Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

[Unternehmen]
- als Verantwortlichem/r, im Folgenden Auftraggeber genannt -

und

der **Elara Digital GmbH, Chausseestraße 103, 10115 Berlin**
- als Auftragsverarbeiter, im Folgenden Auftragnehmer genannt -

Präambel
Ziel dieser Vereinbarung

Der Auftraggeber hat den Auftragnehmer mit der Erbringung von Leistungen im Bereich „Software as a Service“ und Hosting beauftragt.

Diese Vereinbarung zur Auftragsverarbeitung (im Folgenden „Vereinbarung“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich insbesondere aus Art. 28 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) ergeben.

Sie findet Anwendung auf sämtliche Tätigkeiten, bei denen der Auftragnehmer oder durch ihn beauftragte und vom Auftraggeber zuvor genehmigte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten oder mit diesen in Berührung kommen können. Soweit im Folgenden von „Daten“ die Rede ist, sind damit im Zweifel personenbezogene Daten des Auftraggebers gemeint.

§ 1
Gegenstand und Dauer der Vereinbarung
(zu Art. 28 Abs. 3 DSGVO)

Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den im jeweiligen Vertragsverhältnis gemachten Angaben. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber i.S.v.Art.4 Nr.2 und Art.28 DSGVO auf Grundlage dieses Auftrags.

§ 2
Umfang, Art und Zweck der Auftragsverarbeitung, Art der Daten, Kreis der Betroffenen
(zu Art. 28 Abs. 3 DSGVO)

2.1 Beschreibung des Verarbeitungsprozesses (Art. 4 Nr.2 DSGVO)

Art und Zweck der Verarbeitung

Die Verarbeitung von personenbezogenen Daten durch den Auftragnehmer erfolgt im Rahmen und dient der Ermöglichung der Nutzung der angebotenen Software durch den Auftraggeber und dessen Mitarbeiter.

2.2 Art der personenbezogenen Daten (Art. 4 Nr.1 DSGVO):

<u>Kundendaten</u>
- Name (Vorname, Nachname)
- Telefonnummer
- E-Mail-Adresse
- Profilbild
- Kommentare

<u>Mitarbeiterdaten des Kunden</u>
- Name (Vorname, Nachname)
- Telefonnummer
- E-Mail-Adresse
- Profilbild
- Kommentare

2.3 Kategorien betroffener Personen:

- Kunde
- Mitarbeiter des Kunden

§ 3
Weisungen und Weisungsbefugnisse
(zu Art. 28 Abs. 3 lit. a, 29 DSGVO)

3.1 Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers iSv Art. 28 DSGVO (Auftragsverarbeitung), dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch „Weisungsrecht"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

3.2 Weisungen werden vom Auftraggeber grundsätzlich schriftlich erteilt; mündlich erteilte Weisungen sind vom Auftraggeber in Textform zu bestätigen. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung, solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

§ 4
Technische und organisatorische Maßnahmen, Datenschutz- und Datensicherheitskonzept
(zu Art. 28 Abs. 3 lit. c DSGVO)

4.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern. Die Einhaltung der in diesem Vertrag niedergelegten Pflichten wird er mit geeigneten Mitteln nachweisen.

4.2 Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden „Mitarbeiter" genannt), in Schriftform zur Vertraulichkeit verpflichten (Art. 28 Abs. 3 lit. b DSGVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

4.3 Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DSGVO, insbesondere die in Anlage 1 zu diesem Vertrag aufgeführten Maßnahmen, zu

ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrechtzuerhalten.

4.4 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß Anlage 1 nicht mehr ausreichend sind und wird sich mit ihm hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.

4.5 Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der in Anlage 1 bestimmten technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen.

§ 5
Pflichten des Auftragnehmers
(zu Art. 28 Abs. 3 lit. b, e, f DSGVO)

5.1 Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens aber innerhalb von 48 Stunden nach Kenntnis in elektronischer Form informieren. Maßgeblich zur Wahrung der Frist ist der Zugang beim Auftraggeber. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldungen enthalten jeweils zumindest die in Art. 33 Absatz 3 DSGVO genannten Angaben.

5.2 Der Auftragnehmer wird den Auftraggeber in den vorgenannten Fällen bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen. Der Auftragnehmer wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.

5.3 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle gemäß § 7 dieses Vertrages erforderlich sind. Ferner wird der Auftragnehmer dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung stellen.

5.4 Der Auftragnehmer ist auf Anforderung des Auftraggebers verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten

Tätigkeiten der Verarbeitung gem. Art. 30 Absatz 2 DSGVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

5.5 Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.

5.6 Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat. Die vollständigen Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber mit Vertragsschluss in Textform zu übermitteln. Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

5.7 Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

5.8 Alle Daten des Auftraggebers sind in einer geeigneter Form abgespeichert, so dass sie eindeutig zu identifizieren sind und eine Vermischung mit anderen Kunden ausgeschlossen ist.

§ 6
Unterauftragsverhältnisse
(zu Art. 28 Abs. 2, Abs. 3 lit. d, Abs. 4 DSGVO)

6.1 Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen nicht zur Begründung von Unterauftragsverhältnissen mit Subunternehmern ("**Subunternehmerverhältnis**") befugt. Ausnahmen sind nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers im Einzelfall zulässig; diese gilt für die in Anlage 2 genannten Subunternehmen als erteilt. In jedem Fall hat der Auftragnehmer dafür Sorge zu tragen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den von ihm beauftragten Subunternehmen gelten, wobei dem Auftraggeber gegenüber dem Subunternehmer sämtliche Kontrollrechte gemäß diesem Vertrag einzuräumen sind. Subunternehmerverhältnisse zu Dritten außerhalb des Europäischen Wirtschaftsraumes sind nicht gestattet.

6.2 Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste,

Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

§ 7
Kontrollrechte des Auftraggebers, Duldungs- und Mitwirkungspflichten des Auftragnehmers
(zu Art. 28 Abs. 3 lit. h DSGVO)

7.1 Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung aller datenschutzrechtlicher Vorgaben und getroffenen Vereinbarungen, insbesondere der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (s. Anlage 1), zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen. Der Auftragnehmer kann die Nachweise im Einzelfall durch die Einhaltung genehmigter Verhaltensregeln gem. Art. 40, 41 DSGVO oder durch ein geeignetes und genehmigtes Zertifizierungsverfahren gem. Art. 42 DSGVO erbringen.

7.2 Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

7.3 Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8
Rückgabe überlassener Datenträger und Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags
(zu Art. 28 Abs. 3 lit. g DSGVO)

8.1 Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der

Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragnehmer auf Verlangen an den Auftragsgeber herauszugeben.

8.2 Der Auftragnehmer wird dem Auftraggeber die Löschung schriftlich bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

§ 9
Ort der Verarbeitung
(zu Art. 28 Abs. 3 lit. a DSGVO)

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, sofern dieser die Anwendung der DSGVO beschlossen hat, statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Der Auftraggeber ist zur Zustimmung nicht verpflichtet. Er ist in seiner Entscheidung diesbezüglich frei. Der Auftragnehmer trägt dafür Sorge, dass im Falle der Übermittlung in ein Drittland die besonderen gesetzlichen Voraussetzungen erfüllt sind (Art. 44 ff. DSGVO).

§ 10
Vertragsbeendigung

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Wenn der Hauptvertrag aufgrund Aufhebungsvereinbarung, ordentlicher Kündigung oder außerordentlicher Kündigung endet, endet auch diese Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ohne Kündigung des Hauptvertrags ist unzulässig.

§ 11
Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

§ 12
Schlussbestimmungen

12.1 Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich erfolgen. Dies gilt auch für eine Abweichung von diesem Schriftformerfordernis. Änderungen und Ergänzungen bedürfen des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt.

12.2 Sollte eine Bestimmung dieser Vereinbarung unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die Parteien verpflichten sich, anstelle der unwirksamen Bestimmung eine der unwirksamen Bestimmung möglichst nahekommende, wirksame Bestimmung zu vereinbaren.

12.3 Es gilt deutsches Recht. Der Gerichtsstand richtet sich nach den Regelungen im Hauptvertrag.

Anlage 1
Datenschutz- und Datensicherheitskonzept

A. Vertraulichkeit (Art. 32 Abs. lit. b DSGVO)

1. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

a. Maßnahmen am Unternehmenssitz

Alarmanlage mit Verbindung zu Wachdienst oder Polizei	Schriftliche Regelungen zur Zutrittsberechtigung
Automatisches Zugangskontrollsystem	Manuelles Schließsystem
Chipkarten / Transpondersysteme	Sicherheitsschlösser
Biometrische Zugangssperren	Empfang / Rezeption / Pförtner
Liste der ausgegebenen Schlüssel/Transponder wird geführt	Mitarbeiterausweise sind mitzuführen
Schließsystem mit Codesperre	Videoüberwachung
Besucherbuch / Protokoll der Besucher	Besucherausweise werden ausgegeben
Arbeitsbereiche und für Besucher zugängliche Bereiche sind voneinander abgegrenzt	Besucher haben Zutritt zu allen Gebäudebereichen
Zutritt für Besucher nur mit Vertraulichkeitsverpflichtung	Besucher für die gesamte Dauer ihres Besuchs in Begleitung durch Mitarbeiter
Sorgfalt bei Auswahl externer Dienstleister, die Zutritt zum Gebäude erhalten (Wachpersonal, Reinigungsdienste, Handwerker, …)	Alle externen Dienstleister (Wachpersonal, Reinigungsdienste, Handwerker, …) müssen vor erstmaligem Zutritt zum Gebäude eine Vertraulichkeitsverpflichtung unterzeichnen
Schriftliche Regelung zur Auswahl und Überprüfung externer Dienstleister	Weitere Maßnahmen:

b. Maßnahmen bzgl. Serverräumen

Alarmanlage mit Verbindung zu Wachdienst oder Polizei	Schriftliche Regelungen zur Zutrittsberechtigung
Automatisches Zugangskontrollsystem	Manuelles Schließsystem
Chipkarten / Transpondersysteme	Sicherheitsschlösser
Biometrische Zugangssperren	Serverräume abgegrenzt (Sperrbereich)
Liste der ausgegebenen Schlüssel/Transponder wird geführt	Zahl der Personen, die Serverräume betreten dürfen, auf ein Minimum begrenzt
Schließsystem mit Codesperre	Videoüberwachung
Keine Erteilung von Zutrittsberechtigungen für Besucher	Weitere Maßnahmen

2. Zugangskontrolle

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

Schriftliche Regelungen zur Erteilung von Benutzeraccounts vorhanden	Protokollierung von Vergabe und Entzug von Benutzeraccounts
Erteilung von Benutzeraccounts nur durch Administratoren	Nur personalisierte Benutzeraccounts
Login mit biometrischen Daten	Login mit Benutzername + Passwort

Richtlinie für Passwortsicherheit vorhanden (Mindestvorgabe für Passwortlänge und -komplexität)	Einhaltung der Richtlinie für Passwortsicherheit wird technisch erzwungen
Regelmäßiger Passwortwechsel erforderlich	Zugangssperre bei erfolglosen Anmeldeversuchen
Protokollierung erfolgloser Anmeldeversuche	Automatische Bildschirmsperre
Mitarbeiter müssen ihren Desktop beim Verlassen des Arbeitsplatzes sperren	Richtlinie Datenschutz und Datensicherheit vorhanden, aktuell in Ausarbeitung
Anti-Viren-Software für Server	Anti-Viren-Software für Clients
Anti-Viren-Software für mobile Geräte	Firewall
Jede genutzte Anti-Viren-Software und Firewall wird regelmäßig aktualisiert	Intrusion Detection Systeme
Mobile Device Management	Mobile Device Policy
Gehäuseverriegelung	Einsatz VPN bei Remote-Zugriffen
Verschlüsselung von Notebooks / Tablets *Bitlocker, FileVault.*	Verschlüsselung von Datenträgern *Bitlocker, FileVault.*

3. **Zugriffskontrolle**

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Benutzerberechtigungskonzept vorhanden	Minimale Anzahl an Administratoren
Protokollierung von Vergabe und Entzug von Berechtigungen	Erteilung von Berechtigungen nur durch Administratoren
Erteilung von Zugriffsrechten nach dem need-to-know-Prinzip	Erteilung von differenzierten Berechtigungen (z.B. read-only, read-and-write, …)
Erstellen von Benutzerprofilen	Regelmäßige Überprüfung der erteilten Berechtigungen
Protokollierung von versuchten und erfolgten Zugriffen auf Anwendungen und/oder Daten	Richtlinie zur sicheren Löschung/Vernichtung von nicht mehr verwendeten Datenträgern
Datenträger-Management (Regelung der Ausgabe; Verbot der Nutzung eigener Datenträger)	Weitere Maßnahmen:

4. **Trennungskontrolle**

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

Trennung von Produktiv- und Testumgebung	Trennung der Daten verschiedener Verantwortlicher
Physikalische Trennung	Logische Trennung
Trennung über Berechtigungskonzept	*Weitere Maßnahmen:*

5. **Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**

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.

Pseudonymisierung von Daten ist möglich bei Bedarf	Personenbezogene Daten werden so schnell wie möglich pseudonymisiert
Trennung der Zuordnungsdaten zur Aufhebung der Pseudonymisierung in getrenntem und abgesichertem System	Personenbezogene Daten werden anonymisiert (eine erneute Zuordnung zu Personen ist egal mit welchem Aufwand unmöglich)
Aufhebung der Pseudonymisierung nur bei gesetzlicher Grundlage und nur einzelnen	Weitere Maßnahmen:

Mitarbeitern möglich, die speziell im Datenschutzrecht geschult wurden	

B. **Integrität (Art. 32 Abs. 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-Mails, die personenbezogene Daten enthalten, werden ausschließlich verschlüsselt versendet	Bereitstellung von personenbezogenen Daten nur über verschlüsselte Verbindungen
Versand von Datenträgern (Papier oder elektronisch) über Post, Boten oä	Sorgfältige Auswahl von Transportpersonal und Fahrzeugen
Verwendung sicherer Transportbehälter	Dokumentation von Datenempfängern sowie der Dauer der geplanten Überlassung bzw. der vereinbarten Löschfristen
Weitergabe von Daten nur in anonymisierter Form	Weitergabe von Daten nur in pseudonymisierter Form
Einsatz von VPN bei remote Zugriff	Protokollierung bei jedem Abruf von Daten
Protokollierung regelmäßiger Abruf- und Übermittlungsvorgänge	Fernwartung von Systemen, in denen personenbezogene Daten des Verantwortlichen gespeichert werden
Sperre externer Schnittstellen (z.B. USB)	Clean-Desk-Policy
Datenschutztresor vorhanden	Richtlinie zur Löschung und Vernichtung von Datenträgern
Aktenschredder	Externer Aktenvernichter Anbieter: Shred-IT

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.

a) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers überwiegend auf den IT-Systemen des Auftraggebers. Für diese Verarbeitungen sind keine Angaben zur Eingabekontrolle beim Auftragnehmer erforderlich. Es gelten in Bezug auf die Eingabekontrolle die folgenden technischen und organisatorischen Maßnahmen des Auftraggebers, für deren Ein- und Aufrechterhaltung der Auftraggeber verantwortlich ist:
   - Die Eingabe, Veränderung und Löschung von personenbezogenen Daten wird durch eine revisionssichere Protokollierung in den jeweiligen Anwendungen nachgehalten.
   - Detaillierte Berechtigungskonzepte der Anwendungen werden systemseitig implementiert und vorgenommene Änderungen im Ticketsystem dokumentiert.
   - Die durchgeführten Aktivitäten werden protokolliert, und die Protokolle regelmäßig geprüft.
   - Durch die Überwachung von Protokolldateien werden die Verantwortlichen bei kritischen Operationen technisch alarmiert.

b) Soweit in Einzelfällen eine Verarbeitung personenbezogener Daten des Auftraggebers auf den IT-Systemen des Auftragnehmers erfolgt, z.B. durch übermittelte Screenshots von Fehlermeldungen oder Testdatenbestände o.ä., geschieht dies ausschließlich zu Analysezwecken. Diese Daten werden nicht in veränderter Form zur Weiterverwendung an den Auftraggeber zurück übermittelt, sondern nach der abgeschlossenen Analyse beim Auftragnehmer gelöscht. Für diese Daten sind daher keine gesonderten Maßnahmen zur Eingabekontrolle erforderlich; durch die vorstehend unter A. 1. bis 4 aufgeführten Maßnahmen ist jedoch gewährleistet, dass nur berechtigte Personen beim Auftragnehmer auf diese Daten zugreifen können und der Zugriff nachvollzogen werden kann.

C. **Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. lit. b, c DSGVO)**

1. **Verfügbarkeitskontrolle**

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

a. Allgemeine Maßnahmen

Nutzung eines Spamfilters	Schriftliches Back-up- und Recovery-Konzept
Automatische regelmäßige Datensicherung	Angemessen häufige Sicherung der Daten
Aufbewahrung der Sicherungsmedien an einem sicheren Ort	Aufbewahrungszeit für Back-ups schriftlich geregelt
Feuer- und Rauchmeldeanlagen	Unterbrechungsfreie Stromversorgung
Aufbewahrungszeit für Back-ups von der Löschfrist der gesicherten Daten abhängig	Weitere Maßnahmen:

b. Maßnahmen bzgl. Serverräumen

Feuer- und Rauchmeldeanlagen	Feuchtigkeitsüberwachung
Temperaturüberwachung	Schutzsteckdosenleisten
Klimatisierung	Unterbrechungsfreie Stromversorgung
Festplattenspiegelung	Alarmmeldung bei unberechtigtem Zutritt
Keine sanitären Anschlüsse im oder oberhalb des Serverraums	Getrennte Partitionen für Betriebssysteme und Daten
Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)	Weitere Maßnahmen:

2. **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)**

Maßnahmen, die gewährleisten, dass bei zufälliger Zerstörung oder zufälligem Verlust von Daten diese rasch wiederhergestellt werden können.

Regelmäßige Tests zur Datenwiederherstellung	Protokollierung der Ergebnisse der Tests zur Datenwiederherstellung
Weitere Maßnahmen:	

D. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. lit d DSGVO)**

1. **Datenschutzmanagement (Art. 25 Abs. 1 DSGVO)**

Maßnahmen, die sicherstellen, dass stets alle datenschutzrechtlichen Anforderungen eingehalten werden.

Software-Lösungen für Datenschutzmanagement im Einsatz	Schriftliches Datenschutz- und Datensicherheitskonzept vorhanden
Zentrale Dokumentation aller Verfahrensweisungen und Regelungen zum Datenschutz, jederzeit verfügbar für Mitarbeiter (nach Bedarf/Berechtigung)	Mindestens jährliche Überprüfung der Wirksamkeit der Schutzmaßnahmen; im Bedarfsfall erfolgt Anpassung der Schutzmaßnahmen
Dokumentation der Überprüfung der Wirksamkeit der Schutzmaßnahmen	Zertifizierung vorhanden
Vorhandensein eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 2 DSGVO – aktuell noch in Bearbeitung	Regelmäßige Überprüfung und Aktualisierung des Verarbeitungsverzeichnisses -
Regelmäßige Schulung aller Mitarbeiter (Datenschutz sowie Datensicherheit)	Alle Mitarbeiter auf Vertraulichkeit/Datengeheimnis verpflichtet oder unterliegen gesetzlicher Schweigepflicht

Bei entsprechender gesetzlicher Verpflichtung erfolgt die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO	Weitere Maßnahmen:

2. **Incident-Response-Management**

Maßnahmen zur Sicherstellung der schnellen und angemessenen Reaktion auf Sicherheitsverletzungen.

Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und potenziellen Datenschutzverstößen	Formaler Prozess und klare Regelung der Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenschutzverstöße
Regelmäßige Kontrolle der ausselektierten Dateien / der protokollierten Angriffsversuche bei automatisierten Schutzinstallationen	Dokumentation aller Sicherheitsvorfälle und Datenschutzverstöße
Regelung der Verantwortlichkeit der Meldung von Sicherheitsvorfällen und Datenschutzverstößen an den Verantwortlichen	Weitere Maßnahmen:

3. **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**

Maßnahmen, die gewährleisten, dass die Prinzipien Privacy by design und Privacy by default eingehalten werden.

Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich	Einfache Ausübung von Betroffenenrechten möglich
Automatische Löschung von Daten nach Zweckfortfall sichergestellt	Weitere Maßnahmen:

4. **Auftragskontrolle**

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

Sorgfältige Auswahl von Subdienstleistern in Bezug auf Datenschutz und Datensicherheit	Schriftliche Regelung, was bei der Auswahl von Subdienstleistern zu beachten ist
Dokumentation des Auswahlprozesses	Weisungsbefugnisse sind klar festgelegt
Abschluss der notwendigen Verträge (Auftragsverarbeitungsvertrag oder Standardvertragsklauseln) wird durch entsprechende Richtlinien sichergestellt	Auftragsverarbeitungsverträge entsprechen den Anforderungen des Art. 28 DSGVO
Vereinbarung von Vor-Ort-Kontrollen beim Subdienstleister	Laufende, regelmäßige Überprüfung des Subdienstleisters und seines Schutzniveaus
Der Einsatz weiterer Dienstleister durch den Subdienstleister wird unterbunden	Der Subdienstleister darf seinerseits weitere Dienstleister einsetzen
Sämtliche Anforderungen aus dem Auftragsverarbeitungsvertrag mit dem Verantwortlichen werden auch vertraglich mit dem Subdienstleister vereinbart	Weitere Maßnahmen:

Anlage 2
Liste der Unterauftragnehmer

Unterauftragnehmer	Anschrift / Land	Dienstleistung
Microsoft	Unter den Linden 17, 10117 Berlin	Server-Hosting, Azure-Blob Storage

Abschätzung zu US-Datentransfers Microsoft:

Risiken, die sich aus US-Sicherheitsvorschriften ergeben: Foreign Intelligence Surveillance Act (FISA), Abschnitt 702: Gemäß Abschnitt 702 des FISA kann die Regierung der Vereinigten Staaten „Anbieter elektronischer Kommunikationsdienste“ zwingen, Informationen über Nicht-US-Bürger, die sich außerhalb der Vereinigten Staaten befinden, offenzulegen, um Informationen für ausländische Nachrichtendienste zu erlangen. EO 12333 und Presidential Policy Directive 28 („PPD-28“): Gemäß EO 12333 können US-Geheimdienste (wie die U.S. National Security Agency) Überwachungen außerhalb der Vereinigten Staaten durchführen. Insbesondere sind die US-Nachrichtendienste befugt, ausländische „Signals Intelligence“-Informationen zu sammeln, d. h. Informationen, die aus der Kommunikation und anderen Daten gewonnen werden, die über Funk, Draht und andere elektromagnetische Mittel übertragen werden oder zugänglich sind.

Risikoniveau für die betroffenen Personen: Microsoft Deutschland GmbH ist ein europäisches Tochterunternehmen von Microsoft aus den USA. Ein Zugriff aus den USA ist daher nicht auszuschließen. Hier werden durch den Auftragnehmer lediglich die folgenden Daten von [UNTERNEHMEN] verarbeitet:

- Name (Vorname, Nachname)
- Telefonnummer
- E-Mail-Adresse
- Profilbild

Es werden dabei typischerweise keine Informationen verarbeitet, bei denen der Verdacht besteht, dass ein Wissen der US-Sicherheitsbehörden besondere Risiken für die Nutzer darstellt.

Grundlage für die Datenübermittlung in die USA: EU Standard Vertragsklauseln von Microsoft: https://learn.microsoft.com/de-de/compliance/regulatory/offering-eu-model-clauses bzw. Transatlantic Privacy Framework

Technische Sicherheitsvorkehrungen: Die „supplementary measures“ von Elara Digital GmbH werden als Anlage 2a diesem Vertrag beigefügt.

Organisatorische Maßnahmen: Die „supplementary measures“ von Elara Digital GmbH werden als Anlage 2a diesem Vertrag beigefügt.

Anlage 2a

Technische Sicherheitsvorkehrungen:

- Art der verwendeten Datenverschlüsselung:
  - Es werden mehrere starke Verschlüsselungsprotokolle und Technologien eingesetzt, um die Sicherheit und Vertraulichkeit der Daten zu gewährleisten. Dies beinhaltet den Einsatz von Technologien wie Transport Layer Security/Secure Sockets Layer (TLS/SSL) für sichere Datenübertragungen, Internet Protocol Security (IPSec) für gesicherte Internetkommunikation und Advanced Encryption Standard (AES) für die robuste Verschlüsselung von Daten. Diese Maßnahmen bieten einen hohen Schutz gegen unbefugten Zugriff und Datenlecks. Für weitere Informationen besuchen Sie https://learn.microsoft.com/de-de/purview/encryption.
- Systeme und Prozesse für Überwachung und Incident Response:
  - Fortschrittliche Überwachungssysteme und Incident-Response-Prozesse sind implementiert, um proaktiv Sicherheitsvorfälle zu überwachen und darauf zu reagieren. Diese Systeme überwachen kontinuierlich die IT-Infrastruktur, erkennen Anomalien und ungewöhnliche Aktivitäten und ermöglichen eine schnelle Reaktion bei Sicherheitsvorfällen. Detaillierte Informationen finden sich unter https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure-monitoring.

Organisatorische Maßnahmen:

- Standorte der Rechenzentren und deren Datenschutzstandards:
  - Die Standorte der Rechenzentren sind strategisch in Deutschland, speziell in Frankfurt, gewählt, um den strengsten Datenschutzstandards und -gesetzen zu entsprechen. Dies stellt sicher, dass Daten innerhalb der EU gespeichert und verarbeitet werden, was den Anforderungen der DSGVO entspricht. Weitere Details finden Sie unter https://azure.microsoft.com/de-de/explore/global-infrastructure/data-residency/#overview.
- Art der vertraglichen Vereinbarungen mit Unterauftragnehmern bezüglich Datenschutz:
  - Es wird sichergestellt, dass alle Unterauftragnehmer strenge Datenschutzvereinbarungen einhalten, die den DSGVO-Bestimmungen entsprechen. Dies beinhaltet vertragliche Zusicherungen zur Einhaltung der Datenschutzstandards, regelmäßige Überprüfungen und Audits sowie die Verpflichtung zur sofortigen Meldung von Datenschutzverletzungen. Zusätzliche Informationen finden Sie unter https://learn.microsoft.com/de-de/compliance/regulatory/gdpr?view=o365-worldwide verfügbar.

Anlage 3

Datenschutzbeauftragter

Dominik Adamowski
Brunsbütteler Damm 356
13591 Berlin
Telefon: +49 176 4733 8214
dominik@getelara.de