IDO Haus · idohaus.de

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 29.10.2026

Vertragsparteien

Verantwortlicher (Auftraggeber): der Kunde von IDO Haus, wie in seinem Kundenkonto angegeben (im Folgenden „Kunde“)

Auftragsverarbeiter (Auftragnehmer): IDO GmbH, Anderslebener Straße 40, 39387 Oschersleben, vertreten durch den Geschäftsführer Martin Leue, E-Mail info@ido-gmbh.de (im Folgenden „wir“)

Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen von IDO Haus (§ 9 AGB) und gilt für jedes Kundenkonto, ohne dass er gesondert unterschrieben werden muss. Er wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Die aktuelle Fassung steht unter https://idohaus.de/avv; im Kundenkonto steht sie unter „Einstellungen“ als PDF mit den Firmendaten des Kunden bereit.

§ 1 Gegenstand und Dauer

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch uns im Auftrag des Kunden, wenn er IDO Haus (idohaus.de) mit einem Kundenkonto nutzt, um Inhalte auf Bildschirmen an seinen Standorten anzuzeigen. Den Umfang der Leistungen beschreiben die AGB und die Preisseite. Dazu gehören, je nach Nutzung:

- die Speicherung und Auslieferung der Inhalte, die der Kunde hochlädt oder eingibt (Bilder, PDF-Aushänge, Videos, Texte, Webseiten-Verweise), an seine Bildschirme,
- die Verwaltung von Standorten, Bildschirmen, Playlisten und Anzeige-Einstellungen,
- auf Wunsch des Kunden: Nachweise per RFID-Karte (Reinigungsnachweis, Anwesenheit, wiederkehrende Aufgaben) mit den dafür angelegten Personen und Berichten,
- auf Wunsch des Kunden: die Anzeige von Werten einer Photovoltaikanlage oder Wärmepumpe,
- die Überwachung und Fernwartung der Anzeigegeräte (Zustand, Softwarestand, Aktualisierungen).

(2) Nicht Gegenstand dieses Vertrags sind Daten, die wir als eigener Verantwortlicher verarbeiten, zum Beispiel die Zugangs- und Abrechnungsdaten des Kundenkontos, Server-Protokolle, die Reichweitenmessung und Anfragen über das Kontaktformular. Dafür gilt unsere Datenschutzerklärung.

(3) Der Vertrag gilt, solange das Kundenkonto besteht, und darüber hinaus, solange wir noch Daten des Kunden speichern (§ 9). Pflichten, die ihrer Natur nach über das Vertragsende hinaus gelten, insbesondere zur Löschung und zur Vertraulichkeit, bleiben bestehen.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen

(1) **Art der Verarbeitung:** Erheben (Upload, Eingabe, Kartenscan am Gerät), Speichern, Anzeigen auf den Bildschirmen des Kunden, Auswerten zu Berichten, Bereitstellen zum Export (CSV) und Löschen.

(2) **Zweck:** Information von Bewohnern, Patienten, Kunden und Besuchern an den Standorten des Kunden sowie, wenn der Kunde die Funktionen nutzt, der Nachweis von Reinigungen, Anwesenheiten und erledigten Aufgaben.

(3) **Art der Daten:**

- Inhalte, die der Kunde hochlädt oder eingibt, mit allen darin enthaltenen Angaben (zum Beispiel Namen auf einem Aushang),
- Personen, die der Kunde für Nachweise anlegt: Name, Rolle, gegebenenfalls Firma, Kennung der zugeordneten RFID-Karte,
- Nachweisdaten: Beginn, Ende und Dauer von Reinigungen mit Beteiligten, Kommen und Gehen, Quittierung von Aufgaben, Kartenscans mit Gerät und Zeitpunkt,
- Gerätedaten: Name und Standort des Geräts, Zustand, Temperatur, Softwarestand, Ereignisse; Energiewerte der angebundenen Anlagen.

(4) **Betroffene Personen:** Beschäftigte des Kunden und von ihm beauftragter Firmen (etwa Reinigungskräfte, Hausmeister, Handwerker), Personen, die in hochgeladenen Inhalten genannt oder abgebildet sind.

§ 3 Weisungen

(1) Wir verarbeiten die Daten nur auf dokumentierte Weisung des Kunden. Die Weisungen ergeben sich aus diesem Vertrag und aus der Nutzung der Funktionen von IDO Haus: Was der Kunde im Konto hochlädt, anlegt, einstellt (insbesondere die Löschfrist für Nachweise), exportiert oder löscht, gilt als Weisung. Weitere Weisungen erteilt der Kunde in Textform, etwa per E-Mail an info@ido-gmbh.de. Weisungsberechtigt ist, wer Zugang zum Kundenkonto hat oder den Kunden vertritt.

(2) Verpflichtet uns das Recht der EU oder Deutschlands zu einer anderen Verarbeitung, teilen wir dem Kunden das vorher mit, sofern das Recht diese Mitteilung nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(3) Halten wir eine Weisung für rechtswidrig, weisen wir den Kunden unverzüglich darauf hin (Art. 28 Abs. 3 Satz 3 DSGVO).

§ 4 Unsere Pflichten

(1) Wir verarbeiten die Daten ausschließlich, um die vereinbarten Leistungen zu erbringen, nicht für eigene Zwecke, nicht für Werbung und nicht zum Training von KI-Modellen. In Inhalte und Nachweise des Kunden sehen wir nur, soweit es für Support oder Fehlerbehebung nötig ist, und nur auf Anfrage oder mit Zustimmung des Kunden.

(2) Personen, die bei uns Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO).

(3) Wir treffen die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Wir dürfen sie an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt.

(4) Wir unterstützen den Kunden mit geeigneten Maßnahmen dabei, Anfragen betroffener Personen zu beantworten (Art. 12 bis 23 DSGVO). Vieles kann der Kunde selbst im Konto erledigen, etwa die Nachweise zu einer Person ansehen, als CSV exportieren, korrigieren oder die Person löschen. Wenden sich Betroffene direkt an uns, leiten wir die Anfrage unverzüglich an den Kunden weiter.

(5) Wir unterstützen den Kunden bei seinen Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung) im Rahmen der Art der Verarbeitung und der uns vorliegenden Informationen.

(6) Werden uns Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt, melden wir sie dem Kunden unverzüglich per E-Mail an die Adresse seines Kundenkontos, mit den Angaben nach Art. 33

Abs. 3 DSGVO, soweit sie uns vorliegen.

(7) Wir verarbeiten die Daten ausschließlich in Deutschland (§ 7).

§ 5 Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er bestimmt, welche Inhalte angezeigt, welche Personen mit Karten erfasst und wie lange Nachweise aufbewahrt werden.

(2) Nutzt der Kunde Nachweise per Karte für Beschäftigte, informiert er sie vorher und beteiligt, soweit vorhanden, die Arbeitnehmervertretung. Erfasst er Beschäftigte anderer Firmen (etwa eines Reinigungsdienstes), sorgt er dafür, dass diese Firma ihre Beschäftigten informiert.

(3) Er zeigt auf den Bildschirmen nur Inhalte, die er zeigen darf, und achtet darauf, dass Aushänge keine personenbezogenen Daten enthalten, die Vorbeigehende nicht sehen sollen.

(4) Er informiert uns unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde ist mit den in Anlage 2 genannten Unterauftragsverarbeitern einverstanden (allgemeine Genehmigung nach Art. 28 Abs. 2 DSGVO).

(2) Wollen wir einen Unterauftragsverarbeiter hinzunehmen oder ersetzen, informieren wir den Kunden mindestens vier Wochen vorher per E-Mail an die Adresse seines Kundenkontos. Der Kunde kann der Änderung bis zu ihrem Wirksamwerden in Textform widersprechen. Können wir den Einwand nicht ausräumen, kann der Kunde den Vertrag zum Wirksamwerden der Änderung kündigen.

(3) Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO).

(4) Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind der Zahlungsdienstleister Stripe, der nur die Daten des Abos verarbeitet und keinen Zugang zu den Inhalten hat (dafür sind wir selbst Verantwortlicher), sowie der Internetanschluss und die Anlagen des Kunden (etwa der Wechselrichter einer Photovoltaikanlage), mit denen die Geräte vor Ort verbunden sind.

§ 7 Ort der Verarbeitung

Die Verarbeitung auf unseren Servern findet ausschließlich in Rechenzentren in Deutschland statt. Daneben liegen die Inhalte, die ein Bildschirm anzeigt, und offene Kartenscans zwischengespeichert auf dem Anzeigegerät beim Kunden vor Ort, damit die Anzeige auch ohne Internet weiterläuft. Eine Übermittlung in ein Drittland findet nicht statt. KI-Dienste setzen wir für die Verarbeitung nicht ein.

§ 8 Nachweise und Kontrollen

(1) Wir weisen die Einhaltung unserer Pflichten in erster Linie durch Auskünfte und Unterlagen nach, etwa die Beschreibung der Maßnahmen in Anlage 1 und Nachweise unserer Unterauftragsverarbeiter.

(2) Reicht das nicht aus, kann der Kunde sich nach Anmeldung mit angemessener Frist während der üblichen Geschäftszeiten selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer von der Einhaltung überzeugen (Art. 28 Abs. 3 lit. h DSGVO). Die Kontrolle darf den Betrieb nicht unverhältnismäßig stören und muss die Vertraulichkeit der Daten anderer Kunden wahren. Prüfer, die mit uns im Wettbewerb

stehen, dürfen wir ablehnen.

§ 9 Löschung und Rückgabe

(1) Der Kunde kann Berichte zu Reinigungen und Anwesenheiten jederzeit als CSV exportieren und seine hochgeladenen Inhalte selbst herunterladen. Das ist die Rückgabe der Daten im Sinne von Art. 28 Abs. 3 lit. g DSGVO; auf Wunsch stellen wir weitere Daten in einem gängigen Format bereit.

(2) Der Kunde kann einzelne Inhalte, Personen und Nachweise jederzeit selbst löschen und eine Löschfrist einstellen, nach der Nachweise automatisch gelöscht werden.

(3) Löscht der Kunde sein Konto, löschen wir alle Daten des Kontos sofort aus Datenbank und Dateiablage; aus Datensicherungen verschwinden sie, wenn diese turnusmäßig überschrieben werden. Endet das Abo, ohne dass der Kunde sein Konto löscht, bleiben die Daten gespeichert, bis er das Konto löscht oder uns um Löschung bittet; die Geräte zeigen bis dahin den letzten Stand.

(4) Im Einzelnen gelten folgende Fristen:

Daten	Löschung
Reinigungsnachweise, Anwesenheiten, Aufgabenbuchungen und Kartenscans	nach der im Konto unter „Anzeige“ eingestellten Löschfrist in Monaten automatisch; ohne Einstellung, bis der Kunde sie löscht oder das Konto gelöscht wird. Offene Reinigungen und Anwesenheiten bleiben bis zu ihrem Abschluss stehen.
Personen (Name, Rolle, Kartennummer)	sobald der Kunde die Person löscht, spätestens mit dem Konto
Hochgeladene Inhalte (Bilder, PDF, Videos, Texte)	sobald der Kunde sie löscht, spätestens mit dem Konto
Alle Daten des Kontos beim Löschen des Kontos	sofort (Datenbank und Dateien); Datensicherungen werden turnusmäßig überschrieben
Gerätedaten (Zustand, Temperatur, Softwarestand, Ereignisse)	laufend überschrieben; mit dem Gerät gelöscht

§ 10 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln der AGB (§ 10).

(2) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes den AGB vor.

(3) Es gilt deutsches Recht. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

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

Vertraulichkeit

- **Rechenzentrum:** Die Server stehen in einem Rechenzentrum in Deutschland (Anlage 2). Zutritt und physische Sicherheit regelt der Betreiber des Rechenzentrums; wir selbst haben keinen physischen Zugang zu den Servern.
- **Zugang zu den Servern:** nur für beauftragte Administratoren der IDO GmbH, nur über verschlüsselte Verbindungen.

- **Anmeldung im Kundenkonto:** Passwort mit mindestens 10 Zeichen, gespeichert nur als Hash (Argon2id). Zwei-Faktor-Anmeldung mit einer Authenticator-App (TOTP) und Notfallcodes. Nach wiederholten Fehlversuchen ist die Anmeldung vorübergehend gesperrt.
- **Sitzung:** Sitzungs-Cookie nur über HTTPS, für Skripte nicht lesbar (HttpOnly), nicht an fremde Seiten mitgesendet (SameSite), ungültig nach 8 Stunden ohne Aktivität.
- **Geräte:** Jedes Anzeigegerät meldet sich mit einem eigenen, geheimen Schlüssel an und erhält nur die Inhalte und Daten seines eigenen Kontos. Ein Schlüssel lässt sich im Konto jederzeit neu erzeugen; der alte ist dann ungültig.
- **Trennung:** Jede Abfrage ist an das Konto des angemeldeten Kunden gebunden. Unsere Betreiber-Übersicht zeigt Kennzahlen und den Zustand der Geräte; in Inhalte und Nachweise eines Kunden sehen wir nur für Support und nur auf dessen Wunsch.
- **Anzeige:** Auf dem Bildschirm erscheinen von Personen nur Vornamen. Kamera, Mikrofon oder eine Erfassung von Passanten gibt es nicht; gelesen werden nur ausgegebene RFID-Karten.
- **Transport:** Alle Verbindungen zur Anwendung laufen über HTTPS (TLS) mit HSTS, auch die der Geräte.

Integrität

- **Schutz der Anwendung:** CSRF-Schutz für alle Formulare, strenge Content-Security-Policy, keine Skripte oder Schriften fremder Anbieter, Einbetten in fremde Seiten untersagt, Bot-Schutz ohne externen Dienst.
- **Nachvollziehbarkeit:** Korrekturen an Anwesenheiten werden mit Zeitpunkt gespeichert; Kartenscans werden mit Gerät und Zeitpunkt protokolliert.

Verfügbarkeit und Belastbarkeit

- Die Anzeigegeräte halten die aktuellen Inhalte lokal vor und laufen bei einem Ausfall der Internetverbindung oder unseres Servers mit dem letzten Stand weiter; Kartenscans werden nachgereicht.
- Die Datenbank wird regelmäßig gesichert. Vor jeder Aktualisierung der Anwendung wird der neue Stand automatisch geprüft; bei einem Fehler lässt sich der vorherige Stand wiederherstellen.
- Wir sehen, wenn ein Gerät nicht mehr erreichbar ist, und zeigen es dem Kunden im Konto an.

Regelmäßige Überprüfung

- Wir überprüfen die Maßnahmen bei jeder wesentlichen Änderung der Anwendung und passen sie an den Stand der Technik an. Unterauftragsverarbeiter setzen wir nur mit Vertrag zur Auftragsverarbeitung ein (Anlage 2).

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
[Rechenzentrum: Anbieter und Anschrift]	Rechenzentrum und Server: Betrieb der Anwendung und der Datenbank, Speicherung der hochgeladenen Inhalte; Versand unserer Benachrichtigungsmails über unseren eigenen Mailserver	Deutschland kein Drittland

Stand dieser Fassung: 29.10.2026

Dokument erstellt am 01.11.2026 aus https://idohaus.de/avv. Elektronisch geschlossen als Bestandteil der AGB, ohne Unterschrift gültig (Art. 28 Abs. 9 DSGVO). IDO GmbH · Anderslebener Straße 40 · 39387 Oschersleben · Amtsgericht Stendal, HRB 106935