Vertrag über die Auftragsverarbeitung

nach Art. 28 Abs. 3 DSGVO

Zwischen

_____

_____

_____

_____

und

Visisoft OHG

Am Kabutzenhof 21

18057 Rostock

Deutschland

(im Folgenden: Auftragnehmer)

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Das yalst-LiveSupportTool ist eine Software, die Kunden (dem Auftraggeber) u.a. eine Echtzeit-Kommunikation zwischen deren Websitebesuchern des Auftraggebers (genannt Interessenten) und dem Auftraggeber erlaubt. Weiterhin kann das yalst-LiveSupportTool die Aktivitäten der Interessenten auf den Seiten des Auftraggebers direkt wieder geben, beinhaltet vielfältige Statistiken zur gezielten Auswertung der Zugriffe und des Surfverhaltens der Interessenten sowie ein komplettes Werbekampagnen-Management.

Der Auftragnehmer bietet das Hosting der Software auf der Server-Infrastruktur des Auftragnehmers an. Dabei liegen alle Daten über die Aktivitäten der Interessenten und alle weiteren Daten der Interessenten, die Chats, die Software-Einstellungen der Auftraggebers zur Individualisierung der Software sowie die Adresse und Zahlungsdaten der Auftraggebers auf Servern des Auftragnehmers.

Gegenstand des Auftrags zum Datenumgang ist die Durchführung des Hosting der yalst-LiveSupportTool-Software und der damit verbundenen Daten in der Infrastruktur des Auftragnehmers.

(2) Dauer

Die Verarbeitung wird auf unbestimmte Zeit geschlossen. 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

Die Verarbeitung ist folgender Art:

Bei der Bereitstellung des yalst-LiveSupportTools für den Auftragnehmer durch den Auftragnehmer findet auf den Servern grundsätzlich eine Protokollierung der Systemereignisse mit IP-Adresse zur Fehlerbehebung und Abwehr von Angriffen auf die Server des Auftragnehmers statt.

Weiterhin werden Daten des Auftraggebers bezüglich des Vertrags- und Schuldverhältnis gespeichert.

Außerdem kann bei Support- und Betreuungsvorgängen sowie für individuelle Projekte zur Verbesserung oder Anpassung der Software Zugriff auf einige Daten des Auftraggebers (Einstellungen, statistische Daten) erfolgen.

Über das Frontend der Software selbst ist kein Zugriff auf die Chatdaten des Auftraggebers möglich. Allerdings ist dieser über den direkten Zugriff auf die Datenbanken möglich.

Die Verarbeitung dient folgendem Zweck:

Bereitstellung und Hosting eines Live-Supports in Form eines Live-Chats für die unmittelbare und zuverlässige Erreichbarkeit einer Kontaktperson beim Auftraggeber und Ermittlung der Aktivitäten des Besuchers zur Unterstützung der Chatagenten des Auftraggebers.

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.

(2) Art der Daten

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

Allgemeine Log-Files, System- und Errordateien zur Fehlerbehebung und Abwehr von Angriffen auf die Server des Auftragnehmers

Postalische Adressen, Ansprechpartner, E-Mail-Adressen, ggf. Telefonnummern des Auftraggebers zum Vertrags-/Schuldverhältnis, Vertragsanbahnung und zur Kundenbetreuung

Einstellungen in der Software und statistische Daten zur Fehlerbehebung, zum Support und zur Betreuung des Auftragnehmers

Chatdaten des Auftraggebers (Adressen, Telefonnummern, Kunden- und Vertragsnummer usw.)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Kunden des Auftragnehmers
Beschäftige des Auftraggebers
Beschäftige von Dienstleistern des Auftraggebers
Kunden des Auftraggebers
Interessenten des Auftraggebers

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
Als Datenschutzbeauftragter ist beim Auftragnehmer:

Great Oak Datenschutz GmbH & Co. KG
Florian Schirm
Grubenstraße 20
18055 Rostock
Deutschland

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

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 [Auflistung der Unterauftragsverhältnisse in Anlage 2].

(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.

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 aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

(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 (min. 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.

Ort, Datum

Unterschrift Auftraggeber

Name:

Funktion:

Rostock, 22.06.2021

Ort, Datum

Unterschrift Auftragnehmer

Name: Dr. Andreas Beckmann
Funktion: Geschäftsführer Visisoft OHG

Anlagen: Anlage 1 – Technisch-organisatorische Maßnahmen
Anlage 2 – Unterauftragsverhältnisse

Anlage 1 – Technisch-organisatorische Maßnahmen

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

- **Zugangskontrolle** (vormals: Zutrittskontrolle) - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen
  - Sicherheitssysteme in den Rechenzentren der 1&1 IONOS SE im Rahmen der Bereitstellung, Wartung und Reparatur der Server-Hardware zum Schutz der Rohdaten in den Log-Files und Datenbanken (siehe Anlage 2 – Unterauftragsverhältnisse)
  - Sicherheitssysteme in den Rechenzentren der 1&1 IONOS SE (Büro Berlin) im Rahmen der Bereitstellung, Wartung und Reparatur der Server-Hardware für die verschlüsselten Server-Backups (siehe Anlage 2 – Unterauftragsverhältnisse)
  - Sicherheitssysteme (Schlüsselsystem mit speziellen Sicherheitsschlüsseln, gepanzerte Eingangstür, Videoüberwachung mit Bewegungserkennung) in den Büros des Auftragnehmers mit den lokalen Client-Rechnern
  - Schutz der Client-Rechner des Auftragnehmers durch Verschlüsselung der Datenträger

- **Zugriffskontrolle** – Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben
  - Zugriff auf Backup-Daten mit den Rohdaten in den Log-Files und Datenbanken durch die 1&1 IONOS SE im Rahmen der Bereitstellung, Wartung und Reparatur der Server-Hardware (siehe Anlage 2 – Unterauftragsverhältnisse)
  - Zugriff auf Backup-Daten mit den Rohdaten in den Log-Files und Datenbanken durch die 1&1 IONOS SE (Büro Berlin) (siehe Anlage 2 – Unterauftragsverhältnisse) nicht möglich, da diese verschlüsselt sind
  - Zugriff auf die Rohdaten in den Log-Files und Datenbanken nur über spezielle Server-Logins von ausgewählten Berechtigten des Auftragnehmers
  - Zugriff auf alle Daten des Auftraggebers (Vertragsdaten, Softwareeinstellungen, Agentennamen) und die Daten der Besucher (statistische Daten; keine Chatdaten) nur über spezielle Logins von ausgewählten Berechtigten des Auftragnehmers
  - Protokollierung von Zugriffen in speziellen Login-Dateien auf den Servern
  - Keine lokalen Kopien der Backups in der lokalen Infrastruktur des Auftragnehmers oder beim Auftraggeber, bis auf die Daten die auf Wunsch über verschlüsselte Schnittstellen an einige Auftraggeber übertragen werden
  - Schutz der Client-Rechner des Auftragnehmers durch wechselnde, sichere Kennworte und automatische Rechnersperre
  - Schutz der Server des Auftragnehmers durch aktuelle Betriebssysteme (Log-Term-Support), individuell konfigurierte Firewalls mit einer Freigabe von unbedingt benötigten Server-Ports und Intrusion Detection Systeme
  - Wochentägliche, manuelle Kontrolle der Logfiles auf ungewöhnliche Aktivitäten, Logins o.ä.

- **Trennungskontrolle** - Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
    - Mandantenfähigkeit der Software durch verschiedene Datenbanken auf verschiedenen Servern
    - Bei Nutzung desselben Servers durch verschiedene Auftraggeber streng getrennte Instanzen der yalst-Software
    - Bei Instanzierung Trennung der Daten verschiedener Auftraggeber durch separate Tables innerhalb der Datenbanken
    - Trennung der Datenbanken von Test- und Produktivsystemen der Software als auch für einige Auftraggeber

- **Pseudonymisierung & Verschlüsselung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) 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
    - Verschlüsselung der Server-Passworte nach SHA512 (salted)
    - Hashung der Passworte für die Software nach BlowFish128 (salted)
    - Transportverschlüsselung der kompletten Kommunikation zu den Servern des Auftragnehmers nach Transport Layer Security TLS 1.2

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

- **Transport-, Übertragungs-, Datenträger- und Benutzerkontrolle** (vormals: Weitergabekontrolle) - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport sowie Verhinderung der Nutzung automatisierter Verarbeitungssysteme und Gewährleistung der Überprüfung von Stellen, an denen Daten übermittelt oder zur Verfügung gestellt wurden oder werden können
    - Zugriff aus dem Internet auf personenbezogene Daten nur über verschlüsselte Server-to-Server- oder Server-to-Client-Verbindungen (TLS 1.2)
    - Zugriff aus dem Internet auf lokale Rechner in den Büros des Auftragnehmers nur über Virtual Private Networks (VPN)
    - Keine lokalen Kopien der Server-Backups in der lokalen Infrastruktur des Auftragnehmers oder beim Auftraggeber, bis auf die Daten die auf Wunsch über verschlüsselte Schnittstellen an einige Auftraggeber übertragen werden

- **Eingabekontrolle** - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
    - Protokollierung von Zugriffen in speziellen Login-Dateien auf den Servern
    - Protokollierung von Änderungen und Löschungen in speziellen Log-Dateien

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

- **Verfügbarkeitskontrolle** - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
    - Automatische Prüfung der Verfügbarkeit, der Load und verschiedenster Services (E-Mail, Webserver usw.) auf den Servern
    - Regelmäßige Images und Snapshots in der Infrastruktur der 1&1 IONOS SE

- Automatische tägliche und wöchentliche verschlüsselte Backups auf einem anderen Server in einem anderen Rechenzentrum (1&1 IONOS SE (Büro Berlin))
- Wochentägliche, manuelle Erfolgskontrolle der Backups
- Keine lokalen Kopien der Backups in der lokalen Infrastruktur des Auftragnehmers oder beim Auftraggeber, bis auf die Daten die auf Wunsch über verschlüsselte Schnittstellen an einige Auftraggeber übertragen werden
- Schutz der Server des Auftragnehmers durch individuell konfigurierte Firewalls mit einer Freigabe von unbedingt benötigten Server-Ports und Intrusion Detection Systemen

- **Rasche Wiederherstellbarkeit**
  - Einfache Umstellung auf gespeicherte Images oder Snapshots
  - Einfache Wiederherstellung der Skripte und der Datenbank durch Einspielen der Backups auf dem anderen Rechenzentrum

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

- **Datenschutz-Management**
  - Ständige Beratung durch den Datenschutzbeauftragten
  - Ständige Beschäftigung mit aktuellen Datenschutzthemen
  - Schulungen bezüglich Datenschutz
  - Ständige Verbesserungen in der yalst-Software als auch in der internen Infrastruktur des Auftragnehmers
  - Nutzung der Datenschutzmanagement-Software Otris-Privacy

- **Incident-Response-Management:**
  - Meldepflicht beim Datenschutzbeauftragten
  - Meldepflicht bei der zuständigen Datenschutzbehörde

- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO)
  - Bereitstellung von verschiedenen Datenschutzhinweisen in der Software
  - Opt-In für den Besucher beim Starten des Chats in der Software (ab yalst-Version 9.5, Mai 2018)
  - Verschlüsselung aller personenbezogenen Daten in den Datenbanken der Software (ab yalst-Version 9.7, Ende 2018)
  - Konfigurierbare Anzeigenamen für die Agenten in der Software
  - Feingliedriges Rechtesysteme für Agenten und Administratoren in der Software

- **Auftragskontrolle** - Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers
  - Eindeutige Vertragsgestaltung bei Aufträgen durch den Auftraggeber
  - Verhinderung von Zugriff durch externe Dienstleister des Auftragnehmers
  - Vorabüberzeugungspflicht
  - Nachkontrollen
  - Eindeutige Arbeitsanweisungen

Anlage 2 – Unterauftragsverhältnisse

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

Firma Unterauftragnehmer	Anschrift/Land	Leistung
1&1 IONOS SE (Büro Berlin)	Greifswalder Str. 207, 10405 Berlin, Deutschland	Bereitstellung, Wartung und Reparatur der Server-Hardware für das Backup der Software
1&1 IONOS SE	Elgendorfer Straße 57, 56410 Montabaur, Deutschland	Bereitstellung, Wartung und Reparatur der Server-Hardware für das Hosting der Software