Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen dem/der

Vorname:	
Nachname:	
Firma:	
Straße, Hausnummer:	
PLZ, Ort:	
E-Mail:	

- Verantwortlicher - nachstehend „*Auftraggeber*“ genannt -

und der

der boo video GmbH

Billstr. 103, 20539 Hamburg

vertreten durch René Bormann

- Auftragsverarbeiter - nachstehend „*Auftragnehmer*“ genannt -

1. Gegenstand der Vereinbarung

Gegenstände des Verträge zur Auftragsverarbeitung sind:

- Bereitstellung der Videokonferenzen über https://boo.eu inklusive des
- Kundenprotals https://admin.boo.eu.

(1) Der Auftraggeber beauftragt den Auftragnehmer die in einem gesonderten Vertrag spezifizierten Dienstleistungen im Bereich Telekommunikation zu erbringen. Dies sind vorrangig die **Bereitstellung von Videokonferenzen** und die damit zusammenhängenden Leistungen wie Einrichtung der Konferenzen mit Zugangsrechten, Hosting von Daten, Verwaltung von Zugangsdaten und Kundenoberflächen, Beratung, Schulung und technischer und nichttechnischer Support.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages. Die vertraglich vereinbarte Dienstleistung wird **ausschließlich in** einem Mitgliedsstaat der **Europäischen Union** oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2. Laufzeit und Kündigung

- Dieser Vertrag beginnt und endet mit dem Servicevertrag „Beta1“ der Parteien über Konferenzleistungen, sofern nicht die Parteien etwas anderes in Textform vereinbaren.
- 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 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

3. Art und Zweck der Verarbeitung

Die Verarbeitung erfolgt über elektronische Systeme zur Bereitstellung der Konferenzdienstleistungen, einschließlich der Systeme zur Kommunikation mit Kunden und Interessenten.

Der Zweck sind

- Erbringung unsere Dienstleistung, die Auftragsbearbeitung und die Kundenkommunikation und –hilfe (Konferenzen)
- Abrechnung und Inkasso (Abrechnung)

Eine Weitergabe an Dritte zu Marketingzwecken erfolgt nicht..

Art der personenbezogenen Daten:

- Kundendaten: Name/Vorname/Anrede/Titel/Adressdaten/Rufnummer/E-Mail-Adresse
- Vertragsdaten/Bestelldaten (Konferenzen)
- Inhalte und Metadaten der Kommunikation (Konferenzen)
- Abrechnungsdaten: Bankverbindungsdaten/Kreditkartendaten/Bonitätsdaten, Daten zum Zahlungsverhalten (Abrechnung)

Kategorien betroffener Personen:

- Kunden
- Konferenzteilnehmer

4. 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. Die Kosten für eine individuelle Anpassung/Mehraufwand trägt der Auftraggeber.

(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.

5. Berechtigung, Einschränkung und Löschung von Daten

(4) 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) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. 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) 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.

b) 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].

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

d) 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.

e) 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.

f) 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.

g) Ansprechpartner für den Datenschutz beim Auftragnehmer ist René Bormann.
h) Ein Datenschutzbeauftragter ist beim Auftragnehmer nicht benannt, da keine gesetzliche Verpflichtung besteht.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

7. Unterauftragsverhältnisse

(6) 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.

(7) Der Auftragnehmer informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer (weitere Auftragsverarbeiter), wodurch der Auftraggeber die

Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

j) Der Auftraggeber stimmt der Beauftragung der in **[Anlage 2]** aufgeführten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO.

k) 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.

8. 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.

9. 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.

10. Weisungsbefugnis des Auftraggebers

(1) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, welches er durch Einzelweisungen konkretisieren kann.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format.

(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.

(4) Weisungsberechtigte Personen des Auftraggebers sind:
(wenn abweichend von Seite 1, Verantwortlicher / Auftraggeber: Name, E-Mail Adresse)
Vorname:
Nachname:
E-Mail:

(5) Weisungsempfänger beim Auftragnehmer ist:

(5) René Bormann, Geschäftsführer boo video GmbH
Billstraße 103, 20539 Hamburg / E-Mail: support@boo.eu

(6) Für Weisung zu nutzende Kommunikationskanäle:

Die Weisung erfolgt ausschließlich nach Anmeldung über die Webseite boo.eu

boo video GmbH
Billstraße 103
20539 Hamburg
Tel.: +49 (0) 40 / 99999952
E-Mail: support@boo.eu

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

11. 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.

12. Haftung

Die Haftung richtet sich nach den gesetzlichen Vorschriften.

13. Sonstiges

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Der Gerichtsstand für beide Parteien ist der Sitz des Auftragnehmers.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer (boo.eu)

Anlage 1 – Technische und organisatorische Maßnahmen

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

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwerten.

Verwaltung / Büro

- Das Gebäude ist zwischen 18:00 Uhr und 7:00 Uhr abgeschlossen
- Unsere Räume sind immer verschlossen und durch ein elektronisches Schließsystem gesichert. Die Türen sind nur mit Chip zu öffnen
- Die Ausgabe der Schlüssel und Chips wird protokolliert
- Besucher und Fremdpersonal werden zum gewünschten Ansprechpartner begleitet und sind immer unter ständiger Aufsicht durch einen Mitarbeiter in unseren Räumen.
- Wir wählen unser Reinigungspersonal sehr sorgfältig aus.

Rechenzentrum

- Alarmanlage
- Absicherung von Gebäudeschächten
- Videoüberwachung der Zugänge
- Bewegungsmelder
- Sicherheitsschlösser
- Biometrisches Zugangssystem
- Keykarten
- Schlüsselregelung, Schlüsselbuch
- Personenkontrolle bei Zutritt, inklusive Protokollierung (Besucherbuch)
- Automatische Protokollierung der Schließungen
- Sorgfältige Auswahl des Reinigungspersonal
- Sorgfältige Auswahl des Wachpersonal

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme des Auftragnehmers von Unbefugten genutzt werden können.

- Authentifizierung von Anwendern über Benutzername und Passwort
- Verwendung von Berechtigungsrollen für Web-Software
- Jeder Client-PC ist mit Antivirus-Software ausgestattet
- Einsatz von VPN bei Remote-Zugriffen
- Einsatz von Intrusion-Detection-Systemen

- Richtlinien „Sicheres Passwort“, „Clean Desk“ und „Manuelle Desktopsperre“
- Kein Zugang externer Dienstleister außerhalb der Geschäftszeiten

3. Zugriffskontrolle

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

- Verwaltung der Rechte durch internen Systemadministrator.
- Anzahl der Administratoren auf das „Notwendigste“ reduziert. Hinterlegtes Systemadministrator-Passwort bei der Unternehmensleitung.
- Passwortrichtlinie inkl. Passwortlänge, regelmäßiger Passwortwechsel
- Einsatz von Aktenvernichter Stufe 4
- Verschlüsselung von sensiblen E-Mail Anhängen (ZIP-Datei mit Passwort)
- Physische Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von Datenträgern inkl. Protokollierung.

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Physikalische Trennung der Systeme, Datenbanken und Datenträgern
- Logische Kunden- / Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem

5. Pseudonymisierung (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 sind nicht anwendbar.

- Nutzung von Pseudonymisierung wo möglich

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

1. Weitergabekontrolle

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

- E-Mail-Verschlüsselung per TLS Protokoll
- Bereitstellung über sftp und https
- Eigens initiierte Fernwartung bei Verwendung externer IT-Dienstleister
- Versand per E-Mail im ZIP Format. Passwort kennen nur Sender und Empfänger

2. Eingabekontrolle

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

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts. Umsetzung durch Gruppen-, Rollenverteilung
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind.

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

1. Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

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

<u>Verwaltung / Büro</u>

- Einsatz einer Hardware-Firewall
- Backup- & Recovery-Konzept: 7 Tage granulare Wiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Wartungsverträge mit geeigneter Reaktionszeit
- Passender Hardware-Servicevertrag
- Notfallplan

Rechenzentrum

- Unterbrechungsfreie Stromversorgung (USV)
- Notstromaggregat
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Geschütze Steckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlage
- Vorliegendes Backup- und Recovery-Konzept für interne Systeme – Kundensysteme werden auftragsgemäß eingebunden
- Datensicherungen werden in separatem Brandabschnitt vorgehalten

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

1. Datenschutz-Management, Incident-Response-Management, Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DS-GVO)

- Alle Mitarbeiter des Auftragnehmers und seiner Dienstleister werden bei Beginn ihrer Tätigkeit unmittelbar auf die Wahrung der Vertraulichkeit von personenbezogenen Daten und die Wahrung des Postgeheimnisses verpflichtet.
- Es existiert ein Verfahren zum Incident-Response-Management (Meldung von Datenpannen).
- Es werden bei der Planung und Entwicklung von Systemen datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) gewählt.

2. Auftragskontrolle

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

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Keine Verarbeitung von Daten im Auftrag im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:
    - formalisiertes Auftragsmanagement
    - strenge Auswahl von Dienstleistern
    - Kontrollen und Nachkontrollen von Dienstleistern
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Vertragsstrafen bei Verstößen

Anlage 2 – Unterauftragsverarbeiter

1. n@work Internet Informationssysteme GmbH

n@work GmbH
Wandalenweg 35
20097 Hamburg

Folgende Daten werden über Internet Informationssysteme GmbH **transportiert** (während des Transports über das Internet verschlüsselt):

- Audioströme (AES 256 verschlüsselt)
- Videoströme (TLS verschlüsselt)
- Realtime Events (z.B. Betreten/Verlassen des Raumes, Chatnachrichten, Benutzung des Pausebuttons)

Folgende Daten werden über Internet Informationssysteme GmbH verarbeitet:

- Kundendatenbank
- Backend Services: Authentifizierungsservice, Benutzerservice (E-Mailadressen, Rechnungsdaten, Benutzerdaten)

2. Hetzner

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Deutschland
Rechenzentrum (ISO 27001-zertifiziert):

Folgende Daten werden über Hetzner transportiert (während des Transports über das Internet verschlüsselt):

- - Audioströme (AES 256 verschlüsselt)
- - Videoströme (TLS verschlüsselt)
- - Realtime Events (z.B. Betreten/Verlassen des Raumes, Chatnachrichten, Benutzung des Pausebuttons)

3. 1&1 IONOS SE

1&1 IONOS SE
Elgendorfer Str. 57
56410 Montabaur
Deutschland
Rechenzentrum (ISO 27001-zertifiziert): Momentan **nicht aktiv**, d.h. derzeit werden dort keine personenbezogenen Daten transportiert oder verarbeitet.

Bei Bedarf setzen wir dieses Rechenzentrum für Audioströme (AES 256 verschlüsselt), Videoströme (TLS verschlüsselt) oder Realtime Events ein.

4. noris

noris network AG
Thomas-Mann- Straße 16 - 20
D-90471 Nürnberg
Deutschland
Rechenzentrum (ISO 27001-zertifiziert): Momentan **nicht aktiv**, d.h. derzeit werden dort keine personenbezogenen Daten transportiert oder verarbeitet.

Bei Bedarf setzen wir dieses Rechenzentrum für Audioströme (AES 256 verschlüsselt), Videoströme (TLS verschlüsselt) oder Realtime Events ein.

5. Open Telekom Cloud

Open Telekom Cloud
Telekom Deutschland GmbH
Landgrabenweg 151
53227 Bonn
Rechenzentrum (ISO 27001-zertifiziert): Momentan **nicht aktiv**, d.h. derzeit werden dort keine personenbezogenen Daten transportiert oder verarbeitet.

Bei Bedarf setzen wir dieses Rechenzentrum für Audioströme (AES 256 verschlüsselt), Videoströme (TLS verschlüsselt) oder Realtime Events ein.

6. Strato

Strato AG
Pascalstraße 10
10587 Berlin
Rechenzentrum (ISO 27001-zertifiziert): Momentan **nicht aktiv**, d.h. derzeit werden dort keine personenbezogenen Daten transportiert oder verarbeitet.

Bei Bedarf setzen wir dieses Rechenzentrum für Audioströme (AES 256 verschlüsselt), Videoströme (TLS verschlüsselt) oder Realtime Events ein.

7. SysEleven

SysEleven GmbH
Umspannwerk – Aufgang C
Ohlauer Straße 43
10999 Berlin
Rechenzentrum (ISO 27001-zertifiziert): Momentan **nicht aktiv**, d.h. derzeit werden dort keine personenbezogenen Daten transportiert oder verarbeitet.

Bei Bedarf setzen wir dieses Rechenzentrum für Audioströme (AES 256 verschlüsselt), Videoströme (TLS verschlüsselt) oder Realtime Events ein.

8. billwerk GmbH

Mainzer Landstraße 51
60329 Frankfurt am Main
Subscription Management Software und Recurring Billing Service:

Folgende Daten werden von der billwerk GmbH verarbeitet (während des Transports über das Internet verschlüsselt):

- Kundendaten:
  Name/Vorname/Anrede/Titel/Rechnungsadresse/Rufnummer/E-Mail-Adresse
- Vertragsdaten/Bestelldaten
- Abrechnungsdaten: Bankverbindungsdaten/Kreditkartendaten Daten zum Zahlungsverhalten (Abrechnung)