin	Hosting von FileExchange und Support Portal
Amazon Web Service Inc.	410 Terry Avenue North, Seattle, WA 98109-5, USA	Hosting Service, ausschl. in Dt. Rechenzentrum
ProzessPartner / Mohrbacher Management Systeme	Waldstr. 2 DE-66914 Waldmohr	Entwicklungs-, Projekt- und Implementierungsunterstützung für Anwendungskomponente (Audit-Management)
SHD	SHD System-Haus-Dresden GmbH Drescherhäuser 5b DE-01159 Dresden	Entwicklungs-, Projekt- und Implementierungsunterstützung für Anwendungskomponente (ISMS)