Datenschutzerklärung

für Mitarbeiterinnen und Mitarbeiter

Cafe Hexenstübchen · GastroSuite

Personalverwaltung · Zeiterfassung · Schichtplanung

Vertraulich · Stand April 2026

1. Verantwortliche Stelle

Verantwortlich für die Datenverarbeitung im Sinne der Datenschutz-Grundverordnung (DSGVO) ist:

Cafe Hexenstübchen
Altstadt 22
63654 Büdingen
E-Mail: info@hexenstuebchen-buedingen.de

2. Zweck der Datenverarbeitung

Im Rahmen Ihres Beschäftigungsverhältnisses setzen wir das digitale Personalverwaltungssystem **GastroSuite** ein. Dieses System dient der:

- Schichtplanung und Dienstplangestaltung
- Zeiterfassung (Ein-/Ausstempeln per Stempeluhr)
- Verwaltung von Urlaubs-, Krankheits- und Freianträgen
- Verfügbarkeitsplanung
- Lohn- und Gehaltsabrechnung
- Trinkgeldverteilung
- Warenwirtschaft und Einkaufslisten
- Kommunikation zwischen Mitarbeitern und Betriebsleitung (Schichttausch, Umplanungsanfragen)

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Erfüllung des Arbeitsvertrags) sowie Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse des Arbeitgebers an der ordnungsgemäßen Betriebsorganisation).

3. Erhobene Daten

Im System werden folgende personenbezogene Daten verarbeitet:

KATEGORIE	DATEN	ZWECK
Stammdaten	Vollständiger Name, Benutzername	Identifikation im System
Zugangsdaten	PIN (als SHA-256 Hash), Zugangspasswort (als Hash)	Authentifizierung
Beschäftigungsdaten	Beschäftigungsart, Stundenlohn, Wochenstunden-Soll	Lohnberechnung, Schichtplanung

Zeiterfassung	Einstempel-/Ausstempelzeiten, Pausendauer, Arbeitsstunden	Arbeitszeitdokumentation
Schichtdaten	Geplante Schichten, Datum, Uhrzeiten, Posten	Dienstplanung
Abwesenheiten	Urlaubsanträge, Krankheitstage, freie Tage mit Datumsbereich	Personalplanung, Urlaubskonto
Verfügbarkeit	Verfügbare Tage und Schichttypen	Schichtplanung
Vergütung	Berechneter Lohn, Zahlungsstatus, Trinkgeldzuweisungen	Lohnabrechnung
Protokolldaten	IP-Adresse, Zeitstempel, Benutzername bei Anmeldeversuchen	Sicherheit, Missbrauchsprävention

4. Zugangssicherung

Der Zugang zum System ist mehrstufig gesichert:

- **Mitarbeiter-Portal:** Benutzername + individuelles Zugangspasswort + Captcha (Schicht 1), anschließend PIN-Eingabe (Schicht 2)
- **Stempeluhr:** Globales Gerätepasswort + PIN-Eingabe

Alle Passwörter und PINs werden ausschließlich als kryptografische Hash-Werte (SHA-256 mit Salt) gespeichert. Eine Rückrechnung auf das Klartext-Passwort ist technisch nicht möglich.

5. Sicherheitsprotokollierung

Zur Absicherung des Systems werden bei fehlgeschlagenen Anmeldeversuchen folgende Daten protokolliert:

- IP-Adresse des zugreifenden Geräts
- Zeitpunkt des Versuchs
- Eingegebener Benutzername
- Bereich (Mitarbeiter-Portal, Stempeluhr, Administration)

Diese Protokolldaten dienen ausschließlich der Erkennung und Abwehr unbefugter Zugriffsversuche. Sie werden nach **14 Tagen automatisch gelöscht**.

> **Hinweis:** Bei wiederholten Fehlversuchen wird die IP-Adresse temporär gesperrt (30–60 Minuten). Bei PIN-Fehlversuchen kann der Account gesperrt werden. Die Entsperrung erfolgt durch die Betriebsleitung.

6. Speicherdauer

Ihre Daten werden wie folgt aufbewahrt:

DATENART	SPEICHERDAUER
Schichten (Dienstpläne)	2 Jahre, danach automatische Löschung
Zeiteinträge (Stempelzeiten)	2 Jahre, danach automatische Löschung
Urlaubsanträge / Abwesenheiten	Dauer des Beschäftigungsverhältnisses
Lohndaten / Zahlungen	Dauer des Beschäftigungsverhältnisses + gesetzliche Aufbewahrungsfristen
Verfügbarkeit	6 Monate, danach automatische Löschung
Schichttausch-Historie	6 Monate, danach automatische Löschung
Sicherheitsprotokolle	14 Tage, danach automatische Löschung

Nach Beendigung des Beschäftigungsverhältnisses werden Ihre Daten unter Beachtung gesetzlicher Aufbewahrungsfristen (insbesondere § 257 HGB, § 147 AO) gelöscht. Steuerlich relevante Unterlagen (Lohndaten) können bis zu 10 Jahre aufbewahrt werden.

7. Datenverarbeitung durch Dritte

Folgende Dienstleister sind an der Datenverarbeitung beteiligt:

DIENSTLEISTER	ZWECK	STANDORT
Supabase (Self-Hosted)	Datenbanksystem (PostgreSQL)	Hetzner, Deutschland
Hetzner Online GmbH	Server-Hosting	Deutschland
Cloudflare Inc.	Captcha-Verifizierung (Turnstile)	USA (mit EU-Datenschutzabkommen)
ipify.org	IP-Adress-Ermittlung für Sicherheitsprotokollierung	USA

Die Datenbank wird auf einem eigenen Server in Deutschland betrieben (Self-Hosted Supabase bei Hetzner). Es erfolgt keine Übermittlung personenbezogener Daten an Dritte zu Werbezwecken oder

sonstigen nicht genannten Zwecken.

8. Automatisierte Backups

Zur Datensicherung werden regelmäßige automatische Backups erstellt und verschlüsselt gespeichert. Die Backups enthalten:

- Mitarbeiterstammdaten (ohne Klartext-Passwörter oder PINs)
- Schichtpläne und Zeiteinträge
- Urlaubsanträge

9. Ihre Rechte

Sie haben gemäß DSGVO folgende Rechte in Bezug auf Ihre personenbezogenen Daten:

- **Auskunftsrecht (Art. 15):** Sie können jederzeit Auskunft über die zu Ihrer Person gespeicherten Daten verlangen.
- **Berichtigungsrecht (Art. 16):** Sie können die Berichtigung unrichtiger Daten verlangen.
- **Löschungsrecht (Art. 17):** Sie können die Löschung Ihrer Daten verlangen, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- **Einschränkung (Art. 18):** Sie können die Einschränkung der Verarbeitung verlangen.
- **Datenübertragbarkeit (Art. 20):** Sie können die Herausgabe Ihrer Daten in einem maschinenlesbaren Format verlangen.
- **Widerspruchsrecht (Art. 21):** Sie können der Verarbeitung Ihrer Daten widersprechen.
- **Beschwerderecht:** Sie haben das Recht, sich bei der zuständigen Datenschutzaufsichtsbehörde zu beschweren.

Zuständige Aufsichtsbehörde:

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
Gustav-Stresemann-Ring 1
65189 Wiesbaden
poststelle@datenschutz.hessen.de

10. Vertraulichkeit und Pflichten des Mitarbeiters

Als Mitarbeiter/in verpflichten Sie sich:

- Ihre Zugangsdaten (PIN und Zugangspasswort) geheim zu halten und nicht an Dritte weiterzugeben
- Sich nicht mit den Zugangsdaten anderer Mitarbeiter anzumelden

- Die Stempeluhr nur für Ihre eigenen Ein- und Ausstempelungen zu verwenden
- Auffälligkeiten oder den Verdacht auf Missbrauch unverzüglich der Betriebsleitung zu melden
- Bei Verlust oder Kompromittierung der Zugangsdaten sofort die Betriebsleitung zu informieren

11. Änderungen dieser Erklärung

Diese Datenschutzerklärung kann bei Änderungen des Systems oder der rechtlichen Rahmenbedingungen angepasst werden. Über wesentliche Änderungen werden Sie informiert.

Einwilligungs- und Kenntnisnahmeerklärung

Ich bestätige, dass ich die vorstehende Datenschutzerklärung zur Kenntnis genommen habe. Ich bin über die Erhebung, Verarbeitung und Nutzung meiner personenbezogenen Daten im Rahmen des Beschäftigungsverhältnisses informiert worden. Meine Rechte gemäß DSGVO sind mir bekannt.

Ich bin damit einverstanden, dass meine im Abschnitt 3 genannten Daten im System GastroSuite für die genannten Zwecke verarbeitet werden. Mir ist bekannt, dass die Sicherheitsprotokollierung (IP-Adresse, Fehlversuche) zum Schutz des Systems und meiner Daten erfolgt.

Name des Mitarbeiters (Druckschrift) _____ Personalnummer _____

Ort, Datum _____ Unterschrift Mitarbeiter/in _____

Ort, Datum _____ Unterschrift Arbeitgeber _____