aventrel GbR
Rautenbergstraße 15
24306 Plön, Deutschland
Ahmad Taha Tellawi
Mhamed Amjad Tellawi
info@aventrel.com

# Datenschutzerklärung

MizanCheck | Website und Anwendungen | Version 1.0 | Stand 07.10.2026

Diese Hinweise beschreiben die öffentliche Website und die Einrichtung, Nutzung und Betreuung von Restaurant, Delivery und Restaurant plus Delivery. Sie ersetzen nicht die Datenschutzhinweise des jeweiligen Betriebs gegenüber Gästen und Beschäftigten.

## 1. Verantwortlicher und Kontakt

aventrel GbR, vertreten durch Ahmad Taha Tellawi und Mhamed Amjad Tellawi, Rautenbergstraße 15, 24306 Plön, Deutschland. E-Mail und Datenschutzanfragen: info@aventrel.com. Telefon: 0162 6094517.

Öffentliche Produktwebsite: mizanchecklog.com. Die Anwendungen werden unter der Produktdomain mizancheck.app und ihren Anwendungs-Subdomains sowie über die bereitgestellte MizanCheck-App angeboten.

## 2. Verantwortlichkeit und Rechtsgrundlagen

Für eigene Interessenten-, Vertrags-, Rechnungs-, Lizenz-, Geräteverwaltungs- und erforderliche Sicherheitsdaten ist aventrel verantwortlich. Vertragsdurchführung und vorvertragliche Maßnahmen für natürliche Personen als Vertragspartei beruhen auf Art. 6 Abs. 1 Buchst. b DSGVO. Für Unternehmensansprechpartner gilt regelmäßig Art. 6 Abs. 1 Buchst. f DSGVO; berechtigtes Interesse ist die Bearbeitung der Anfrage und Geschäftsbeziehung. Gesetzliche Pflichten beruhen auf Art. 6 Abs. 1 Buchst. c DSGVO.

Für operative Gäste-, Kunden-, Bestell-, Fahrer- und Beschäftigtendaten bestimmt grundsätzlich der Restaurant- oder Lieferdienstbetrieb Zwecke, Rechtsgrundlagen, Berechtigungen und Fristen. Soweit aventrel diese Daten für ihn verarbeitet, erfolgt dies nach Art. 28 DSGVO auf Grundlage einer AVV und dokumentierter Weisungen. Diese Funktionsbeschreibung ist keine pauschale Einwilligung der Betroffenen.

## 3. Aufruf, Hosting und Sicherheit

Für Auslieferung, Fehleranalyse und Angriffsschutz werden technisch erforderliche Verbindungsdaten verarbeitet, insbesondere IP-Adresse, angeforderte Adresse, Zeitpunkt, Status und technische Browserangaben. In unserer eigenen Verantwortung ist Grundlage Art. 6 Abs. 1 Buchst. f DSGVO; unser Interesse ist ein sicherer, funktionsfähiger Dienst.

Zentrale Anwendung und Datenbank laufen bei Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland. Für zentrale Sicherungs- und Speicheraufgaben wird außerdem eine Hetzner Storage Box eingesetzt. Verbindungsprotokolle, Betriebsdaten und Sicherungen sind getrennte Bestände. Aus dem Anbieter allein folgt keine Zusage eines bestimmten Speicherorts oder einer vollständigen Verschlüsselung aller Daten.

Technische Protokolle sind nur für erforderliche Diagnose, Sicherheit und die Aufklärung konkreter Vorfälle vorzuhalten. Danach sind sie zu löschen oder zu anonymisieren, soweit keine gesetzliche Pflicht oder konkrete Rechtsverteidigung entgegensteht. Es wird kein ungeprüfter pauschaler automatischer Löschlauf zugesagt.

## 4. Kontaktformular

Das Formular übermittelt Betriebsname, E-Mail-Adresse, optional Telefonnummer, gewünschtes Produkt und Paket, gegebenenfalls Gerätezahl sowie Nachricht an unseren Server. Betriebsname, E-Mail und Nachricht sind erforderlich. Die Anfrage wird in der Datenbank gespeichert und im geschützten Admin-Center bearbeitet; ein eigenes E-Mail-Programm muss nicht geöffnet werden. Für E-Mail- und Telefonkontakt gelten dieselben zweckbezogenen Grundlagen aus Abschnitt 2.

Zur Missbrauchsbegrenzung verwenden wir eine zeitliche Begrenzung je E-Mail und ein unsichtbares Formularfeld. In der Anfragedatenbank wird keine zusätzliche IP-Adresse gespeichert; technisch notwendige Sicherheitsprotokolle sind davon getrennt. Aufbewahrung erfolgt für die Bearbeitung, eine daraus entstehende Geschäftsbeziehung, gesetzliche Pflichten oder konkrete Rechtsansprüche. Entfallen diese Zwecke, sind die Angaben zu löschen.

## 5. Darstellung und Kampagnenangaben

Darstellung und Datenschutz-Auswahl werden lokal im Browser gespeichert. Die Entscheidung ist höchstens 180 Tage gültig; die Darstellung bleibt bis zur Änderung oder Löschung der Website-Daten erhalten. Grundlage für notwendige Einstellungen ist § 25 Abs. 2 Nr. 2 TDDDG; soweit personenbezogen Art. 6 Abs. 1 Buchst. f DSGVO.

Nur nach gesonderter Zustimmung werden vorhandene UTM-Kampagnenangaben für die Browsersitzung gespeichert und einer abgesendeten Anfrage beigefügt. Sie werden nicht an externe Analysedienste übertragen. Grundlagen sind § 25 Abs. 1 TDDDG und Art. 6 Abs. 1 Buchst. a DSGVO. Dies aktiviert nicht automatisch unsere eigene Webseiten-Analyse. Über „Cookie-Einstellungen“ ist jederzeit ein Widerruf für die Zukunft möglich; lokale Kampagnenangaben werden dann entfernt. Für bereits übermittelte Angaben können Sie uns kontaktieren.

Schriften und Bilder werden selbst ausgeliefert; die Seitensuche läuft im Browser. Google Analytics und externe Werbetracker sind nicht eingebunden. Bewusst geöffnete externe Links unterliegen den Hinweisen des Zielanbieters.

## 6. Freiwillige eigene Webseiten-Analyse

Nur mit gesonderter Zustimmung erfassen wir öffentliche Seitenaufrufe, ausgewählte Kontakt- und Produktklicks, grobe Gerätegruppen und Herkunftskategorien wie Instagram oder Google auf unserem Hetzner-Server. Vollständige Herkunftsadressen, Suchbegriffe, URL-Parameter und Formulareingaben werden nicht übertragen. Admin- und Kundenzugänge sind ausgeschlossen.

Nach Zustimmung wird im Sitzungsspeicher des Tabs eine zufällige Kennung angelegt. Nach 30 Minuten ohne Ereignis oder spätestens 24 Stunden beginnt eine neue Sitzung. Der Server verarbeitet die Kennung nur als schlüsselabhängigen Digest. Besuchs- und Ereignis-Digests verfallen nach 48 Stunden, Tageswerte nach 180 Tagen; abgelaufene Einträge werden bei der nächsten Erfassung oder Auswertung gelöscht. Es gibt keine dauerhafte Besucherkennung, kein Fingerprinting und keine Verknüpfung mit Kundenkonten.

Grundlagen sind Art. 6 Abs. 1 Buchst. a DSGVO und § 25 Abs. 1 TDDDG. Widerruf über „Cookie-Einstellungen“ beendet neue Ereignisse und entfernt die Sitzungskennung. Do Not Track und Global Privacy Control werden berücksichtigt.

Datenschutz-Entscheidungen werden auch als reine Tageszähler ausgewertet. Bei Ablehnung werden keine Sitzungskennung, Seite, Herkunft oder Gerätegruppe übertragen. Zur Missbrauchsbegrenzung dieses Endpunkts werden kurzzeitig schlüsselabhängige minutenbezogene Netzwerk-Digests verarbeitet und spätestens nach zwei Minuten zur Löschung vorgesehen. Rohe IP-Adressen und Browserkennungen werden nicht in den Analyse-Daten gespeichert. Grundlage für Schutz und Verwaltung dieser Auswahl ist Art. 6 Abs. 1 Buchst. f DSGVO; notwendige Serverprotokolle sind getrennt.

## 7. Cloudflare und Leistungsmessung

Cloudflare, Inc. liefert die öffentliche Website aus und schützt sie vor Angriffen. Dabei fallen Verbindungs- und Sicherheitsdaten an. Grundlage für diese notwendige Auslieferung und Absicherung ist Art. 6 Abs. 1 Buchst. f DSGVO; Interesse ist ein sicherer Webauftritt.

Zusätzlich ist Cloudflare Web Analytics zur technischen Leistungsmessung eingerichtet. Außerhalb der EU kann das Skript Ladezeiten und Seitenaufrufe erfassen. In unserer Konfiguration ist seine automatische Einbindung für Besucher aus der EU ausgeschlossen. Admin- und Kundenzugänge sind nicht für das Statistik-Skript freigegeben. Die Messung ist von unserer freiwilligen eigenen Analyse getrennt.

Nach Anbieterangaben setzt Web Analytics keine Analyse-Cookies ein und verfolgt Besucher nicht über verschiedene Kunden-Websites hinweg. Dies bedeutet nicht, dass Auslieferung und Sicherheit ohne personenbezogene Daten auskommen. Weitere Informationen: Cloudflare-Datenschutzrichtlinie und Web-Analytics-Dokumentation.

## 8. Verträge, PDFs und Bildschirmunterschriften

Für Angebote, Verträge, AVV, Lizenzen, Rechnungen und Support verarbeiten wir erforderliche Firmen- und Kontaktangaben, Vertretungsrollen, gebuchten Umfang, Konditionen, Laufzeiten, Zahlungsstatus und Kommunikation nach Abschnitt 2.

Das Service-Center erstellt kundenspezifische PDF-Kopien. Nach Prüfung und ausdrücklicher Bestätigung kann eine gezeichnete Unterschrift mit Finger, Stift, Maus oder Trackpad in genau diesen Dokumentensatz eingesetzt werden. Name, Rolle, Ort, Zeitpunkt, Dokumentversion und Prüfsummen werden dokumentiert. Frühere Fassungen bleiben für erforderliche Nachweise erhalten. Eine Unterschrift wird nicht automatisch auf geänderte Unterlagen übertragen.

Die Zeichnung ist keine zertifikatsbasierte qualifizierte elektronische Signatur; es erfolgt keine biometrische Identitätsprüfung anhand der Zeichnung. Vertragsnachweise werden während der Beziehung und nach den einschlägigen Aufbewahrungs- und Verjährungsregeln vorgehalten. Die Dauer richtet sich nach Dokumentart, Abschlussjahr und offenen Ansprüchen. Operative Supportanhänge werden auf den konkreten Zweck begrenzt und nach Kundenweisung beziehungsweise Zweckende entfernt.

## 9. Lizenz und Gerätezuordnung

Die Lizenz ordnet den Zugang einem Betrieb zu. Die App-Auswahl Restaurant, Delivery oder beide erweitert keine Rechte. Weitere Geräte setzen bestehende PINs nicht allein durch ihre Einrichtung zurück. Authentifizierungswerte werden serverseitig als geschützte Hashwerte verarbeitet, nicht als Klartext-PIN in der Geräteverwaltung.

Erfasst werden erzeugte Geräte- oder Installationskennung, öffentlicher Geräteschlüssel und Digest, Bezeichnung, Zweck, Plattform sowie Einrichtungs-, letzte Nutzungs- und Widerrufszeitpunkte. Dies dient Zuordnung, Sicherheit und Prüfung gebuchter Service-, Küchen- und Kassengeräte. Abgewiesene Überschreitungsversuche können mit Geräte-, Akteur- und Zeitbezügen protokolliert und berechtigten Administratoren angezeigt werden.

Es wird keine MAC-Adresse ausgelesen und kein Werbe-Fingerprinting eingesetzt. Zuordnung und Schlüssel werden im vorgesehenen geschützten Gerätespeicher beziehungsweise im Browser in IndexedDB gespeichert, bis zur Entfernung oder Neueinrichtung. Widerruf beendet die Berechtigung, entfernt aber nicht automatisch lokale Reste. Grundlage sind Vertragsdurchführung und Missbrauchsschutz; für unbedingt erforderlichen Endgerätespeicher § 25 Abs. 2 Nr. 2 TDDDG. Nachweise werden für Vertragszuordnung, Widerrufsschutz und erforderliche Rechtsansprüche vorgehalten, nicht unbegrenzt für allgemeine Beobachtung.

## 10. Cloud, App und Hybridbetrieb

Im Cloudbetrieb ist die zentrale Plattform die operative Datenbank. Eine App-Installation macht dies nicht zu ausschließlich lokaler Speicherung. Restaurant umfasst je nach Buchung Tische, Reservierungen, Kundenkontakte, Gerichte, Zutaten, Rezepte, Lagerbewegungen, Bestellungen, Gangfreigaben, Küchenbereiche, Zahlungen, Belege und Abschlüsse. Delivery ergänzt Lieferadressen, Telefonnummern, Kundenhistorie, Fahrerzuordnungen, Schichten und Lieferstatus.

Änderungsprotokolle enthalten gegebenenfalls Zeit, Mitarbeiter, Grund sowie Zustände vor und nach Anlage, Änderung, Storno oder Rabatt. Küchenmonitore zeigen relevante Positionen und Hinweise. Das Protokoll und ein Vorbereitungsstatus sind keine TSE-Signatur. Ein TSE-Anbieter ist erst nach konkreter Beauftragung und Einrichtung ein zusätzlicher Empfänger; eine nicht verbundene TSE ist keine erfolgreiche Absicherung.

Ein ausdrücklich eingerichteter lokaler Restaurant-Gateway verarbeitet vereinbarte Daten zusätzlich auf der lokalen Zentrale und gleicht bestätigte Vorgänge mit der Cloud ab. Dabei entstehen Benutzer-, Geräte-, Bestell-, Küchen-, Zahlungs-, Beleg-, Revisions- und Synchronisierungsbezüge. Bei Internetausfall bleiben funktionsfähiges lokales WLAN oder LAN, Stromversorgung und die eingerichteten Geräte nötig. Die lokale Speicherung allein ermöglicht keine Übergabe zur Küche bei vollständigem Netzausfall. Delivery-Entwürfe sind kein freigegebener lokaler Mehrgerätebetrieb.

Die App kann Zuordnung und unfertige Bestellentwürfe einschließlich eingegebener Kundendaten im geschützten nativen Speicher ablegen. Dies dient dem angeforderten Vorgang, nicht Werbung (§ 25 Abs. 2 Nr. 2 TDDDG; im Übrigen Kundenweisung oder Vertragszweck). Entwürfe sind nach Zweckende und vor Geräteweitergabe zu berücksichtigen; zentrale Löschung entfernt sie nicht zwangsläufig. Die Weboberfläche unterscheidet Schutz laufender Eingaben von dauerhafter zentraler Speicherung.

## 11. Mitarbeiter und Lohnkosten

Teamfunktionen können Name und Kennung, Rolle, Rechte, Schichten, Arbeitszeiten und Pausen, Stundenlöhne sowie errechnete Arbeitsstunden und Bruttolohnkosten verarbeiten. Vorgangsprotokolle können den handelnden Mitarbeiter zuordnen.

Der Arbeitgeber bestimmt zulässige Zwecke, Fristen und Zugriffe und informiert Beschäftigte. Je nach Zweck kommt § 26 BDSG in Verbindung mit der DSGVO in Betracht; die App-Nutzung begründet keine allgemeine Einwilligung. Mitbestimmungsrechte bleiben unberührt. Lohnkostenanzeigen sind keine vollständige steuerliche oder sozialversicherungsrechtliche Lohnabrechnung. aventrel trifft keine ausschließlich automatisierten Beschäftigtenentscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung.

## 12. Allergiehinweise

Die Auswahl „Wegen Allergie“ oder „Keine Allergie“ bei Zutatenentfernung kann mit Gericht und Auftrag gespeichert und der zuständigen Küche angezeigt werden. Auch Tisch- und Bestellbezüge können Personen identifizierbar machen. Personenbezogene Allergieangaben sind gegebenenfalls Gesundheitsdaten nach Art. 9 DSGVO.

Der Betrieb benötigt neben einer allgemeinen Rechtsgrundlage eine geeignete Ausnahme nach Art. 9 Abs. 2 DSGVO, etwa eine tatsächlich ausdrücklich erteilte Einwilligung, soweit deren Voraussetzungen vorliegen. Der Klick des Kellners ist nicht selbst die Einwilligung des Gastes. Angaben sind auf notwendige Zutaten- und Küchenhinweise zu beschränken; unnötige Diagnosen und dauerhafte Gesundheitsprofile sind zu vermeiden. Zugriff und kurze zweckbezogene Fristen sind in der Kundenweisung festzulegen. Die Funktion ersetzt keine sichere Küchenpraxis.

## 13. Sprache und Adressvorschläge

Spracherkennung beginnt nach bewusster Betätigung und erforderlicher Mikrofonfreigabe. Je nach Browser oder Betriebssystem kann der Anbieter Sprache auf eigenen Servern verarbeiten, auch außerhalb des EWR. Ausschließlich lokale Erkennung wird nicht zugesichert. Die Browserberechtigung ist nicht automatisch eine datenschutzrechtliche Zustimmung aller Betroffenen.

MizanCheck speichert keine Audioaufnahme. Erkannter oder eingegebener Text kann zur Vorschau an unseren Server übermittelt und gegen Katalog beziehungsweise Adresseingaben geprüft werden. Erst bestätigte Angaben werden als Auftrag oder Kundendaten übernommen. Telefonate werden nicht automatisch aufgenommen; Texteingabe bleibt möglich. Vor Einsatz für personenbezogene Inhalte prüft der Betrieb den tatsächlich verwendeten Sprachanbieter, die Rechtsgrundlage und etwaige Drittlandübermittlungen.

Für angeforderte Adressvorschläge fragt unser Server OpenPLZ API mit Straßenname oder Suchmuster, gegebenenfalls Ort und regionaler Postleitzahlfilterung ab. Namen, Telefonnummern, Hausnummern, Bestellpositionen und die Geräte-IP des Besuchers werden dabei nicht bewusst an diesen Dienst übertragen. Der Anbieter erhält Suchangaben und Serververbindung. Die Suche ist regional begrenzt; Ergebnisse werden vorübergehend prozessintern zwischengespeichert und müssen geprüft werden. Grundlage ist der angeforderte Bestellablauf im Kundenauftrag. Anbieterinformationen: OpenPLZ-Dokumentation.

## 14. Notwendige Sitzungen

Die gemeinsame Restaurant- und Produkt-Websitzung verwendet __Host-mizancheck_online_session mit höchstens zwölf Stunden. Delivery verwendet je nach Zugang mizancheck_delivery_session oder mizancheck_delivery_de_session mit höchstens 16 Stunden. Die Verwaltungssitzung verwendet mizancheck_admin_session mit höchstens zwölf Stunden. Abmeldung beendet die jeweilige Sitzung, nicht die Aufbewahrung erforderlicher Betriebsdaten.

Die genannten Cookies sind in Produktion HttpOnly und Secure. Produkt- und Delivery-Sitzungen nutzen SameSite=Strict, die Verwaltungssitzung SameSite=Lax. Native Sitzungen folgen dem Anmeldeablauf der App. Gerätezuordnung, Darstellungs- und Bedienpräferenzen sind von freiwilliger Website-Analyse getrennt. Entwürfe und Gatewaydaten können über eine Sitzung hinaus bestehen und folgen dem betrieblichen Löschkonzept.

## 15. Empfänger und Drittlandbezüge

Zugriff erhalten erforderliche berechtigte Personen und rechtmäßig eingesetzte Dienstleister. Microsoft 365 kann für geschäftliche E-Mail, Dokumentenablage und nötige Supportkommunikation verwendet werden; Anbieter ist insbesondere Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland. Dies ist kein regulärer Speicher der vollständigen operativen Datenbank. Supportinhalte sind zu minimieren. Banken, Steuerberatung, Behörden, Gerichte oder Rechtsdienstleister können bei Zahlung, gesetzlicher Pflicht oder Rechtsverteidigung Empfänger sein.

Bei Cloudflare, Microsoft und externen Sprachdiensten können außereuropäische Verarbeitungen oder Zugriffe nicht pauschal ausgeschlossen werden. Soweit erforderlich, sind ein anwendbarer Angemessenheitsbeschluss oder geeignete Garantien nach Art. 46 DSGVO, insbesondere Standardvertragsklauseln und erforderliche ergänzende Maßnahmen, Voraussetzung. Eine aktive Zertifizierung oder ein bestimmter Vertragsabschluss wird nicht ohne Prüfung bestätigt. Informationen zu konkret geltenden Empfängern und Garantien können bei info@aventrel.com angefragt werden. Cloudflare-Vertragsinformationen erläutern die vom Anbieter vorgesehenen Instrumente.

## 16. Aufbewahrung und Löschung

Der Betrieb legt dokumentierte Fristen und Weisungen für operative Daten fest. Kundenkontakte, Lieferhinweise, Allergieangaben, Arbeitszeitdaten, Finanzbelege und Sicherheitsprotokolle benötigen unterschiedliche Regeln. Storno und Gegenbuchung ersetzen keine spätere datenschutzrechtliche Löschung oder Anonymisierung. Protokollfunktionen rechtfertigen keine unbegrenzte Aufbewahrung.

Bei Vertragsende richten sich sichere Herausgabe und Löschung nach AVV und zwingendem Recht. Ein längerfristiges Abschlussarchiv besteht nur bei ausdrücklicher Vereinbarung und technischer Bereitstellung. Sicherungen können bis zum Ende ihrer vereinbarten Rotation zugriffsbeschränkt verbleiben; wirksame Löschungen sind nach Wiederherstellung erneut zu berücksichtigen. Lokale Daten und Sicherungen bleiben unter Kontrolle des Kunden. Lösch- und Sicherungsplan müssen zur beauftragten Betriebsart passen.

## 17. Rechte und erforderliche Angaben

Im gesetzlichen Umfang bestehen Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit. Einer Verarbeitung aus berechtigten Interessen können Sie aus Gründen Ihrer besonderen Situation widersprechen; bei Direktwerbung ohne diese Begründung. Einwilligungen können für die Zukunft widerrufen werden, ohne die Rechtmäßigkeit der vorherigen Verarbeitung zu berühren. Datenschutzanfragen: info@aventrel.com. Angemessene Identitäts- oder Vertretungsnachweise können erforderlich sein. Für Betriebsdaten ist grundsätzlich der jeweilige Betrieb zuständig; aventrel unterstützt nach AVV.

Beschwerden sind bei einer Datenschutzaufsichtsbehörde möglich, etwa beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstraße 98, 24103 Kiel. Pflichtangaben werden im jeweiligen Ablauf benannt; ohne notwendige Kontakt-, Vertrags- oder Anmeldedaten kann die Leistung nicht erbracht werden. Freiwillige Angaben und Funktionen sind getrennt. Es besteht keine allgemeine gesetzliche Pflicht zur Verwendung unseres Kontaktformulars.

## 18. Änderungen

Diese Hinweise werden bei wesentlichen Änderungen von Diensten, Datenflüssen oder Rechtslage aktualisiert. Wesentliche vertragsbezogene Änderungen werden zusätzlich über vereinbarte Kommunikationswege mitgeteilt. Eine Veröffentlichung allein ändert keine bestehenden Verträge oder unterschriebenen Dokumentensätze.