Vertrag über die Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen dem **Kunden des Atendu-Cloud-Dienstes** – Verantwortlicher im Sinne der DSGVO, im Folgenden „Auftraggeber" – und

Rico Kirsten (Atendu), Wilhelm-Raabe-Str. 22, 01157 Dresden, Deutschland – Auftragsverarbeiter im Sinne der DSGVO, im Folgenden „Auftragnehmer".

Präambel

Der Auftraggeber nutzt den Dienst „Atendu Cloud" (Hauptvertrag gemäß AGB), mit dem wartende Endkunden des Auftraggebers über den Aufruf ihrer Nummer benachrichtigt werden (Warteseite und optionale Push-Benachrichtigung). Dabei verarbeitet der Auftragnehmer personenbezogene Daten der Endkunden des Auftraggebers in dessen Auftrag. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien. Er wird elektronisch geschlossen und ist Bestandteil der Buchung des Cloud-Abos (§ 10).

§ 1 Gegenstand und Dauer

1. Gegenstand des Auftrags ist der Betrieb der Kunden-Warteseite und die Zustellung von Aufruf-Benachrichtigungen an Endkunden des Auftraggebers.
2. Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags (Cloud-Abo). Die Kündigung des Hauptvertrags beendet zugleich diesen Vertrag.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, Kreis der Betroffenen

1. **Art und Zweck:** Speicherung von Benachrichtigungs-Abonnements; Anzeige aufgerufener Nummern auf der Warteseite; Versand von Push-Benachrichtigungen bei Aufruf; technische Protokollierung zum sicheren Betrieb.
2. **Art der Daten:**

- pseudonyme Push-Abonnements (Endpunkt-URL des Browser-Push-Dienstes, Verschlüsselungsschlüssel, gewählte Nummer, Spracheinstellung)
- aufgerufene Nummern mit Zeitstempel
- IP-Adressen und technische Metadaten in Server-Logs

Es werden keine Namen, Kontakt- oder Profildaten der Endkunden verarbeitet.
3. **Kreis der Betroffenen:** Endkunden des Auftraggebers, die die Warteseite aufrufen oder Benachrichtigungen abonnieren.

§ 3 Ort der Verarbeitung, Drittlandübermittlung

1. Die Verarbeitung findet auf Servern in Deutschland statt (Unterauftragsverarbeiter siehe § 6).
2. Ausnahme: Die Zustellung von Push-Benachrichtigungen erfolgt systembedingt über den Push-Dienst des jeweiligen Endgeräts bzw. Browsers (z. B. Google Firebase Cloud Messaging, Apple Push-Dienst, Mozilla Push Service); dabei kann eine Übermittlung in die USA stattfinden. Google Firebase Cloud Messaging ist unter dem EU-US Data Privacy Framework zertifiziert (Art. 45 DSGVO); im Übrigen stützt sich die Übermittlung auf Art. 49 Abs. 1 lit. b DSGVO, da sie für die Zustellung der von der betroffenen Person angeforderten Benachrichtigung erforderlich ist und nur anlassbezogen erfolgt. Der Nachrichteninhalt ist nach dem Web-Push-Standard (RFC 8291) Ende-zu-Ende-verschlüsselt und für den Push-Dienst nicht lesbar; Klardaten (Name, E-Mail-Adresse) werden nicht übermittelt. Der Push-Dienst wird durch das Endgerät des Betroffenen bestimmt und ist vom Auftragnehmer nicht wähl- oder ersetzbar; die Push-Dienste handeln insoweit als eigenständige Verantwortliche und sind keine Unterauftragsverarbeiter des Auftragnehmers.
3. Darüber hinaus übermittelt der Auftragnehmer im Auftrag verarbeitete Daten nur dann in ein Drittland, wenn dies auf dokumentierte Weisung des Auftraggebers geschieht oder er rechtlich dazu verpflichtet ist; in beiden Fällen werden die Anforderungen des Kapitels V DSGVO eingehalten.

§ 4 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Vertrags und nach dokumentierten Weisungen des Auftraggebers, sofern er nicht durch Unions- oder Mitgliedstaatenrecht zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt er dem Auftraggeber diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

2. Der Auftragnehmer verwendet die Daten für keine anderen, insbesondere keine eigenen Zwecke.
3. Personen, die Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet.
4. Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Anlage 1 (Art. 32 DSGVO) und passt sie dem Stand der Technik an, sofern das vereinbarte Schutzniveau nicht unterschritten wird.
5. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Betroffenenrechte (Art. 12–22 DSGVO) sowie der Pflichten aus Art. 32–36 DSGVO. An den Auftragnehmer gerichtete Anfragen Betroffener, die erkennbar den Auftraggeber betreffen, leitet er unverzüglich weiter.
6. Der Auftragnehmer benennt keinen Datenschutzbeauftragten (nicht erforderlich nach § 38 BDSG). Kontakt für alle datenschutzrechtlichen Belange: info@atendu.eu.

§ 5 Meldung von Verletzungen

Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes der im Auftrag verarbeiteten personenbezogenen Daten unverzüglich nach Bekanntwerden (Art. 33 Abs. 2 DSGVO) an die im Kundenkonto hinterlegte E-Mail-Adresse und unterstützt den Auftraggeber bei dessen Melde- und Benachrichtigungspflichten. Die Meldung enthält – soweit zum Meldezeitpunkt verfügbar – mindestens: eine Beschreibung der Art der Verletzung, die Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Abhilfemaßnahmen. Noch nicht verfügbare Informationen liefert der Auftragnehmer ohne unangemessene Verzögerung schrittweise nach.

§ 6 Unterauftragsverhältnisse

1. Der Auftraggeber erteilt die allgemeine Genehmigung zur Einschaltung der folgenden Unterauftragsverarbeiter:

Unterauftragsverarbeiter	**Sitz**	**Leistung**
Hetzner Online GmbH	Deutschland	Server-Infrastruktur (Hosting) und Datensicherung (Backup-Inhalt clientseitig verschlüsselt)

Hinweis: mailbox.org (E-Mail-Versand) und Lexware/Haufe Service Center (Rechnung) verarbeiten ausschließlich Konto-/Abrechnungsdaten des Auftraggebers, für die der Auftragnehmer selbst Verantwortlicher ist – keine Endkundendaten dieses

Auftragsverhältnisses. Sie sind daher hier keine Unterauftragsverarbeiter.

2. Über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung) informiert der Auftragnehmer den Auftraggeber mindestens vier Wochen vor Wirksamwerden in Textform; der Auftraggeber kann binnen zwei Wochen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund widersprechen. Bleibt eine einvernehmliche Lösung aus, können beide Parteien den Hauptvertrag zum Zeitpunkt der Änderung kündigen.
3. Die Browser-Push-Dienste (§ 3 Abs. 2) sind keine vom Auftragnehmer beauftragten Unterauftragsverarbeiter; ihre Einschaltung ergibt sich aus der technischen Funktionsweise des Web-Push-Standards und der Gerätewahl des Betroffenen.
4. Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter im Wege eines Vertrags im Wesentlichen dieselben Datenschutzpflichten auf, wie sie in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO), insbesondere hinreichende Garantien für technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Unterauftragsverarbeiters.

§ 7 Kontrollrechte

Der Auftraggeber kann sich vor Beginn und während der Verarbeitung von der Einhaltung dieses Vertrags überzeugen, insbesondere durch Auskünfte des Auftragnehmers und Vorlage der Dokumentation der technischen und organisatorischen Maßnahmen. Der Auftragnehmer stellt alle erforderlichen Informationen zum Nachweis der Pflichten aus Art. 28 DSGVO bereit und ermöglicht auf Verlangen Überprüfungen – einschließlich Inspektionen – durch den Auftraggeber oder einen von diesem beauftragten, zur Vertraulichkeit verpflichteten Prüfer und trägt zu ihnen bei (Art. 28 Abs. 3 lit. h DSGVO). Zeitpunkt und Umfang werden mit angemessenem Vorlauf abgestimmt; Geschäftsgeheimnisse des Auftragnehmers und Daten anderer Kunden bleiben geschützt.

§ 8 Weisungen

Weisungen erfolgen in Textform an info@atendu.eu bzw. support@atendu.eu. Weisungsberechtigt ist der Inhaber des Kundenkontos (Buchungs-E-Mail-Adresse). Hält der Auftragnehmer eine Weisung für datenschutzrechtlich unzulässig, weist er den Auftraggeber unverzüglich darauf hin.

§ 9 Löschung nach Auftragsende

1. Benachrichtigungs-Abonnements und Aufruf-Daten werden bereits während der Laufzeit automatisiert gelöscht (Aufruf-Status nach wenigen Stunden, ungültige Abonnements sofort).
2. Nach Ende des Hauptvertrags löscht der Auftragnehmer nach Wahl des Auftraggebers alle verbleibenden im Auftrag verarbeiteten Daten (Push-Abonnements) oder gibt sie in einem gängigen, maschinenlesbaren Format an ihn heraus und löscht sie anschließend. Trifft der Auftraggeber keine Wahl, erfolgt spätestens 30 Tage nach Vertragsende die automatisierte Löschung. Server-Logs rotieren unabhängig davon nach 7 Tagen.
3. Eigene Daten des Auftraggebers (Konto-, Vertrags- und Abrechnungsdaten) sind nicht Gegenstand dieses Vertrags; insoweit ist der Auftragnehmer selbst Verantwortlicher (siehe Datenschutzerklärung).

§ 10 Schlussbestimmungen

1. Dieser Vertrag wird elektronisch geschlossen (Art. 28 Abs. 9 DSGVO): Er ist Bestandteil der Buchung des Cloud-Abos und wird mit der dortigen Bestätigung akzeptiert; Fassungsstand und Zeitpunkt der Zustimmung werden vom Auftragnehmer dokumentiert.
2. Es gilt deutsches Recht. Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- Transportverschlüsselung durchgängig (HTTPS/TLS)
- Server in Deutschland; Zugang ausschließlich per SSH-Schlüssel, nur der Auftragnehmer
- Datensparsamkeit by Design: keine Namen/Kontaktdaten der Endkunden; Push-Abonnements als pseudonyme Endpunkt-Tokens; Nummern statt Identitäten
- Push-Nachrichteninhalte nach Web-Push-Standard verschlüsselt (für Zustelldienste nicht lesbar)
- Zugriffsschutz der Schnittstellen durch Token-Authentifizierung; Rate-Limits und Missbrauchs-Schutzmechanismen
- Datensicherung: tägliche Backups, vor Off-site-Übertragung clientseitig verschlüsselt (AES-256, Schlüssel nur beim Auftragnehmer); automatische Rotation
- Log-Rotation nach 7 Tagen; automatisierte Löschroutinen (Aufruf-Status nach wenigen Stunden, Abonnements abgelaufener Verträge nach 30 Tagen)
- Keine externen CDNs, keine Analyse-/Tracking-Dienste

- Patch-Management: sicherheitsrelevante Updates des Server-Betriebssystems werden täglich automatisch installiert; dafür erforderliche Neustarts erfolgen automatisch im nächtlichen Wartungsfenster (03–06 Uhr MEZ). Die Abhängigkeiten der Anwendung werden wöchentlich auf bekannte Schwachstellen geprüft
- Minimalrechte: die Anwendung läuft unter einem eigenen, unprivilegierten Systemkonto in einer systemd-Sandbox (nur Lesezugriff auf das System, Schreibzugriff ausschließlich auf ihre Datenbank)
- Betriebsüberwachung: automatische Prüfungen von Verfügbarkeit, Dienstzustand und Neustarts mit Alarmierung des Auftragnehmers

Fassung

Fassung dieses Auftragsverarbeitungsvertrags: 12.10.2026 (Vorfassung 12.07.2026; geändert: Anlage 1 – Ergänzung um Patch-Management, Minimalrechte und Betriebsüberwachung. Davor 07.07.2026; geändert: § 3 Abs. 2 – Präzisierung der Drittlandübermittlung bei Push-Diensten)