

# **Vereinbarung über die Auftragsverarbeitung gem. Art. 28 Datenschutz-Grundverordnung 2016/679/EU (DSGVO)**

zwischen

als Verantwortlicher i.S.d. Art. 4 Z. 7 DSGVO  
*- Im Folgenden Auftraggeber genannt -*

und

**Acquedus Business Services GmbH**  
Wiedner Hauptstraße 76/2/DG  
1040 Wien

als Auftragsverarbeiter i.S.d. Art. 4 Z. 8 DSGVO  
*- im Folgenden Auftragnehmer genannt -*

## Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in Abschnitt 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung

### 1. Gegenstand, Laufzeit

- (1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Unternehmensverwaltung und Unternehmenssteuerung. Dabei erhält der Auftragnehmer Zugriff auf personenbezogenen Daten und verarbeitet diese ausschließlich im Auftrag des Auftraggebers. Umfang und Zweck der Datenverarbeitung ergeben sich aus der Art der Leistungen und den zugehörigen Leistungsbeschreibung, welche im zwischen Auftraggeber und Auftragnehmer geschlossenen Vertrag zur Erbringung von Leistungen im Bereich der Unternehmensverwaltung und Unternehmenssteuerung vereinbart wurden
- (2) Diese Vereinbarung ist als Ergänzung zu dem geschlossenen Vertrag zur Erbringung von Dienstleistungen im Bereich Unternehmensverwaltung und Unternehmenssteuerung zu verstehen.
- (3) Die Laufzeit der Vereinbarung richtet sich nach der Laufzeit des geschlossenen Vertrags zur Erbringung von Dienstleistungen im Bereich Unternehmensverwaltung und Unternehmenssteuerung, sofern sich aus den nachfolgenden Bestimmungen nicht weitergehende Verpflichtungen oder Kündigungsrechte ergeben.

### 2. Art der verarbeiteten Daten, Betroffene Personen

- (1) Im Rahmen der Auftragsdurchführung erhält der Auftragnehmer Zugriff auf die in Anlage 1 spezifizierten personenbezogenen Daten.
- (2) Die Kategorien der betroffener Personen, die der Verarbeitung unterliegen, werden in Anlage 1 näher definiert.

### 3. Rechte, Pflichten, Weisungsbefugnisse des Auftraggebers

- (1) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
- (2) Weisungsempfänger beim Auftragnehmer sind:

Name	Kontakt	Funktion
Bernhard Frühlinger	bernhard.fruehlinger@acquedus.com +43 670 2042206	Geschäftsführer, CFO
Christian Löw	christian.loew@acquedus.com +49 172 1060653	Geschäftsführer, COO

- (3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.
- (4) Der Auftragnehmer darf Daten nur im Rahmen des geschlossenen Vertrags zur Erbringung von Dienstleistungen im Bereich Unternehmensverwaltung und Unternehmenssteuerung und gemäß den Weisungen des Auftraggebers verarbeiten.
- (5) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union

oder der Mitgliedstaaten. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

- (6) Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
- (7) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (8) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

#### **4. Pflichten des Auftragnehmers**

- (1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.
- (2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
- (3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 2 zu entnehmen).
- (4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
- (5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
- (6) Der Auftragnehmer führt für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO.
- (7) Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.
- (8) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht – grundsätzlich nach Terminvereinbarung - Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt.
- (9) Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

- (10) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.

## **5. Ort der Durchführung der Datenverarbeitung**

- (1) Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

## **6. Sub-Auftragsverarbeiter**

- (1) Der Auftragnehmer kann Sub-Auftragsverarbeiter hinzuziehen. Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann.
- (2) Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingetht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen.
- (3) Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

## **7. Außerordentliches Kündigungsrecht**

- (1) Der Auftraggeber kann den geschlossenen Vertrag zur Erbringung von Dienstleistungen im Bereich Unternehmensverwaltung und Unternehmenssteuerung jederzeit ohne Einhaltung einer Frist außerordentlich zu kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
- (2) Bei unerheblichen Verstößen setzt Acquedus dem Servicepartner eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung berechtigt.

## **8. Beendigung des geschlossenen Vertrags zur Erbringung von Dienstleistungen im Bereich Unternehmensverwaltung und Unternehmenssteuerung**

- (1) Der Auftragnehmer ist nach Beendigung des geschlossenen Vertrags zur Erbringung von Dienstleistungen im Bereich Unternehmensverwaltung und Unternehmenssteuerung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben.
- (2) Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

## 9. Schlussbestimmungen

- (1) Dieser Vertrag unterliegt deutschem Recht, nach welchem er auch auszulegen ist. Bei Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag oder über deren Gültigkeit ist ausschließlicher Gerichtsstand Darmstadt.
- (2) Änderungen oder Ergänzungen dieses Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform; auch eine Änderung dieses Formerfordernisses bedarf der Schriftform. Mündliche Nebenabreden bestehen nicht.
- (3) Sollte eine Bestimmung dieses Vertrags ganz oder teilweise unwirksam oder undurchsetzbar sein oder werden, werden die Wirksamkeit und Durchsetzbarkeit aller übrigen Bestimmungen dieses Vertrags davon nicht berührt. Die unwirksame oder undurchsetzbare Bestimmung ist als durch diejenige wirksame und durchsetzbare Bestimmung ersetzt anzusehen, die dem von den Parteien mit der unwirksamen oder undurchsetzbaren Bestimmung verfolgten wirtschaftlichen Zweck am nächsten kommt.

### Anlagen

Anlage 1 – Schutzbedürftige Daten und Betroffene

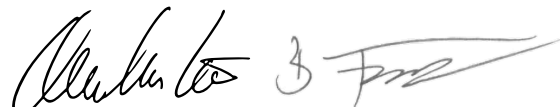
Anlage 2 – Technisch organisatorische Maßnahmen (TOM)

Wien,

Ort, Datum

Christian Löw, Bernhard Frühlinger

Name (in Druckbuchstaben)



Unterschrift

Ort, Datum

Name (in Druckbuchstaben)

Unterschrift

**Acquedus Business Services GmbH**

## Anlage 1 – Schutzbedürftige Daten und Betroffene

Beschreibung der besonders schutzbedürftigen Daten und Datenkategorien und Betroffenen.

### Definitionen

Kunde	Das Unternehmen, das die IT-Plattform „Adam“ nutzt
Nutzer	MitarbeiterIn des Kunden, welche die IT-Plattform „Adam“ verwendet
Kundes-Kunde	Kunden des Kunden
„Adam“-IT-Plattform	IT-Plattform der Acquedus Business Services GmbH, über welche Daten ausgetauscht und verarbeitet werden

<b>Datenkategorie</b>	Kundendaten für Controlling & Reporting	
<b>Betroffene</b>	Unternehmen	
<b>Beschreibung</b>	Mit der Registrierung zu und Nutzung der „Adam“-IT-Plattform und des Moduls „Controlling & Reporting“ werden folgende Daten verarbeitet und bis zur Löschung gespeichert.	
<b>Zweck der Verarbeitung</b>	<ul style="list-style-type: none"> <li>• Nutzung der „Adam“-IT-Plattform</li> <li>• Rechnungsstellung</li> <li>• Erstellung der Berichte und Auswertungen im Rahmen des Moduls „Controlling &amp; Reporting“</li> </ul>	
<b>Erhobene Daten</b>	<b>Beschreibung</b>	<b>Speicherdauer</b>
Kundenstammdaten	Die Stammdaten des Kunden können personenbezogenen Daten beinhalten	bis auf Widerruf
Vorname / Nachname	Ansprechpartner können für die Nutzung der Anwendung und für die Rechnungsstellung gespeichert sein	bis auf Widerruf
E-Mailadresse	Zum Login und zum Versand der Berichte und Notifications wird eine E-Mail-Adresse angegeben. Es können nutzerbasierte Konten angelegt werden	bis auf Widerruf
Buchhalterische Konten der Gewinn & Verlustrechnung bzw. Einnahmen-Ausgabenrechnung	Im Rahmen der Erstellung der Berichte werden die buchhalterischen Konten der Gewinn- und Verlustrechnung bzw. der Einnahmen-Ausgabenrechnung übernommen, aggregiert und in den Berichten visualisiert.	bis auf Widerruf
Buchhalterische Konten der Bilanz	Im Rahmen der Erstellung der Berichte werden die buchhalterischen Konten der Bilanz übernommen, aggregiert und in den Berichten visualisiert.	bis auf Widerruf

<b>Datenkategorie</b>	Daten von Kundes-Kunden für Controlling & Reporting	
<b>Betroffene</b>	Unternehmen, Privatpersonen, Berufsheimnisträger	
<b>Beschreibung</b>	Nach Durchführung der Buchhaltung werden Daten für die Erstellung der Berichte und Auswertungen im Rahmen des Moduls „Controlling & Reporting“ verarbeitet. Dabei werden Daten der Kundes-Kunden verarbeitet.	
<b>Zweck der Verarbeitung</b>	Erstellung der Berichte und Auswertungen im Rahmen des Moduls „Controlling & Reporting“	
<b>Erhobene Daten</b>	<b>Beschreibung</b>	<b>Speicherdauer</b>
Stammdaten der Kundes-Kunden	Die Stammdaten der Kundes-Kunden können personenbezogenen Daten beinhalten	bis auf Widerruf durch den Kunden
Debitorische Buchhaltungsdaten	Im Rahmen der Erstellung der Berichte werden debitorische (buchhalterische) Konten übernommen, aggregiert und in den Berichten visualisiert.	bis auf Widerruf durch den Kunden

<b>Datenkategorie</b>	Daten von Lieferanten des Kunden für Controlling & Reporting	
<b>Betroffene</b>	Unternehmen, Privatpersonen, Berufsheimnisträger	
<b>Beschreibung</b>	Nach Durchführung der Buchhaltung werden Daten für die Erstellung der Berichte und Auswertungen im Rahmen des Moduls „Controlling & Reporting“ verarbeitet. Dabei werden Daten der Lieferanten des Kunden verarbeitet.	
<b>Zweck der Verarbeitung</b>	Erstellung der Berichte und Auswertungen	
<b>Erhobene Daten</b>	<b>Beschreibung</b>	<b>Speicherdauer</b>
Stammdaten der Lieferanten des Kunden	Die Stammdaten der Lieferanten des Kunden können personenbezogenen Daten beinhalten.	bis auf Widerruf durch den Kunden
Kreditorische Buchhaltungsdaten	Im Rahmen der Erstellung der Berichte werden kreditorische (buchhalterische) Konten übernommen, aggregiert und in den Berichten visualisiert.	bis auf Widerruf durch den Kunden

## Anlage 2 – Technisch-organisatorische Massnahmen

### A. VERTRAULICHKEIT

**Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

<input checked="" type="checkbox"/> Schlüssel	<input checked="" type="checkbox"/> Magnet- oder Chipkarten
<input checked="" type="checkbox"/> Elektrische Türöffner	<input checked="" type="checkbox"/> Portier
<input checked="" type="checkbox"/> Sicherheitspersonal	<input checked="" type="checkbox"/> Alarmanlagen
<input checked="" type="checkbox"/> Videoanlage	<input checked="" type="checkbox"/> Einbruchshemmende Fenster und/oder Sicherheitstüren
<input checked="" type="checkbox"/> Anmeldung beim Empfang mit Personenkontrolle	<input checked="" type="checkbox"/> Begleitung von Besuchern im Unternehmensgebäude
<input checked="" type="checkbox"/> Tragen von Firmen-/Besucherausweisen	<input type="checkbox"/> Sonstiges:

**Zugangskontrolle:** Schutz vor unbefugter Systembenutzung durch:

<input checked="" type="checkbox"/> Kennwörter (einschließlich entsprechender Policy)	<input type="checkbox"/> Verschlüsselung von Datenträgern
<input type="checkbox"/> Automatische Sperrmechanismen	<input type="checkbox"/> Sonstiges:
<input type="checkbox"/> Zwei-Faktor-Authentifizierung	

**Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

<input checked="" type="checkbox"/> Standard-Berechtigungsprofile auf „need to know-Basis“	<input type="checkbox"/> Standardprozess für Berechtigungsvergabe
<input checked="" type="checkbox"/> Protokollierung von Zugriffen	<input type="checkbox"/> Sichere Aufbewahrung von Speichermedien
<input checked="" type="checkbox"/> Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten	<input type="checkbox"/> Datenschutzgerechte Wiederverwendung von Datenträgern
<input type="checkbox"/> Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	<input type="checkbox"/> Clear-Desk/Clear-Screen Policy
<input type="checkbox"/> Sonstiges:	

**Pseudonymisierung:** Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

<input checked="" type="checkbox"/> Ja	<input type="checkbox"/> Nein
--	-------------------------------

**Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

<input type="checkbox"/> Ja	<input checked="" type="checkbox"/> Nein
-----------------------------	--

### B. DATENINTEGRITÄT<sup>1</sup>

**Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

<input type="checkbox"/> Verschlüsselung von Datenträgern	<input type="checkbox"/> Verschlüsselung von Dateien
<input type="checkbox"/> Virtual Private Networks (VPN)	<input type="checkbox"/> Elektronische Signatur
<input checked="" type="checkbox"/> Sonstiges: SSL-Verschlüsselung der Kommunikationswege	



**Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

<input checked="" type="checkbox"/> Protokollierung	<input type="checkbox"/> Dokumentenmanagement
<input type="checkbox"/> Sonstiges:	

### C. VERFÜGBARKEIT UND BELASTBARKEIT

**Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

<input checked="" type="checkbox"/> Backup-Strategie (online/offline; on-site/off-site)	<input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
<input checked="" type="checkbox"/> Virenschutz	<input checked="" type="checkbox"/> Firewall
<input checked="" type="checkbox"/> Meldewege und Notfallpläne	<input checked="" type="checkbox"/> Security Checks auf Infrastruktur- und Applikationsebene
<input checked="" type="checkbox"/> Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum	<input type="checkbox"/> Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
<input type="checkbox"/> Sonstiges:	

**Rasche Wiederherstellbarkeit:**

<input checked="" type="checkbox"/> Ja	<input type="checkbox"/> Nein
--	-------------------------------

### D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

**Datenschutz-Management**, einschließlich regelmäßiger Mitarbeiter-Schulungen:

<input type="checkbox"/> Ja	<input checked="" type="checkbox"/> Nein
-----------------------------	--

**Incident-Response-Management:**

<input checked="" type="checkbox"/> Ja	<input type="checkbox"/> Nein
--	-------------------------------

**Datenschutzfreundliche Voreinstellungen:**

<input checked="" type="checkbox"/> Ja	<input type="checkbox"/> Nein
--	-------------------------------

**Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch:

<input checked="" type="checkbox"/> Eindeutige Vertragsgestaltung	<input type="checkbox"/> Formalisiertes Auftragsmanagement
<input type="checkbox"/> Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)	<input type="checkbox"/> Vorabüberzeugungspflicht
<input checked="" type="checkbox"/> Nachkontrollen	<input type="checkbox"/> Sonstiges: