

Auftragsverarbeitungsvertrag

Zwischen

.....

.....

.....

- Im folgenden Auftraggeber genannt -

Und der

Splitbot GmbH

Seelandstr. 1, Geb. 6

23569 Lübeck

- Im folgenden Auftragnehmerin genannt -

Inhalt

Präambel.....	2
§ 1 Gegenstand/Umfang der Beauftragung.....	2
§ 2 Weisungsbefugnisse des Auftraggebers.....	2
§ 3 Schutzmaßnahmen der Auftragnehmerin.....	3
§ 4 Informationspflichten der Auftragnehmerin.....	3
§ 5 Sonstige Verpflichtungen der Auftragnehmerin.....	4
§ 6 Subunternehmerverhältnisse.....	4
§ 7 Kontrollrechte.....	5
§ 8 Rechte der betroffenen Personen und deren Anfragen.....	5
§ 9 Laufzeit dieses Vertrages.....	6
§ 10 Löschung und Rückgabe nach Vertragsende.....	6
§ 11 Haftung.....	6
§ 12 Schlussbestimmungen.....	6
Anlagen.....	7

Präambel

- (1) Zwischen dem Auftraggeber und der Auftragnehmerin wird folgender Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen. Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten im Rahmen der Bereitstellung von KI-gestützten Dienstleistungen.

§ 1 Gegenstand/Umfang der Beauftragung

- (1) Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass die Auftragnehmerin Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend **"Auftraggeberdaten"**) erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO verarbeitet.
- (2) Die Anlage 1 zu diesem Vertrag enthält eine Auflistung bzgl. Art, Umfang, Zweck der Datenverarbeitung und Kreis der von der Datenverarbeitung betroffenen Personen. Die Verarbeitung der Auftraggeberdaten durch die Auftragnehmerin erfolgt ausschließlich in dem dort genannten Umfang.
- (3) Die Verarbeitung der Auftraggeberdaten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Abweichend hiervon ist die Datenübermittlung an die in Anlage 3 ausgewiesenen Drittlandverarbeiter zulässig, sofern die dort genannten Transfermechanismen nach Art. 44 ff. DSGVO eingehalten werden. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.
- (4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen die Auftragnehmerin und ihre Beschäftigten oder durch die Auftragnehmerin Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

§ 2 Weisungsbefugnisse des Auftraggebers

- (1) Die Auftragnehmerin verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers 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 die Auftragnehmerin durch das Recht der Europäischen Union oder der Mitgliedstaaten, der sie unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt sie dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.
- (2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform (z.B. E-Mail) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

- (3) Die Parteien teilen der jeweils anderen Partei die Kontaktdaten der weisungs- und empfangsberechtigten Personen mit. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Bis zum Zugang dieser Mitteilung bei der jeweiligen Partei gelten die benannten Personen weiter als weisungs-, und empfangsberechtigt.
- (4) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch von der Auftragnehmerin zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
- (5) Ist die Auftragnehmerin der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat sie den Auftraggeber unverzüglich darauf hinzuweisen. Die Auftragnehmerin ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Die Auftragnehmerin darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 3 Schutzmaßnahmen der Auftragnehmerin

- (1) Die Auftragnehmerin 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.
- (2) Ferner wird die Auftragnehmerin alle Personen, die von ihr mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden "Mitarbeiter" genannt), in Schriftform zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen. Auf Verlangen des Auftraggebers wird die Auftragnehmerin dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.
- (3) Die Auftragnehmerin wird ihre innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie trifft, alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DSGVO, insbesondere die in Anlage 2 zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.
- (4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt der Auftragnehmerin vorbehalten, wobei sie sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 4 Informationspflichten der Auftragnehmerin

- (1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen der Auftragnehmerin, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch die Auftragnehmerin, bei ihr im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird die Auftragnehmerin den Auftraggeber unverzüglich in Schriftform oder elektronischer Form informieren. Dasselbe gilt für Prüfungen der Auftragnehmerin durch die Da-

tenschutz-Aufsichtsbehörde. Die Meldungen enthalten jeweils zumindest folgende Informationen:

- a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
 - b. eine Beschreibung der von der Auftragnehmerin ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (2) Die Auftragnehmerin wird den Auftraggeber im Falle des § 4 Abs. 1 bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen. Die Auftragnehmerin trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierrüber den Auftraggeber und ersucht um weitere Weisungen. Die Auftragnehmerin ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.
- (3) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 3 Abs. 3 wird die Auftragnehmerin den Auftraggeber unverzüglich unterrichten.

§ 5 Sonstige Verpflichtungen der Auftragnehmerin

- (1) Die Auftragnehmerin und gegebenenfalls ihr Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung (Verarbeitungsverzeichnis), das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.
- (2) An der Erstellung des Verarbeitungsverzeichnisses durch die Auftragnehmerin hat der Auftraggeber im angemessenen Umfang mitzuwirken. Er hat der Auftragnehmerin die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
- (3) Die Auftragnehmerin ist unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen verpflichtet, den Auftraggeber bei der Einhaltung seiner Pflichten aus Art. 32-36 DSGVO zu unterstützen.
- (4) Die Auftragnehmerin bestätigt, dass sie – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat. Im Falle der Pflicht zur Benennung eines Datenschutzbeauftragten veröffentlicht die Auftragnehmerin die stets aktuellen Kontaktdaten des Datenschutzbeauftragten auf ihrer Internetseite.
- (5) Sollten die Auftraggeberdaten bei der Auftragnehmerin durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die Auftragnehmerin den Auftraggeber unverzüglich darüber zu informieren, sofern ihr dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Die Auftragnehmerin 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.

§ 6 Subunternehmerverhältnisse

- (1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. Die Auftragnehmerin ist im Rahmen ihrer vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Sie setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Die Auftragnehmerin ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Die Auftragnehmerin hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat die Auftragnehmerin sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Die Auftragnehmerin wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.
- (2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn die Auftragnehmerin 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 die Auftragnehmerin für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht der Auftragnehmerin, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

§ 7 Kontrollrechte

- (1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen der Auftragnehmerin. Hierfür kann er z. B. Auskünfte der Auftragnehmerin einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen der Auftragnehmerin nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zur Auftragnehmerin steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe der Auftragnehmerin dabei nicht unverhältnismäßig stören.
- (2) Die Auftragnehmerin verpflichtet sich, dem Auftraggeber auf dessen Anforderung (schriftlich oder in Textform) innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen der Auftragnehmerin erforderlich sind.
- (3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es der Auftragnehmerin mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er die Auftragnehmerin unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Ver-

meidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber der Auftragnehmerin die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Rechte der betroffenen Personen und deren Anfragen

- (1) Die Auftragnehmerin unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.
- (2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber der Auftragnehmerin geltend, so reagiert diese nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 9 Laufzeit dieses Vertrages

- (1) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags bzw. der zwischen den Parteien bestehenden Geschäftsbeziehung. Dieser Vertrag gilt aber mindestens solange fort, wie die Geschäftsbeziehung z. B. durch die aufeinanderfolgende Einzelbeauftragung, zwischen den Parteien fortbesteht.
- (2) Die vorliegende Vereinbarung bleibt zudem über das Ende des Hauptvertrags hinaus solange gültig, wie die Auftragnehmerin über personenbezogene Daten verfügt, die ihr vom Auftraggeber zugeleitet wurden oder die sie für diesen erhoben hat.

§ 10 Löschung und Rückgabe nach Vertragsende

- (1) Die Auftragnehmerin wird dem Auftraggeber nach Beendigung des Hauptvertrags bzw. der bestehenden Geschäftsbeziehung oder jederzeit auf dessen Anforderung alle ihr überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Dies betrifft auch etwaige Datensicherungen bei der Auftragnehmerin. Die Auftragnehmerin hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sowie Datenträger sind nach DIN 66399 zu vernichten.
- (2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten bei der Auftragnehmerin in geeigneter Weise zu kontrollieren.
- (3) Die Auftragnehmerin ist verpflichtet, auch über das Ende des Hauptvertrags bzw. der bestehenden Geschäftsbeziehung hinaus die ihr im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

§ 11 Haftung

- (1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zur Auftragnehmerin alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.
- (2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 Schlussbestimmungen

- (1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch die Auftragnehmerin i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.
- (2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.
- (3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
- (4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Sitz des Auftragsverarbeiters (Lübeck).

Ort, Datum und Unterschrift (Auftraggeber)

Ort, Datum und Unterschrift (Auftragnehmerin)

Anlagen

Anlage 1

Beschreibung der Art der personenbezogenen Daten, besonderen Kategorien personenbezogener Daten und Kategorien betroffener Personen.

Art der personenbezogenen Daten	Umfang und Zweck der Datenverarbeitung	Kategorien betroffener Personen
Identifikationsdaten (Name, Benutzername, E-Mail-Adresse)	- Bereitstellung kontextuell relevanter und faktenbasierter Antworten	- Nutzer des Chatbot-Systems
Kontakt Daten (Telefonnummer, Anschrift)	- Abfrage und Durchsuchung interner Wissensdatenbanken	- Kunden
Kommunikationsinhalte und -verlauf	- Indexierung und Vektorisierung von Dokumenten	- Mitarbeiter
Zeitpunkt und Dauer der Interaktion	- Anreicherung der Modellantworten mit abgerufenen Informationen	- Autoren von Dokumenten in der Wissensbasis
Gerätedaten und technische Informationen (IP-Adresse, Browser-Typ, Betriebssystem)	- Verknüpfung von Nutzeranfragen mit relevanten Dokumenten	- Dritte, die in der Kommunikation erwähnt werden
Standortdaten	- Verbesserung der Antwortgenauigkeit durch zusätzlichen Kontext	
Dokumenten- und Wissensbasen-Zugriffsdaten	- Optimierung der Relevanzkriterien für Dokumentensuche	
Nutzerkontext und vorherige Interaktionen	- Sicherstellung der Aktualität der bereitgestellten Informationen	
Feedback-Daten zur Relevanz der Antworten	- Quellenangaben und Nachvollziehbarkeit der generierten Antworten	

Anlage 2

Technisch und organisatorische Maßnahmen (TOM)

Stand 01.04.2026

Das vorliegende Dokument beschreibt die Anforderungen und die Umsetzung der Maßnahmen zum sicheren und datenschutzkonformen Umgang mit personenbezogenen Daten, um ein dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau zu gewährleisten. Das o.g. Unternehmen erfüllt diesen Anspruch durch folgende Maßnahmen:

(Werkstandorte Rechenzentren Hamburg und Lübeck)

Zutrittskontrolle

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

- Alarmanlage
- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Schließsystem mit Codesperre
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal

Zugangskontrolle

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

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort

- Zuordnung von Benutzerprofilen zu IT-Systemen
- Gehäuseverriegelungen
- Einsatz von VPN-Technologie
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

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.

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)

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.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln

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

Auftragskontrolle

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

- Auswahl der Auftragnehmerin unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an die Auftragnehmerin (z. B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 DSGVO
- Verpflichtung der Mitarbeiter der Auftragnehmerin auf das Datengeheimnis (§ 5 BDSG)

Verfügbarkeitskontrolle

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

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- und Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Serverräume nicht unter sanitären Anlagen
- In Hochwassergebieten: Serverräume über der Wassergrenze

Trennungsgebot

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

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

(Werkstandorte außerhalb der Rechenzentren Hamburg und Lübeck)

Zutrittskontrolle

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

- Videoüberwachung der Zugänge
- Zutrittssperren mit Transpondersystemen
- Schlüsselregelung (z. B. Schlüsselausgabe)

- Besucherregelung
- Verschlussene Serverräume mit separater Zutrittskontrolle
- Sorgfältige Auswahl von Wachpersonal

Zugangskontrolle

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

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern
- Einsatz von Anti-Viren Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz von Hardware-Firewall
- Einsatz von Software-Firewall

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigungen 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.

- Einsatz rollenbasierter Berechtigungskonzepte
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Sichere Aufbewahrung von Datenträgern
- Physische Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Richtlinie: Clean Desk Policy

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.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln

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

Auftragskontrolle

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

- Auswahl der Auftragnehmerin unter Sorgfältigkeitspunkten (insbesondere hinsichtlich Datensicherheit)
- Schriftliche Weisungen an die Auftragnehmerin (z. B. durch Auftragsdatenverarbeitungsvertrag) i. S. d. Art. 28 DSGVO
- Verpflichtung der Mitarbeiter der Auftragnehmerin auf das Datengeheimnis (§ 5 BDSG)

Verfügbarkeitskontrolle

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

- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen

Datenschutzmanagement

Maßnahmen zur Überwachung der Einhaltung der Bestimmungen zum Datenschutz in angemessener Weise.

- Einsatz von digitaler Datenschutzmanagement-Lösung
- Regelmäßige Überprüfung des Stands der Technik
- Regelmäßige Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen (jährlich)
- Benennung eines internen Datenschutzbeauftragten
- Mitarbeiter geschult auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Überprüfung der Verarbeitungsprozesse
- Regelmäßige Überprüfung der Auftragsverarbeiter
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener

Anlage 3

Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind vom Auftraggeber genehmigte Subunternehmer:

Name und Anschrift des Unter-Auftragsverarbeiters	Beschreibung der Teilleistungen	Ort der Leistungserbringung
Kontor Business IT GmbH Seelandstraße 1 Gebäude 6, D-23569 Lübeck	Hosting der Chatbotsysteme	Deutschland, Hamburg und Lübeck
Google Ireland Limited Gordon House, Barrow Street, Dublin 4, Irland	Durchführung von Internetsuchanfragen bei Aktivierung durch den Nutzer; Übermittlung der zur Suchdurchführung erforderlichen Prompt- Inhalte; systemseitig deaktivierbar	EU (Irland); Weiterübermittlung an Google LLC (USA) als weiteren Unterauftragsverarbeiter. Absicherung der Drittlandübermittlung durch den Angemessenheitsbeschluss zum EU-US Data Privacy Framework (Art. 45 DSGVO), ergänzend durch Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO).