

Auftragsverarbeitungsvertrag mit Anlage der technischen und organisatorischen Maßnahmen

gemäß Art. 28 DS-GVO

zwischen

| | |
|----------------|--|
| Unternehmen | |
| Straße HausNr. | |
| PLZ Ort | |

– nachfolgend „**Auftraggeber**“ genannt –

und

| | |
|----------------|--|
| Dienstleister | Auxilium Business Center GmbH & Co. KG |
| Straße HausNr. | Hollerallee 26 |
| PLZ Ort | 28209 Bremen |

– 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 | Mitarbeiterdaten des Verantwortlichen, auch Daten gem. Art. 9 DSGVO |
| 2 | jegliche Art von Daten, die der Verantwortliche den Auftragsverarbeiter aufzunehmen angewiesen hat |
| 3 | Bewerberdaten |
| 4 | Interessentendaten |
| 5 | Kundendaten |
| 6 | Lieferantendaten |
| 7 | Daten sonstiger Dritter |
| 8 | |
| 9 | |
| 10 | |

Folgende Dienstleistungen werden erbracht:

| | |
|---|--|
| 1 | Entgegennahme und Weiterleitung von eingehenden Anrufen |
| 2 | Verfassen von Rückrufnotizen und Weiterleitung via E-Mail, SMS und Telefax. |
| 3 | Überprüfung einzelner Datensätze, wie beispielsweise Kundenkonten, zum Zwecke der Hilfestellung und Überprüfung von Fehlern |
| 4 | Öffnen und Scannen nach Weisung des Verantwortlichen von Postsendungen für den Verantwortlichen und Weiterleitung an ihn via E-Mail |
| 5 | Empfangen von Kunden und Entgegennahme der Kontaktdaten und Unterlagen. Weiterleitung in Form von Notizen und Dateien via E-Mail, Briefsendung und Telefax |

Maßgabe ist der zwischen den Parteien geschlossene Vertrag vom

§ 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 Datenschutzbeauftragter

Als Datenschutzbeauftragter ist beim Auftragsverarbeiter benannt:

| | |
|----------------|--------------------------|
| Name | Jürgen Recha |
| Unternehmen | interev GmbH |
| Straße HausNr. | Robert-Koch-Straße 55 |
| PLZ Ort | 30853 Langenhagen |
| Telefon | 0511 897984 10 |
| E-Mail | Juergen.Recha@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.

§ 6 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.

§ 7 Datentransport, Datenberichtigung sowie -sperre

Die Verantwortung für den Transport der Daten obliegt dem Auftraggeber. Der Auftragsverarbeiter weist dem Auftraggeber die von ihm üblicherweise eingerichteten Verlostsicherungsmaßnahmen 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.

§ 8 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.

§ 9 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.

§ 10 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.

§ 11 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.

§ 13 Gerichtsstand

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

| | |
|-----------------|--------|
| Ort/Unternehmen | Bremen |
|-----------------|--------|

§ 14 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.

| | |
|--------|--|
| Ort: | |
| Datum: | |



Unterschrift
Auftraggeber



Unterschrift
Auftragsverarbeiter

Anlage: Technische und organisatorische Maßnahmen

gem. Art. 32 Abs. 1 DS-GVO

1. 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.

2. Gewährleistung der Vertraulichkeit

Zutrittskontrolle:

| | |
|--|-------------------|
| Zutrittskontrolle beim Auftragsverarbeiter | Token / Schlüssel |
|--|-------------------|

Zugriffskontrolle:

| | |
|--|-------------------|
| Zugriffskontrolle beim Auftragsverarbeiter | Benutzer-Passwort |
|--|-------------------|

Belehrung der Mitarbeiter:

| | |
|--|-------------------------|
| Art der Belehrung beim Auftragsverarbeiter | Datenschutzbeauftragter |
|--|-------------------------|

Trennungskontrolle:

| | |
|---|-------------------------|
| Trennungskontrolle beim Auftragsverarbeiter | Datenschutzbeauftragter |
|---|-------------------------|

3. Gewährleistung der Integrität

Eingabekontrolle:

| | |
|---|-------------------|
| Eingabekontrolle beim Auftragsverarbeiter | Benutzer-Passwort |
|---|-------------------|

4. Gewährleistung der Verfügbarkeit

Verfügbarkeitskontrolle:

| | |
|--|-------------------------|
| Verfügbarkeitskontrolle beim Auftragsverarbeiter | Datenschutzbeauftragter |
|--|-------------------------|

5. Gewährleistung der Belastbarkeit der Systeme

| | |
|--|------------------|
| Art der Gewährleistung beim Auftragsverarbeiter | Rade 5-Verfahren |
|--|------------------|

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

| | |
|--|------------------|
| Wiederherstellungs- verfahren beim Auftragsverarbeiter | Rade 5-Verfahren |
|--|------------------|

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

| | |
|--|-------------------------|
| Kontrolle der Wirksamkeit beim Auftragsverarbeiter | Datenschutzbeauftragter |
|--|-------------------------|

Merkblatt

Auftragsverarbeitung (AV)

Bei einem Auftragsverarbeitungsvertrag geht es um die Sicherheit der personenbezogenen Daten die der Auftraggeber dem Auftragsverarbeiter (Dienstleister) übermittelt. Der Kunde hat einen Vertrag mit dem Unternehmen und nicht mit den Dienstleistern des Unternehmens. Dementsprechend braucht es diesen Vertrag, damit Beide wissen, wie der Andere mit den Daten umgeht.

Beispiel:

Unternehmen A möchte an alle seine Kunden eine Weihnachtskarte schicken. Im Unternehmen ist das nicht möglich, also sucht er sich einen Dienstleister (Druckerei), welcher genau den Anforderungen gewachsen ist. Unternehmen A muss dafür aber die Namen und Adressen an die Druckerei schicken, dieses sind allerdings personenbezogene Daten. Unternehmen A fordert vom Dienstleister einen AV-Vertrag an. In diesem ist beschrieben, wie die Druckerei mit den Daten umgeht. Wofür werden meine Daten 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, schließlich sind es seine Kundendaten.

Muster für die Anlage der technischen und organisatorischen Maßnahmen.

2. Gewährleistung der Vertraulichkeit

Zutrittskontrolle beim Auftragsverarbeiter: Das Firmengelände verfügt über einen zentralen Eingang, zu den Geschäftszeiten ist der Empfang ständig besetzt. Die Büroräume sind verschlossen.

Zugriffskontrolle: Zugriff nur nach einem Berechtigungskonzept; Notebooks sind verschlüsselt.

Belehrung der Mitarbeiter: 1x im Monat eine E-Learning Schulung.

Trennungskontrolle: Es existiert eine logische Trennung von Servern.

3. Gewährleistung der Integrität

Eingabekontrolle: Protokollierung aller Eingaben

4. Gewährleistung der Verfügbarkeit

Verfügbarkeitskontrolle: Datensicherung täglich, Virenschutzkonzept, Notfallplan, Feuerlöscher

5. Gewährleistung der Belastbarkeit der Systeme

Gewährleistung: tägliche Datensicherung

6. Verfahren zur Wiederherstellung der Verfügbarkeit ...

Wiederherstellungsverfahren: Ein Notfallplan und Sicherheitskonzept sind vorhanden.

7. Verfahren regelmäßiger Überprüfung, ...

Kontrolle der Wirksamkeit: es wird 1x im Monat kontrolliert.