Auftragsverarbeitungsvertrag

mit Anlage der technischen und organisatorischen Maßnahmen gemäß
Art. 28 DS-GVO

zwischen

Kunde gemäß „AGB“
– nachfolgend „**Auftraggeber“** genannt –

und
AirLST GmbH, Seitzstr. 23, 80538 München
– nachfolgend „**Auftragsverarbeiter“** genannt –

§ 1 Auftragsgegenstand

Der Auftragsverarbeiter erfüllt Dienstleistungen oder andere Arbeiten für den Auftraggeber. Im Rahmen des Auftrags werden personenbezogene Daten des Verfügungsbereichs des Auftraggebers an den Auftragsverarbeiter übergeben und durch ihn verarbeitet. Es liegt in der ausschließlichen Verantwortung des Auftraggebers, die Art und den Umfang des Zugriffs auf Daten des Auftraggebers zu bestimmen.
Der vorliegende Vertrag zur Auftragsdatenverarbeitung beinhaltet folgende personenbezogenen Daten:

1	Firmenname
2	Vorname
3	Nachname
4	Geschlecht
5	E-Mail-Adresse
6	Weitere Daten, dessen Art der Auftraggeber bestimmt und die vom Auftraggeber in das System des Auftragnehmers geladen werden.

Von Gästen, die mit einer Landingpage interagieren, werden darüber hinaus gespeichert:

1	IP-Adresse
2	Browser
3	Zeitpunkt der Interaktion

Folgende Dienstleistungen werden erbracht:

1	Bereitstellung der SaaS-Lösung AirLST Suite für die eigenständige Nutzung durch den Auftraggeber zur Organisation und Durchführung eines digitalen Gästemanagements mit der Möglichkeit des E-Mail-Versands durch den Veranstalter an die Gäste, Online-Registrierung der Gäste über die zugehörigen Webseiten sowie Check-In der Gäste über die Check-In App. Darüber hinaus werden die Daten für die weitere Auswertung inkl. Statistiken zur Erfolgsmessung des Gästemanagements verarbeitet.
2	Erbringung von Support-Leistungen (z. B. Erstellung von Events, Datenimport, Templates, Designanpassungen, Fehlerkorrektur)

§ 2 Weisungsgebundenheit

Der Auftragsverarbeiter ist bei der Auftragserfüllung zur Verarbeitung personenbezogener Daten nur im Rahmen der Weisungen des Auftraggebers berechtigt. Diese Weisungen bedürfen zumindest der Textform.

§ 3 Meldepflicht

Der Auftragsverarbeiter hat den Auftraggeber unverzüglich darauf hinzuweisen, wenn er der Ansicht ist, dass eine Weisung des Auftraggebers gegen die europäische Datenschutz-Grundverordnung (DS-GVO), das Bundesdatenschutzgesetz (BDSG) oder andere, insbesondere spezialgesetzliche Vorschriften über den Datenschutz verstößt.

Auftragsverarbeiter und Auftraggeber werden sich gegenseitig unverzüglich informieren, wenn Störungen, Unregelmäßigkeiten oder der Verdacht auf Datenschutzverletzungen auftreten. Insbesondere wird der Auftragsverarbeiter den Auftraggeber unverzüglich schriftlich unterrichten, wenn die Datenschutzbehörden (Landesbeauftragte für Datenschutz und Informationsfreiheit) Mängel im Betrieb des Auftragsverarbeiters feststellen, die auch die Datenverarbeitung für den Auftraggeber betreffen.

§ 4 Verpflichtung auf das Datengeheimnis

Der Auftragsverarbeiter ist verpflichtet, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten für den Auftraggeber die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 sowie Art. 29, 32 Abs. 4 DS-GVO zu gewährleisten. 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter 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.

§ 5 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 in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen, angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer [siehe Anlage 2] zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS- GVO.

(3) Bei der Unterbeauftragung sind dem Unterauftragnehmer die gleichen vertraglichen Regelungen aufzuerlegen, wie sie für den Auftragnehmer gelten. Dem Auftraggeber sind gegenüber dem Unterauftragnehmer die gleichen Weisungs-, Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und dem Art. 28 DSGVO einzuräumen, wie sie gegenüber dem Auftragnehmer gelten.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) 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.

(6) 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.

§ 6 Mitwirkungs- und Unterstützungspflichten

Der Auftragnehmer verpflichtet sich, im Rahmen des Art. 28 Abs. 3 lit. e und f DSGVO, die für das Verzeichnis von Verarbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutzfolgenabschätzung erforderlichen Informationen unverzüglich zur Verfügung zu stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutzfolgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen zu unterstützen.

Wenn dem Auftragsverarbeiter hinsichtlich der verarbeiteten Daten eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO bekannt wird („Datenschutzvorfall“), meldet er dies dem Verantwortlichen unverzüglich. Im Rahmen der Meldung gem. Art. 33 Abs. 2 DSGVO teilt der Auftragsverarbeiter dem Auftraggeber nach Möglichkeit den Zeitpunkt sowie Art und Ausmaß des Vorfalls, das betroffene IT-System, die betroffenen Personen, den Zeitpunkt der Entdeckung und alle evtl. bekannt gewordenen Folgen des Datenschutzvorfalls sowie die gegebenenfalls daraufhin ergriffenen Maßnahmen mit.

Für vorstehende Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder auf ein Fehlverhalten vom Auftragnehmer zurückzuführen sind und die gesetzlichen Unterstützungspflichten übersteigen, kann der Auftragnehmer eine angemessene Vergütung verlangen.

§ 7 Datenschutzbeauftragter

Als Datenschutzbeauftragter ist beim Auftragsverarbeiter benannt:

Herr Jürgen Recha
c/o interev GmbH Robert-Koch-Straße 55
30853 Langenhagen 0511 89798410
info@interev.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragsverarbeiters leicht zugänglich hinterlegt. Stellt der Datenschutzbeauftragte in diesem Zusammenhang Unregelmäßigkeiten fest, ist unverzüglich der Datenschutzbeauftragte des Auftraggebers oder ein sonstiger, für Datenschutzangelegenheiten benannter Mitarbeiter des Auftraggebers, zu informieren.

§ 8 Rechte der Betroffenen, Datenschutzfolgeabschätzung

Die Rechte, der durch die Datenverarbeitung beim Auftragsverarbeiter betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. Er ist verantwortlich für die Wahrung dieser Rechte. Der Auftragsverarbeiter hat den Auftraggeber bei der Wahrung dieser Rechte, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Sperrung und Löschung im Rahmen seiner Möglichkeiten zu unterstützen.

Im Falle des Vorliegens der Voraussetzungen des Art. 35 Abs. 1 DS-GVO wird der Auftragsverarbeiter die erforderliche Datenschutzfolgeabschätzung nach Maßgabe der Regelungen in Art. 35 Abs. 7 DS-GVO unter Einbeziehung seines Datenschutzbeauftragten vornehmen.

§ 9 Datentransport, Datenberichtigung sowie -sperre

Die Verantwortung für den Transport der Daten obliegt dem Auftraggeber. Der Auftragsverarbeiter weist dem Auftraggeber die von ihm üblicherweise eingerichteten Verlustsicherungsmaßnahmen nach. Zusätzliche Anforderungen des Auftraggebers und daraus resultierende Maßnahmen sind schriftlich zu vereinbaren.

Der Auftragsverarbeiter wird Weisungen des Auftraggebers im Zusammenhang mit der Berichtigung oder der Sperre von überlassenen Daten der Kunden des Auftraggebers unverzüglich umsetzen.

§ 10 Nachvertragliche Pflichten, Datenlöschung

Bei Beendigung des Auftragsverhältnisses verpflichtet sich der Auftragsverarbeiter, alle ihm aus Anlass und im Zusammenhang mit der Auftragsabwicklung übergebenen Unterlagen zurückzugewähren bzw. den Nachweis der ordnungsmäßigen Vernichtung zu führen. Dokumentationen, die dem Nachweis der ordnungsmäßigen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren, sofern die Verpflichtung zur Aufbewahrung nicht durch den Auftraggeber übernommen wird.

Der Auftragsverarbeiter hat im Regressfall dem Auftraggeber auch nach Vertragsende etwaig noch vorhandene Dokumentationen zur Führung des Entlastungsbeweises zu überlassen. Eine entsprechende Pflicht zur Datenlöschung trifft den Auftragsverarbeiter, sofern der Auftraggeber den Auftragsverarbeiter entsprechend schriftlich anweist.

Die Vertragsparteien sind verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus Stillschweigen über die im Zusammenhang mit dem Auftrag bekannt gewordenen Daten zu wahren.

§ 11 Technische und organisatorische Datenschutzmaßnahmen

Der Auftragsverarbeiter 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 durch ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, und Art. 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.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 12 Eigentum an Daten

Der Auftragsverarbeiter erkennt ausdrücklich an, dass sämtliche ihm von dem Auftraggeber überlassenen Daten ausschließlich im Eigentum des Auftraggebers verbleiben. Dem Auftragsverarbeiter ist es strikt untersagt, die Daten zu anderen als den vertraglich vereinbarten Zwecken zu nutzen oder diese an Dritte weiterzugeben.

§ 13 Kontrollmaßnahmen des Auftraggebers

Der Auftraggeber ist berechtigt und verpflichtet, die Einhaltung der datenschutzrechtlichen Bestimmungen sowie der Verpflichtungen aus diesem Vertrag im Unternehmen des Auftragsverarbeiters vor Beginn der Datenverarbeitung und sodann kontinuierlich zu überprüfen. Zu diesem Zwecke wird der Auftragsverarbeiter dem Auftraggeber bzw. von diesen beauftragten Mitarbeitern oder sonstigen Dritten Zugang zu den Geschäftsräumen, in denen Datenverarbeitungsprozesse für den Auftraggeber stattfinden bzw. stattfinden sollen, sowie Zugriff auf erforderliche Unterlagen und/oder Daten gewähren. Ferner wird der Auftragsverarbeiter sämtliche Mitwirkungspflichten erbringen, die für eine effiziente Kontrolle der Einhaltung der datenschutzrechtlichen Pflichten des Auftragsverarbeiters durch den Auftraggeber erforderlich sind.

Der Auftragsverarbeiter ist darüber unterrichtet, dass der Auftraggeber die Ergebnisse seiner Kontrollen dokumentiert. Der Auftraggeber wird dem Auftragsverarbeiter auf dessen schriftliches Verlangen Auskunft über das Ergebnis seiner Kontrollen erteilen.

§ 14 Gerichtsstand

Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist München.

§ 15 Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Änderung des Schriftformerfordernisses selbst.

Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen Bestimmung tritt die entsprechende gesetzliche Regelung. Gleiches gilt für den Fall, dass eine Regelung undurchführbar wird oder diese Vereinbarung eine Regelungslücke enthält.

Diese Vereinbarung zur Auftragsverarbeitung wird als integraler Bestandteil der Allgemeinen Geschäftsbedingungen der AirLST GmbH geschlossen. Sie gilt mit Abschluss des Hauptvertrages über die Nutzung der SaaS-Plattform sowie durch die Nutzung der Leistungen als vereinbart.
Eine gesonderte Unterzeichnung ist nicht erforderlich.

Anlage 1: Technische und organisatorische Maßnahmen

gem. Art. 32 Abs. 1 DS-GVO

1. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr spezifischen betroffenen Personen zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen:

Eine Pseudonymisierung erfolgt in Abhängigkeit

- der Daten
- des Auftrags
- der Umsetzungsmöglichkeit

☐ Die Vertragspartner haben bei dem vorliegenden Vertrag eine Pseudonymisierung vereinbart.

☐ Pseudonymisiert werden folgende Datenfelder:

2. Verschlüsselung

Eine Verschlüsselung erfolgt in Abhängigkeit

- der Daten
- des Auftrags
- der Umsetzungsmöglichkeit

Die Verschlüsselung erfolgt mit angemessener Verschlüsselungstechnik in Abhängigkeit zu den technischen, organisatorischen und finanziellen Mitteln.

☒ Eine Verschlüsselung der Datentransfers ist bei dem vorliegenden Vertrag vereinbart.

☒ Eine Verschlüsselung der Datenhaltung ist bei dem vorliegenden Vertrag vereinbart

3. Gewährleistung der Vertraulichkeit

Zutrittskontrolle:
Übersicht aller getroffen Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet oder genutzt werden, zu verwehren.

☒ Personenkontrolle beim Pförtner/Empfang, Chipkarten-/Transponder-Schließsystem

☒ Schließsystem mit Chipsperre

☒ Manuelles Schließsystem

☒ Schlüsselregelung (Schlüsselausgabe etc.)

☒ Videoüberwachung der Zugänge

☒ Protokollierung der Besucher

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

☒ Protokollierung der Vernichtung

☒ Sichere Aufbewahrung von Datenträgern

☒ physische Löschung von Datenträgern vor Wiederverwendung

☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)

☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz Gütesiegel)

☒ Verschlüsselung von Datenträgern

☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☒ Multi-Faktor-Authentifizierung auf allen kritischen Systemen

Belehrung der Mitarbeiter:

☒ Schulung durch Datenschutzbeauftragten

☒ Internes Information Security Awareness Training

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

☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☒ Logische Mandantentrennung (softwareseitig)

☒ Erstellung eines Berechtigungskonzepts

☒ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☒ Trennung von Produktiv- und Testsystem

☒ Festlegung von Datenbankrechten

4. Gewährleistung der Integrität

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.

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten

☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☒ Protokollierung der Änderung von Gästedaten

☒ Nachvollziehbarkeit von Änderung von Gästedaten durch individuelle Benutzernamen (nicht Benutzergruppen)

5. Gewährleistung der Verfügbarkeit

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- & Recoverykonzepts

☒ Testen von Datenwiederherstellung

☒ Erstellen eines Notfallplans

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☒ Serverräume nicht unter sanitären Anlagen

☒ In Hochwassergebieten: Serverräume über der Wassergrenze

☒ Kameraüberwachung in Serverräumen

☒ Datensicherung täglich

☒ Datensicherung monatlich

☒ Virenschutzkonzept

☒ Notfallplan

6. Gewährleistung der Belastbarkeit der Systeme

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

☒ Storage-Systeme nach Stand der Technik (bzgl. Toleranz und Resilienz ggü. Fehlern und Störungen)

☒ Backup Hard- und Software sind nach Stand der Technik ausgewählt und eingesetzt

☒ Notfallkonzepte

☒ Kapazitätsmanagement

☒ Patch-Management

☒ tägliche Datensicherung

☒ Vulnerability Scans und Penetration Tests

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

☒ Notfallplan

☒ Cloud Services

☒ Kontinuitätsmanagement - Konzept Spiegelungen in Externe Rechenzentren

☒ Redundante Datenspeicherung

☒ Redundante IT-Infrastruktur

☒ Regelmäßige Tests der Backups auf Datenwiederherstellung

☒ Backup- und Recoverykonzept

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Maßnahmen, die gewährleisten, dass eine systematische und regelmäßige Überprüfung sowie eine sach- und fachgerechte Bewertung und Behandlung der Wirksamkeit der technischen und organisatorischen Maßnahmen erfolgt.

☒ Datenschutzmanagement installiert regelmäßige Tests/Risikoanalyse inkl. Dokumentation (für den Bereich IT)

☒ Interne Audits, Externe Audits

☒ Zertifizierungen (z.B. TISAX) Change-Management für IT-Systeme

☒ Kontrolle durch externen Datenschutzbeauftragten

☒ monatliche Kontrolle

☒ Datenschutzmanagement installiert

Anlage 2: Unterauftragnehmer

Unterauftragnehmer	Anschrift	Leistung	Betroffene
Cloud-Dienstleister: Amazon Web Services EMEA SARL	Amazon Services Europe S.a.r.l, 5, Rue Plaetis, L-2338 Luxemburg	Hosting	Benutzer, Gäste des Auftraggebers
Kundendienst-Software: Zendesk International Ltd.	Neue Schönhauser Str. 3-5 10178 Berlin Deutschland	Support Chat	Benutzer des Auftraggebers
Software-Anbieter: Microsoft Deutschland GmbH	Konrad-Zuse-Str.1 85716 Unterschleißheim Germany	Cloud und Office Service	Ggf. Benutzer des Auftraggebers

Merkblatt

Auftragsverarbeitung (AV)

Bei einem Auftragsverarbeitungsvertrag geht es um die Sicherheit der personenbezogenen Daten die der Auftraggeber dem Auftragsverarbeiter (Dienstleister) übermittelt.
Ihr Kunde/Mitarbeiter hat einen Vertrag mit Ihrem Unternehmen und nicht mit einem Dienstleister Ihres Unternehmens. Daher ist ein Auftragsverarbeitungsvertrag (AV-Vertrag) zwischen Ihrem Unternehmen und Ihrem Dienstleister notwendig, damit zwischen ihnen geregelt ist, wie mit personenbezogenen Daten umzugehen ist. So können Sie auch Ihren Kunden und Mitarbeitern gegenüber gewährleisten, dass ihre Daten bei einem weiteren Dienstleister so behandelt werden, wie es mit Ihrem Unternehmen vereinbart wurde.

Beispiel:
Unternehmen A möchte allen seinen Kunden eine Weihnachtskarte schicken. Im Unternehmen selbst ist die Erstellung nicht möglich, also sucht es sich einen Dienstleister (Druckerei), der für ihn diese Aufgabe übernimmt. Unternehmen A muss dafür aber die Namen und Adressen an die Druckerei geben. Und hierbei handelt es sich um personenbezogene Daten. Unternehmen A fordert vom Dienstleister (der Druckerei) einen AV-Vertrag an. In diesem ist beschrieben, wie die Druckerei mit den Daten umgeht. Wofür werden die personenbezogenen Daten von Unternehmen A verwendet? Was passiert mit den Daten? Wer hat Einsicht in diese Daten? Wie lange werden diese aufbewahrt? Usw. Unternehmen A muss jetzt entscheiden, ob es die aufgeführten Bedingungen im AV-Vertrag akzeptieren kann, denn schließlich sind es seine Kundendaten.