GEBÄUDEMANAGEMENT
RETIS

AV

Vereinbarung für Auftragsverarbeitung

RETIS Gebäudemanagement GmbH

Version	AV 1.0
Datum	04.04.2023
Klassifizierung	Nur für internen Gebrauch
Dateiname	ADVV RETIS.pdf

Inhaltsverzeichnis

Vertraulichkeitserklärung

Der Inhalt sämtlicher Dokumente, welche RETIS übergibt ist Eigentum der RETIS Gebäudemanagement GmbH. Es gehen keine Rechte aus besagtem Material an den Kunden über. Diese Dokumente dürfen nicht veröffentlicht, dupliziert oder anderweitig zugänglich gemacht werden, als Ganzes oder in Teilen, ohne vorherige schriftliche Zustimmung von RETIS.

Vereinbarung für Auftragsverarbeitung (AV)

Der Verantwortliche (Auftraggeber)

und

Der Auftragsverarbeiter (Auftragsnehmer)
RETIS Gebäudemanagement GmbH
Rosenweg 3
3375 Inkwil

schliessen die folgende Vereinbarung ab.

1 Einleitung

Mit dieser Vereinbarung wird der Art. 28 der EU-Datenschutzgrundverordnung (DSGVO) über die datenschutzrechtlichen Verpflichtungen der Vertragsparteien bei der Erbringung von IT-Dienstleistungen entsprechend konkretisiert.

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeitende des Auftragsverarbeiters oder durch ihn beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können. Die Laufzeit der Gültigkeit richtet sich an der Dauer der Auftragsbestätigung.

2 Umfang der Auftragsverarbeitung

a. Geltender Umfang der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter über die Erbringung informationstechnischer Dienstleistung, die mit der Nutzung der webbasierten Software von RETIS. Bei dieser Erbringung handelt es sich um weisungsgebunde Verarbeitung personenbezogener Daten seitens des Auftragsverarbeiter für den Verantwortlichen.
b. Gegenstand ist dabei insbesondere die Erbringung folgender Leistungen seitens Auftragsverarbeiter:
    - Hosting der webbasierten Tools gemäss Rahmenvertrag und Gewährleistung der Lauffähigkeit
    - Bereitstellung der Serverinfrastruktur für die webbasierten Tools
    - Sicherstellen der Backup und Datensicherheit zwischen Server und der Weboberfläche im Auftrag des Verantwortlichen
c. Mitarbeiter des Auftragsverarbeiters haben im Rahmen der Dienstleistungserbringung Zugang zu allen in den Tools abgespeicherten personenbezogenen Daten.
d. Beschränkt auf den Zweck der ordnungsgemässen Erbringung der oben genannten IT-Dienstleistungen darf der Auftragsverarbeiter personenbezogene Daten für den Verantwortlichen erheben, speichern, verändern, übermitteln und nutzen.
e. Betroffen von der Datenverwendung können sein (abhängig vom Aufgabengebiet des Verantwortlichen):
    - Mitarbeitende
    - Kunden
    - Lieferanten
    - Bewohner
    - Sonstige:

Diese Vereinbarung der Auftragsverarbeitung (AV) gilt ausschliesslich für die Verarbeitung der Daten durch den Auftragsverarbeiter und dessen beigezogenen Subunternehmern. Beauftragt der Kunde den Auftragsverarbeiter mit der Verarbeitung von Daten auf Infrastruktur

oder mit Software von Dritten, so ist der Kunde für die Einhaltung der Datenschutzbestimmungen durch diesen Dritten verantwortlich.

3 Verantwortlichkeit und Weisung

Der Verantwortliche ist nach Art. 4 Abs. 7 DSGVO alleine verantwortlich für die Beurteilung der rechtlichen Zulässigkeit, für die im Rahmen der Auftragsbestätigung durchgeführten Verarbeitung und Nutzung personenbezogener Daten durch den Auftragsverarbeiter, im Blick auf die Regelungen in der DSGVO, dem Bundesgesetz über den Datenschutz der Schweiz (DSG) und anderer Vorschriften über den Datenschutz.
Der Verantwortliche kann während der Laufzeit und nach Beendigung der Auftragsbestätigung die Löschung, Sperrung und Herausgabe von personenbezogenen Daten verlangen.
Dem Verantwortlichen obliegt allein die Prüfung der rechtlichen Zulässigkeit bestimmter von ihm durchgeführter oder geplanter Verarbeitungstätigkeiten.
Der Auftragsverarbeiter verarbeitet die Daten ausschliesslich für die Zwecke der Auftragsbestätigung und gemäss den dokumentierten Weisungen des Verantwortlichen. Weisungen (Bpsw. Zugangsdaten, Userlisten etc.) müssen stets schriftlich oder in elektronischer Form erfolgen. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

3.1 Pflichten des Verantwortlichen (Auftraggebers)

Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und regelmässig von den technischen und organisatorischen Massnahmen des Auftragsverarbeiters und dokumentiert das Ergebnis.

- Der Verantwortliche beurteilt die Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen. Der Verantwortliche gewährleistet, dass die Verarbeitung der Daten durch den Auftragsverarbeiter gemäss dieser AV und den Weisungen keine anwendbaren gesetzliche Bestimmungen verletzt.
- Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei Prüfung der Auftragsverarbeitung feststellt.
- Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen des Auftragsverarbeiters vertraulich zu behandeln.
- Der Verantwortliche ist verpflichtet, seine Weisungen an den Auftragsverarbeiter zu dokumentieren.

3.2 Pflichten des Auftragsverarbeiter (Auftragnehmers)

- Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die dieser benötigt, um die Einhaltung der Vorschriften zur Auftragsverarbeitung gemäss Art. 28 DSGVO dokumentieren und nachweisen zu können. Aufgetretene Mängel sind unverzüglich und unter Erbringung eines schriftlichen Nachweises vom Auftragsverarbeiter zu beseitigen.
- Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über datenschutzrelevante Betriebsstörungen, bei Indizien für mögliche oder feststehende Datenschutzverletzungen, bei sonstigen Unregelmässigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten sowie bei Verstössen gegen die Bestimmung dieser Vereinbarung.
- Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung der Daten befugten Personen (z.B. Mitarbeiter, Subunternehmer, etc.) sich vertraglich zur Wahrung der Vertraulichkeit und Sicherheit verpflichtet haben oder einer geeigneten gesetzlichen Vertraulichkeits- und Sicherheitsverpflichtung unterliegen.

- Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragsverarbeiter hat angemessene technische und organisatorische Massnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen und die den Anforderungen der DSGVO genügen.
- Der Auftragsverarbeiter kann die Massnahmen im Laufe des Auftragsverhältnisses den technischen und organisatorischen Weiterentwicklungen anpassen – diese dürfen die vereinbarten Standards jedoch nicht unterschreiten.

3.3 Schutz personenbezogener Daten vor Missbrauch

Der Auftragsverarbeiter legt besonderen Wert auf die vertrauliche Behandlung persönlicher Daten und die Einhaltung der geltenden Datenschutzbestimmungen. Personenbezogene Informationen die in den webbasierten Tools von RETIS Gebäudemanagement GmbH gespeichert werden, dürfen nur im Rahmen der hier aufgeführten Richtlinien verarbeitet werden.
Die Verbindungen zwischen der Weboberfläche und dem Server, sowie auf dem Testsystem und dem Server erfolgen ausschliesslich über verschlüsselte SSL-Verbindungen.

- Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen bei der Wahrung Betroffenenrechten (Auskunft, Berichtigung, Einschränkung und Löschung der Daten) zu unterstützen.
- Soweit die betroffene Person gegenüber der verantwortlichen Stelle ein Recht geltend machen kann, stellt der Auftragsverarbeiter sicher, dass der Verantwortliche die verarbeiteten personenbezogenen Daten in einer lesbaren Form erhalten kann.
- Der Auftragsverarbeiter darf personenbezogene Daten nur nach dokumentierter Weisung des Verantwortlichen herausgeben, berichtigen, löschen oder deren Verarbeitung einschränken. Auskünfte und Ersuche betroffener Personen sind erst nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen zu erteilen.

4 Einhaltung der Pflichten und Nachweis der Einhaltung

Der Auftragsverarbeiter unterstützt den Verantwortlichen angemessen bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Für die Umsetzung der Betroffenenrechte ist grundsätzlich der Verantwortliche zuständig.
Der Verantwortliche kann sich im Falle eines begründeten Zweifels an den vorgelegten Unterlagen oder eines datenschutzrechtlich relevanten Vorfalls, nach rechtzeitiger Anmeldung unter schriftlicher Angabe der Gründe zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs, persönlich überzeugen. Die mit einem solchen Audit verbundenen Kosten trägt der Verantwortliche.

- Der Auftragsverarbeiter leitet allfällige Anfragen von betroffenen Personen, soweit die Anfrage dem Verantwortlichen zugeordnet werden kann, an den Verantwortlichen weiter.
- Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des Verantwortlichen bekannt werden.
- Der Auftragsverarbeiter weist dem Verantwortlichen die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

Sollten im Einzelfall Audits durch den Verantwortlichen oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Den berechtigten Geheimhaltungsinteressen sowie gesetzlichen sowie vertrag-

lichen Geheimhaltungspflichten ist bei der Inspektion angemessen Rechnung zu tragen. Die prüfenden Personen müssen vor der Inspektion eine Verschwiegenheitserklärung hinsichtlich der Daten des Auftragsverarbeiters sowie anderer Kunden und der eingerichteten technischen und organisatorischen Massnahmen unterzeichnen.

Alle Kosten des Auftragsverarbeiters (inkl. jene für die/den beizustellende/-n Mitarbeiter/-in) sind durch den Verantwortlichen zu tragen.

4.1 Übermittlung von Personendaten ins Ausland

Alle Datenverarbeitungstätigkeiten werden ausschliesslich innerhalb der Schweiz und Deutschland durchgeführt. Jede Verlagerung in ein anderes Land bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die Voraussetzungen anwendbaren Datenschutzrechts erfüllt sind.

4.2 Beschreibung der Dienstleistungen

Die Dienstleistung umfasst das Hosting, die Bereitstellung und den Support von onlinebasierten Tools im Bereich von Facility Management, Mahlzeitenverwaltung und der Erfassung, Verarbeitung und Nutzung von personenbezogenen Daten im Sinne des Art. 4 Nr. 1, 2 DSGVO.

4.3 Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die Benutzung eines Datenverarbeitungssystems die Berechtigten ausschliesslich auf die ihnen berechtigten Daten zugreifen können. Insbesondere, dass personenbezogene Daten bei der Verarbeitung, Nutzung und der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Folgende Massnahmen verhindern einen unbefugten Zugriff:

- Gemeinsame Festlegung der Zugriffsberechtigungen
- Regelung der Wiederherstellung von Daten aus Backups
- Regelmässige Überprüfung der Berechtigungen durch den Verantwortlichen
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken mittels Berechtigungen
- Einschränkungsmöglichkeiten des Verantwortlichen auf Zugriff von personenbezogenen Daten in smartReporting
- Möglichkeit der Auswertung von Protokollen (Logfiles, Auswertung kostenpflichtig)
- Verwenden von sicheren Passwörtern

Die Trennungskontrolle soll gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Grund dafür ist u.a. das Zuordnen der Daten zu bestimmten Tools, aber auch Bereichen, Abteilungen, Personen etc. Dabei kann das Ziel durch unterschiedliche Weise erreicht werden. Beispielsweise durch ein entsprechendes Berechtigungs- und Zugriffskonzept innerhalb der webbasierten Anwendungen. Dies kann mit folgenden Massnahmen sichergestellt werden:

- Trennung von Kunden (Mandantenfähigkeit des Systems)
- Berechtigungskonzept, in Absprache mit dem Verantwortlichen
- Trennung von Test- und Produktivsystem

4.4 Integrität

Die Weitergabe- und Eingabekontrolle nach Art. 32 Abs. 1 lit. B DSGVO soll gewährleisten, dass die Übertragung von personenbezogenen Daten und auch die Eingabe nicht unbefugt bearbeitet resp. nachvollzogen werden kann. Zum Schutz der Daten werden nachfolgende Massnahmen vorgenommen:

- Datenaustausch erfolgt über https-Verbindung (Verschlüsselung mittels Zertifikat)
- Festlegung von Benutzerberechtigungen
- Differenzierte Benutzerberechtigungen die sich auf verschiedene Rechte beschränken, wie Lesen, Ändern, Löschen, Teilzugriff etc.
- Protokollierung von Eingaben und Löschungen
- Verpflichtungen auf das Datengeheimnis
- Log-Daten bei persönlichen Accounts

5 Übersicht von Verarbeitungstätigkeiten

Nachfolgend die Übersicht der Auftragsverarbeiter und Sub-Auftragsverarbeiter gemäss Artikel 30 Abs. 2 DSGVO.

5.1 Auftragsverarbeiter

RETIS Gebäudemanagement GmbH
Rosenweg 3
3375 Inkwil
info@retis-gmbh.ch
www.retis-gmbh.ch

5.2 Sub-Auftragsverarbeiter

Der Auftragsverarbeiter ist befugt folgende Unternehmen als Sub-Auftragnehmer zu beauftragen:

Programmierung und Bereitstellung der Software:
Lum GmbH
Universitätstrasse 52
DE-35037 Marburg

Beabsichtigte Änderungen der Sub-Auftragsverarbeiter sind dem Verantwortlichen rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragsverarbeiter 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 eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

5.3 Sub-Auftragsverarbeiter ohne Zugriff auf personenrelevanter Daten

Bereitstellung von Serverleistungen:
Hetzner Online GmbH

Industriestrasse 25
DE-91710 Gunzenhausen

Bereitstellung von Domainleistungen und Zertifikate:
Hetzner Online GmbH
Industriestrasse 25
DE-91710 Gunzenhausen

Swizzonic AG
Postfach 2172
8021 Zürich

5.4 Zugangssteuerung, Zutrittskontrolle und physische Sicherheit der Server

- Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen per Chipkarten und elektrischem Türöffner. In den Rechenzentren zusätzlicher Schutz vor unbefugtem Zutritt über einen Portier, Sicherheitspersonal, Alarmanlagen und Videoanlagen.
- Zugangskontrolle: Schutz vor unbefugter Systembenutzung über sichere Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung und Verschlüsselung von Datenträgern.
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems über Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.
- Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt und gesondert aufbewahrt.
- Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung werden Daten in den Kategorien vertraulich/intern/öffentlich klassifiziert.

6 Sonstige Bestimmungen

6.1 Löschung und Herausgabe

Der Auftragsverarbeiter wird personenbezogene Daten nur solange aufbewahren, wie vom Verantwortlichen angewiesen. Sofern keine konkrete Weisung vorliegt, werden die personenbezogenen Daten vor der Vernichtung nur solange aufbewahrt, wie es für die jeweilige Auftragsverarbeitung notwendig ist.
Auf Verlangen des Verantwortlichen sowie nach Beendigung dieser Vereinbarung wird der Auftragsverarbeiter sämtliche personenbezogene Daten unter Einhaltung einschlägiger datenschutzrechtlicher Bestimmungen löschen.
Dokumentationen, die dem Nachweis der Auftrags- und ordnungsgemässen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend den jeweiligen gesetzlichen oder vertraglich vereinbarten Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Es kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.
Der Auftragsverarbeiter weist dem Verantwortlichen die Löschung auf Verlangen schriftlich nach.

6.2 Kontrollverfahren

Folgende Massnahmen sind zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmassnahmen implementiert:

- Prozesse zur Meldung neuer/veränderter Verfahren werden dokumentiert
- Es werden datenschutzfreundliche Voreinstellungen gewählt, in der Software wird darauf hingewiesen
- Getroffene Sicherheitsmassnahmen werden einer regelmässigen internen Kontrolle unterzogen

6.3 Auftragskontrolle

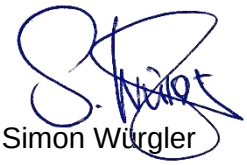
Die Auftragskontrolle soll gewährleisten, dass Daten die im Auftrag durch den Sub-Auftragsverarbeiter verarbeitet werden, nur gemäss der Weisung des Auftragsverarbeiters verarbeitet werden.
In Bezug auf technische und organisatorische Massnahmen ist folgendes zur Sicherstellung implementiert:

- Zentrale Erfassung vorhandener Verantwortliche (einheitliches Vertragsmanagement)
- Überprüfung des Datensicherheitskonzepts bei Sub-Auftragsverarbeiter
- Überprüfung vorhandener IT-Sicherheitszertifikate des Auftragsverarbeiters

RETIS Gebäudemanagement GmbH
Geschäftsführer

Markus Wisler

Software Engineering
Stv. Geschäftsführer



Simon Würgler