Datenschutzerklärung für Getränkewart 2.0

Version 1.1 – Stand: 18.09.2026

1. Verantwortlicher und Kontakt

Verantwortlich für die Verarbeitung personenbezogener Daten, soweit die sparse creations GmbH selbst über Zwecke und Mittel der Verarbeitung entscheidet, ist:

sparse creations GmbH
Düsseldorfer Straße 60
33647 Bielefeld
Deutschland

Vertreten durch den Geschäftsführer Bernd Volkmer
E-Mail: info@getraenkewart.com

Diese Datenschutzerklärung gilt für die Software „Getränkewart 2.0” einschließlich der mobilen Anwendungen, der Webanwendung, der zentralen Tablet-Anwendung sowie der damit verbundenen Administrations- und Onlinedienste. Nachfolgend wird dieses Produkt als „Software” bezeichnet.

2. Datenschutzrechtliche Rollen

Die Software wird überwiegend innerhalb einer Organisation genutzt. Organisationen können insbesondere Vereine, Unternehmen, Behörden, Mannschaften, Personengruppen oder sonstige Zusammenschlüsse sein.

Soweit eine Organisation personenbezogene Daten ihrer Mitglieder, Mitarbeiter, Ehrenamtlichen, Gäste oder sonstigen Nutzer in der Software verwaltet und über die Zwecke dieser Verarbeitung entscheidet, ist grundsätzlich die jeweilige Organisation datenschutzrechtlich Verantwortlicher. Ist die Organisation keine rechtsfähige Person oder Personenvereinigung, ist Verantwortlicher der Administrator, der die Organisation in der Software eingerichtet hat oder für sie handelt. Die sparse creations GmbH verarbeitet diese Daten im Auftrag der Organisation auf Grundlage eines Auftragsverarbeitungsvertrags.

Die sparse creations GmbH ist dagegen selbst Verantwortlicher, soweit sie personenbezogene Daten für eigene Zwecke verarbeitet. Dies betrifft insbesondere:

- die Anlage und technische Verwaltung persönlicher Benutzerkonten,
- die Authentifizierung und IT-Sicherheit,
- die Verwaltung des Vertrags- und Abonnementverhältnisses,
- die Dokumentation der Bestätigung rechtlicher Dokumente,
- die technische Bereitstellung, Fehlerdiagnose und Missbrauchsprävention,
- die Bearbeitung von Support- und Kontaktanfragen,
- die Erfüllung eigener gesetzlicher Pflichten.

Für organisationsbezogene Verarbeitungen informiert die jeweilige Organisation die betroffenen Personen über ihre eigenen Zwecke, Rechtsgrundlagen und Aufbewahrungsfristen. Anfragen zu organisationsbezogenen Mitglieds-, Buchungs-, Konto- oder Abrechnungsdaten sollten daher grundsätzlich zunächst an die jeweilige Organisation gerichtet werden. Wir unterstützen die Organisation bei der Bearbeitung solcher Anfragen.

3. Allgemeine Hinweise, Rechtsgrundlagen und Datenquellen

Wir verarbeiten personenbezogene Daten nur, soweit dies für die Bereitstellung und Nutzung der Software, für die Erfüllung vertraglicher Pflichten, für die technische Sicherheit, für Support und Administration oder zur Erfüllung gesetzlicher Pflichten erforderlich ist.

Soweit wir selbst Verantwortlicher sind, erfolgt die Verarbeitung insbesondere auf folgenden Rechtsgrundlagen:

- Art. 6 Abs. 1 lit. b DSGVO, soweit die Verarbeitung zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist,
- Art. 6 Abs. 1 lit. a DSGVO, soweit eine Einwilligung erteilt wurde,
- Art. 6 Abs. 1 lit. c DSGVO, soweit wir einer rechtlichen Verpflichtung unterliegen,
- Art. 6 Abs. 1 lit. f DSGVO, soweit die Verarbeitung zur Wahrung unserer berechtigten Interessen erforderlich ist und keine überwiegenden Interessen oder Rechte der betroffenen Person entgegenstehen.

Unsere berechtigten Interessen liegen insbesondere im sicheren, stabilen und wirtschaftlichen Betrieb der Software, in der Fehleranalyse, der Missbrauchsprävention, der Bearbeitung von Anfragen sowie der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Soweit die jeweilige Organisation Verantwortlicher ist, bestimmt sie die anwendbare Rechtsgrundlage. Diese kann sich insbesondere aus einem Vertragsverhältnis, einer rechtlichen Verpflichtung, einer Einwilligung oder einem berechtigten Interesse der Organisation ergeben.

Personenbezogene Daten erhalten wir insbesondere:

- unmittelbar von den Nutzern,
- von Administratoren oder sonstigen berechtigten Personen der jeweiligen Organisation,
- durch die Nutzung der Software,
- vom verwendeten Endgerät,
- von App-Store-Betreibern und RevenueCat im Zusammenhang mit Abonnements,
- von Stripe bei Einrichtung oder Nutzung der optionalen Zahlungsfunktion,
- von technischen Dienstleistern, soweit dies für die jeweilige Funktion erforderlich ist.

Pflichtangaben sind als solche erkennbar. Ohne die für Registrierung, Authentifizierung oder Zuordnung erforderlichen Daten kann ein persönliches Benutzerkonto oder eine bestimmte Funktion gegebenenfalls nicht bereitgestellt werden. Freiwillige Angaben können grundsätzlich weggelassen oder später gelöscht werden, soweit keine anderen Gründe entgegenstehen.

Die planmäßige Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist nicht vorgesehen. Nutzer und Organisationen sollen insbesondere keine Gesundheitsdaten, Angaben zur ethnischen Herkunft, politischen Meinung, Religion, Gewerkschaftszugehörigkeit, sexuellen Orientierung oder vergleichbare besonders geschützte

Daten in Freitextfelder, Nachrichten, Profilbilder oder sonstige Inhalte einstellen, sofern dies nicht zuvor ausdrücklich datenschutzrechtlich abgesichert wurde.

4. Registrierung, Authentifizierung und Benutzerkonto

Bei der Registrierung und Nutzung eines persönlichen Benutzerkontos können insbesondere folgende Daten verarbeitet werden:

- Vorname und Nachname,
- E-Mail-Adresse,
- technische Benutzerkennung,
- Passwort in technisch gesicherter und durch den Authentifizierungsdienst verwalteter Form,
- E-Mail-Bestätigungsstatus,
- Zeitpunkte der Kontoerstellung und Anmeldung,
- Kontostatus und Sitzungsinformationen,
- Zuordnung zu einer oder mehreren Organisationen,
- optionale Profildaten, insbesondere Geburtsdatum oder Profilbild,
- Einstellungen und Sprach- oder Anzeigepräferenzen.

Die Verarbeitung dient der Anlage und Verwaltung des Benutzerkontos, der Authentifizierung, der Zuordnung zu Organisationen, der Bereitstellung geschützter Funktionen und der Sicherung des Zugangs.

Passwörter werden uns nicht im Klartext angezeigt. Für Registrierung, E-Mail-Bestätigung und Passwortzurücksetzung können systemseitige E-Mails durch Firebase Authentication versandt werden.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO. Sicherheits- und Protokolldaten verarbeiten wir ergänzend auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO.

5. Organisations-, Rollen- und Administrationsdaten

Zur Abbildung einer Organisation und ihrer internen Strukturen können insbesondere folgende Daten verarbeitet werden:

- Name und Kennung der Organisation,
- Mitglieds-, Mitarbeiter- oder Gaststatus,
- Rollen und Berechtigungen,
- Administratorenstatus,
- Zuordnung zu Gruppen, Abteilungen, Konten oder Gemeinschaftskonten,
- Einladungs-, Freischaltungs- und Bestätigungsstatus,
- organisatorische Einstellungen und Konfigurationen,
- administrative Änderungen und Zeitstempel.

Administratoren können Nutzer aufnehmen, bestätigen, sperren oder entfernen, Rollen vergeben und organisatorische Einstellungen verwalten. Die Sichtbarkeit und Bearbeitbarkeit der Daten richtet sich nach den innerhalb der Organisation vergebenen Berechtigungen.

Bei der Bestätigung rechtlicher Dokumente können insbesondere Benutzer- oder Administrator-ID, Organisation, Zeitpunkt, Dokumentart und Dokumentversion gespeichert werden. Dies betrifft je nach Rolle insbesondere die AGB, die Datenschutzerklärung und den Auftragsverarbeitungsvertrag.

Löst ein Administrator ein kostenpflichtiges Abonnement aus, speichern wir zusätzlich die Bestätigung, dass er berechtigt ist, für die ausgewählte Organisation beziehungsweise Gruppe zu handeln. Dabei können insbesondere Organisation, Administrator, Zeitpunkt, Textversion der Bestätigung, ausgewähltes Produkt beziehungsweise Abonnement und Plattform dokumentiert werden.

Soweit diese Daten der Verwaltung des eigenen Vertragsverhältnisses und dem Nachweis von Erklärungen dienen, ist die sparse creations GmbH selbst Verantwortlicher. Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b, lit. c und lit. f DSGVO.

6. Produkte, Verzehrsbuchungen, Konten und Abrechnungen

Im Rahmen der organisationsinternen Nutzung können insbesondere folgende Daten verarbeitet werden:

- Produkte, Preise und Verfügbarkeiten,
- gebuchte Produkte und Mengen,
- Buchungsdatum und Buchungszeit,
- buchender und betroffener Nutzer,
- verwendetes persönliches oder gemeinschaftliches Konto,
- Buchungsart und Buchungsstatus,
- Stornierungen und Korrekturen,
- persönlicher Kontostand,
- Einzahlungen, Überweisungen, Gutschriften und Belastungen,
- Umlagen,
- offene und ausgeglichene Beträge,
- Verwendungszwecke und interne Bemerkungen,
- Abrechnungszeiträume,
- Export- und Auswertungsdaten,
- gegebenenfalls das verwendete zentrale Tablet.

Die Verarbeitung dient der organisationsinternen Erfassung und Abrechnung von Produktverbräuchen und sonstigen Buchungen. Die jeweilige Organisation entscheidet über Produkte, Preise, Konten, Buchungsregeln, Aufbewahrungsfristen und Zugriffsberechtigungen.

Persönliche Konten, Gemeinschaftskonten, „Deckel” und Kontostände innerhalb der Software sind technische Aufzeichnungen organisationsinterner Vorgänge. Sie sind keine Bank- oder Zahlungskonten.

Bei der manuellen Erfassung einer Einzahlung werden die zugehörigen Buchungsangaben in der Software gespeichert. Für die optionale Zahlungsfunktion über Stripe gelten ergänzend die folgenden Hinweise.

6.1 Optionale Zahlungen über Stripe

Stripe ist eine optionale Zahlungsfunktion. Die Nutzung von Getränkewart 2.0 setzt keine Nutzung von Stripe voraus. Eine Organisation kann diese Funktion nach Freischaltung und Einrichtung eines verbundenen Stripe-Kontos anbieten. Nutzer entscheiden bei einer Einzahlung, ob sie diesen Zahlungsweg wählen. Ohne Einrichtung oder Nutzung der Stripe-Funktion übermitteln wir im Rahmen dieser Integration keine Daten an Stripe.

Wenn ein Administrator die Einrichtung startet, legen wir ein verbundenes Stripe-Konto an und übermitteln die Organisationskennung zur Zuordnung. Die weiteren Angaben zur Organisation, zu ihren vertretungsberechtigten Personen, zur Identitätsprüfung und zum Auszahlungskonto werden im Einrichtungsprozess von Stripe erhoben. In Getränkewart speichern wir die Stripe-Kontokennung und den Einrichtungsstatus.

Wenn ein Nutzer eine Stripe-Zahlung startet, übermitteln wir insbesondere seine E-Mail-Adresse, Zahlungsbetrag, Währung, Gebührenbetrag und die Stripe-Kontokennung der empfangenden Organisation an Stripe. Zahlungsdaten werden auf der von Stripe bereitgestellten Zahlungsseite eingegeben. Dort kann Stripe auch technische Daten wie die IP-Adresse und Geräteinformationen verarbeiten. Vollständige Kartennummern und Kartenprüfnummern werden nicht in Getränkewart gespeichert.

Zur Zuordnung und Verbuchung speichern wir insbesondere Benutzer- und Organisationskennung, E-Mail-Adresse, Beträge, Gebühren, Währung, Stripe-Konto- und Zahlungsvorgangskennung sowie Zeitpunkte und Verarbeitungsstatus. Stripe meldet uns den Zahlungsstatus zurück; nach einer bestätigten Zahlung wird die Einzahlung dem internen Konto zugeordnet. Die Verarbeitung dient der Einrichtung, Durchführung, Zuordnung und Dokumentation der gewählten Zahlungsfunktion sowie der Vermeidung fehlerhafter oder mehrfacher Verbuchungen.

Soweit wir für diese Verarbeitung selbst verantwortlich sind, erfolgt sie auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO zur Erbringung der angeforderten Zahlungsintegration, von Art. 6 Abs. 1 lit. f DSGVO für die sichere und nachvollziehbare Abwicklung sowie von Art. 6 Abs. 1 lit. c DSGVO, soweit gesetzliche Aufbewahrungspflichten bestehen. Für Verarbeitungen im Auftrag der Organisation gelten die in Abschnitt 2 beschriebenen Rollen. Die Aufbewahrung richtet sich nach Abschnitt 18.

Stripe verarbeitet Daten je nach Tätigkeit als Auftragsverarbeiter oder in eigener Verantwortung, etwa zur Erfüllung gesetzlicher Prüfpflichten und zur Betrugsprävention. Dabei kann es auch zu Übermittlungen in Drittländer, insbesondere die USA, kommen. Die zuständigen Stripe-Gesellschaften, Verarbeitungszwecke, Aufbewahrungsregeln und verwendeten Übermittlungsgarantien, insbesondere Angemessenheitsbeschlüsse und Standardvertragsklauseln, sind in den Datenschutzhinweisen von Stripe und im Stripe Privacy Center erläutert. Ergänzend gilt Abschnitt 17.

7. Zentrale Tablets, PIN und NFC

Organisationen können zentrale Tablets einsetzen, über die Nutzer Buchungen auslösen. Zur Identifikation und Autorisierung können insbesondere verarbeitet werden:

- persönliche PIN,
- NFC-Kennung oder eine daraus abgeleitete technische Referenz,
- technische Tablet-Kennung,

- Organisations- und Benutzerzuordnung,
- Zeitpunkt und Ergebnis der Identifikation,
- mit der Identifikation verbundene Buchungen.

PIN und NFC dienen ausschließlich der technischen Zuordnung und Autorisierung. Eine biometrische Verarbeitung findet nicht statt.

Die Organisation entscheidet, ob PIN- oder NFC-Funktionen aktiviert werden, und ist für die korrekte Zuordnung, die Sperrung verlorener NFC-Tags und den Schutz zentraler Tablets verantwortlich.

8. Nachrichten und Push-Benachrichtigungen

Soweit die jeweilige Organisation Nachrichten- oder Mitteilungsfunktionen verwendet, können insbesondere Absender, Empfänger oder Empfängergruppen, Betreff, Inhalt, Erstellungs- und Versandzeitpunkt sowie Zustellstatus verarbeitet werden.

Für Push-Benachrichtigungen verarbeiten wir technische Push-Kennungen, insbesondere FCM- oder APNs-Token, sowie die für die Zustellung erforderlichen technischen Nachrichteninformationen. Push-Benachrichtigungen können zum Beispiel über Buchungen, Kontobewegungen, Nachrichten oder andere organisationsbezogene Ereignisse informieren.

Die Berechtigung für Push-Benachrichtigungen kann jederzeit in den Einstellungen des Endgeräts geändert oder widerrufen werden. Je nach Geräteeinstellung können Benachrichtigungsinhalte auf dem Sperrbildschirm sichtbar sein.

9. Profilbilder, Uploads und sonstige Inhalte

Soweit die Software Upload-Funktionen bereitstellt, verarbeiten wir hochgeladene Dateien und die zugehörigen technischen Metadaten, um sie zu speichern, anzuzeigen und einem Benutzer, einer Organisation, einer Nachricht oder einem sonstigen Datensatz zuzuordnen.

Dies kann insbesondere Profilbilder, Nachrichtenanhänge oder sonstige von Nutzern bereitgestellte Inhalte betreffen. Die jeweilige Organisation und die einstellenden Nutzer sind dafür verantwortlich, dass die erforderlichen Rechte und datenschutzrechtlichen Voraussetzungen vorliegen.

10. Abonnements, App-Stores und RevenueCat

Für die technische Verwaltung, Validierung, Synchronisierung, Zuordnung und Wiederherstellung von In-App-Abonnements verwenden wir RevenueCat, Inc.

Dabei können insbesondere folgende Daten verarbeitet werden:

- RevenueCat-App-User-ID oder eine vergleichbare technische Kennung,
- App- und Geräteinformationen,
- verwendete Plattform und Store,
- Produkt- oder Abonnementkennung,
- Kauf-, Verlängerungs-, Kündigungs- und Ablaufstatus,
- Start-, Verlängerungs- und Ablaufzeitpunkte,

- Apple-Beleginformationen oder Google-Purchase-Token,
- technische Transaktions- und Synchronisierungsdaten,
- Zuordnung des erworbenen Leistungsumfangs zur ausgewählten Organisation.

RevenueCat verarbeitet Endnutzerinformationen zur Bereitstellung seines Dienstes in unserem Auftrag. RevenueCat kann Daten in den USA verarbeiten.

Die eigentliche Zahlungsabwicklung erfolgt über den Apple App Store beziehungsweise Google Play. Zahlungsdaten wie Kreditkarten- oder Bankdaten erhalten wir grundsätzlich nicht. Apple und Google verarbeiten die bei ihnen anfallenden Konto-, Zahlungs- und Transaktionsdaten nach ihren eigenen Datenschutzbestimmungen und in eigener datenschutzrechtlicher Verantwortung.

Rechtsgrundlage für die Verarbeitung durch uns ist Art. 6 Abs. 1 lit. b DSGVO. Soweit die Verarbeitung dem Nachweis, der Betrugs- oder Missbrauchsprävention und der technischen Zuordnung dient, ist ergänzend Art. 6 Abs. 1 lit. f DSGVO einschlägig.

Weiterführende Informationen:

- RevenueCat Datenschutz: https://www.revenuecat.com/privacy/
- Apple Datenschutz: https://www.apple.com/legal/privacy/
- Google Datenschutz: https://policies.google.com/privacy

11. Kontaktaufnahme und Support

Wenn Sie mit uns Kontakt aufnehmen, beispielsweise per E-Mail oder über eine Supportfunktion, verarbeiten wir die von Ihnen übermittelten Daten zur Bearbeitung und Beantwortung der Anfrage.

Dies können insbesondere Name, E-Mail-Adresse, Organisation, Benutzerkennung, Inhalt der Anfrage, Anhänge, technische Diagnosedaten und der Bearbeitungsverlauf sein.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, soweit die Anfrage ein Vertragsverhältnis betrifft. Im Übrigen erfolgt die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Soweit gesetzliche Aufbewahrungspflichten bestehen, gilt ergänzend Art. 6 Abs. 1 lit. c DSGVO.

12. Firebase und technische Infrastruktur

Wir verwenden Dienste von Google Firebase und Google Cloud zur technischen Bereitstellung der Software. Je nach verwendeter Funktion umfasst dies insbesondere:

- Firebase Authentication für Registrierung, Anmeldung und Kontoverwaltung,
- Cloud Firestore für die Speicherung appbezogener Daten,
- Cloud Functions für serverseitige Logik und automatisierte Prozesse,
- Firebase Storage für Dateien und Medien,
- Firebase Cloud Messaging für Push-Benachrichtigungen,
- Firebase Crashlytics für Fehler- und Absturzdiagnose,
- Firebase Analytics für Nutzungsanalysen, soweit diese Funktion in der jeweiligen App-Version aktiviert ist.

Dabei können Benutzer-, Organisations-, Buchungs-, Kommunikations-, Authentifizierungs-, Geräte-, Push- und Protokolldaten verarbeitet werden, soweit dies für die jeweilige Funktion

erforderlich ist.

Vertragspartner ist Google Cloud EMEA Limited beziehungsweise die jeweils vertragsführende Google-Gesellschaft. Die Datenverarbeitung kann in der Europäischen Union und an weiteren rechtlich abgesicherten Standorten erfolgen.

Weiterführende Informationen:

- Firebase Privacy and Security: https://firebase.google.com/support/privacy/
- Google Datenschutz: https://policies.google.com/privacy

13. Fehlerdiagnose, Nutzungsanalyse und App-Sicherheit

Firebase Crashlytics wird eingesetzt, um Fehler und Abstürze zu erkennen, zu analysieren und die Stabilität der Software zu verbessern. Dabei können insbesondere Geräteinformationen, Betriebssystem, App-Version, Zeitpunkt und technische Umstände eines Fehlers, Stack-Traces, technische Kennungen und gegebenenfalls eine technische Benutzerreferenz verarbeitet werden.

Firebase Analytics kann, soweit in der jeweiligen App-Version aktiviert, technische Nutzungs- und Ereignisdaten verarbeiten. Dazu können insbesondere App-Instanzkennungen, Geräte- und Appinformationen, aufgerufene Bildschirmbereiche, technische Ereignisse und Zeitpunkte der Nutzung gehören.

Die Daten werden nicht für personalisierte Werbung oder appübergreifendes Werbetracking verwendet. Getränkewart 2.0 enthält keine Werbeanzeigen und verwendet kein Google AdMob.

Die Verarbeitung dient unserem berechtigten Interesse an einem sicheren, stabilen und nutzerfreundlichen App-Angebot und erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Soweit für das Speichern oder Auslesen von Informationen auf dem Endgerät oder für eine Analyse eine Einwilligung gesetzlich erforderlich ist, erfolgt die Verarbeitung nur nach einer entsprechenden Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

14. App-Berechtigungen und lokale Speicherung

Je nach Endgerät und genutzter Funktion kann die Software Berechtigungen anfragen, insbesondere für:

- Push-Benachrichtigungen,
- NFC,
- Zugriff auf Fotos, Kamera oder Dateien, soweit Uploads angeboten werden.

Eine Berechtigung wird nur für die jeweils beschriebene Funktion verwendet. Sie kann in den Einstellungen des Endgeräts geändert oder entzogen werden. Ohne eine Berechtigung kann die betreffende Funktion eingeschränkt sein.

Auf dem Endgerät können technisch erforderliche Informationen lokal gespeichert werden, insbesondere Anmeldestatus, Sitzungstoken, Einstellungen, bereits bestätigte Dokumentversionen, Zwischenspeicher und technische Konfigurationsdaten. Soweit hierfür nach den Vorschriften über den Zugriff auf Endeinrichtungen eine Einwilligung erforderlich ist, wird diese eingeholt. Technisch unbedingt erforderliche Speicherungen erfolgen zur Bereitstellung der ausdrücklich gewünschten App-Funktionen.

15. Exporte, Teilen-Funktionen und externe Links

Die Software kann Datenexporte und systemseitige Teilen-Funktionen bereitstellen. Wenn ein Nutzer einen Export erstellt oder Daten an eine andere App, einen Cloud-Speicher, einen E-Mail-Dienst oder einen sonstigen Empfänger übermittelt, kann dort eine eigenständige Datenverarbeitung stattfinden.

Für die Auswahl des Empfängers, die weitere Verarbeitung exportierter Daten und deren Schutz außerhalb der Software ist grundsätzlich der ausführende Nutzer beziehungsweise die jeweilige Organisation verantwortlich.

Externe Links führen zu Angeboten anderer Anbieter. Für deren Datenverarbeitung gelten die jeweiligen Datenschutzbestimmungen.

16. Empfänger personenbezogener Daten

Personenbezogene Daten werden nur offengelegt, soweit dies für die beschriebenen Zwecke erforderlich ist, eine rechtliche Verpflichtung besteht, eine Einwilligung vorliegt oder berechtigte Interessen dies erlauben.

Empfänger können insbesondere sein:

- berechtigte Administratoren und Nutzer innerhalb der jeweiligen Organisation,
- Google beziehungsweise Google Cloud für Hosting, Authentifizierung, Datenbank, Push, Analyse und Fehlerdiagnose,
- Apple für Push-Zustellung und App-Store-Dienste,
- Google für Google-Play-Dienste,
- RevenueCat für die technische Verwaltung von Abonnements,
- Stripe bei Einrichtung oder Nutzung der optionalen Zahlungsfunktion,
- technische Support- und Infrastruktur-Dienstleister,
- Rechts-, Steuer- oder sonstige Berater, soweit dies erforderlich ist,
- Behörden oder Gerichte, soweit eine gesetzliche Verpflichtung besteht.

Dienstleister werden, soweit erforderlich, als Auftragsverarbeiter vertraglich verpflichtet. Soweit ein Empfänger selbst über Zwecke und Mittel entscheidet, verarbeitet er die Daten in eigener Verantwortung.

17. Datenverarbeitung in Drittländern

Bei der Nutzung einzelner Dienstleister kann es zu einer Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums kommen, insbesondere in den USA.

Eine Übermittlung erfolgt nur, wenn die gesetzlichen Voraussetzungen erfüllt sind. Hierzu können insbesondere ein Angemessenheitsbeschluss der Europäischen Kommission, eine Zertifizierung des Empfängers nach dem EU-U.S. Data Privacy Framework, Standardvertragsklauseln der Europäischen Kommission oder andere geeignete Garantien gehören.

Soweit keine geeigneten Garantien bestehen, erfolgt eine Übermittlung nur unter den besonderen gesetzlichen Voraussetzungen, insbesondere aufgrund einer ausdrücklichen Einwilligung oder wenn die Übermittlung zur Vertragserfüllung erforderlich ist.

18. Speicherdauer und Löschung

Wir speichern personenbezogene Daten nur so lange, wie dies für die jeweiligen Zwecke erforderlich ist. Anschließend werden die Daten gelöscht, anonymisiert oder in ihrer Verarbeitung eingeschränkt, sofern gesetzliche Aufbewahrungspflichten, offene Vorgänge oder berechtigte Gründe für eine weitere Speicherung bestehen.

Es gelten insbesondere folgende Grundsätze:

- Konto- und Authentifizierungsdaten werden grundsätzlich für die Dauer des persönlichen Nutzungsverhältnisses gespeichert.
- Bei Löschung eines persönlichen Benutzerkontos werden die persönliche E-Mail-Adresse und die zugehörigen Authentifizierungsdaten grundsätzlich entfernt, soweit keine entgegenstehenden Gründe bestehen.
- Organisationsbezogene Buchungs-, Konto- und Abrechnungsdaten können trotz Löschung des persönlichen Kontos erhalten bleiben, wenn die Organisation diese für offene Vorgänge, Nachweise oder gesetzliche Aufbewahrungspflichten benötigt.
- Push-Token werden gespeichert, solange sie für die Zustellung benötigt werden oder bis sie ungültig werden beziehungsweise gelöscht werden.
- Vertrags-, Abonnement-, Rechnungs- und Bestätigungsdaten werden entsprechend den gesetzlichen Aufbewahrungsfristen und Verjährungszeiträumen gespeichert.
- Supportdaten werden so lange gespeichert, wie dies für die Bearbeitung, Dokumentation und mögliche Anschlussfragen erforderlich ist.
- Analyse- und Fehlerdaten werden entsprechend der jeweiligen Konfiguration und den technisch vorgesehenen Löschfristen gespeichert und anschließend gelöscht oder anonymisiert.

Nach Beendigung eines Organisationsvertrags kann die Organisation einen technisch vorgesehenen Datenexport grundsätzlich innerhalb von 30 Tagen anfordern. Produktivdaten werden grundsätzlich innerhalb von 90 Tagen nach Vertragsende gelöscht, sofern keine abweichende Weisung, gesetzliche Aufbewahrungspflicht oder berechtigte technische Notwendigkeit entgegensteht. Daten in Sicherungskopien werden im Rahmen der regulären Überschreib- und Löschzyklen gelöscht. Für die Point-in-Time-Recovery beträgt die Aufbewahrungsdauer sieben Tage, für reguläre Sicherungskopien maximal 30 Tage.

19. Minderjährige Nutzer

Die Software kann auch von Minderjährigen innerhalb einer Organisation genutzt werden, soweit dies gesetzlich zulässig ist und die Organisation beziehungsweise die gesetzlichen Vertreter die erforderlichen Voraussetzungen sicherstellen.

Soweit eine Verarbeitung auf einer datenschutzrechtlichen Einwilligung beruht und die betroffene Person die gesetzlich erforderliche Altersgrenze nicht erreicht hat, ist die Zustimmung oder Genehmigung der gesetzlichen Vertreter erforderlich.

20. Automatisierte Entscheidungen

Eine ausschließlich automatisierte Entscheidungsfindung einschließlich Profiling, die gegenüber einer Person rechtliche Wirkung entfaltet oder sie in ähnlich erheblicher Weise beeinträchtigt, findet nicht statt.

21. Rechte betroffener Personen

Betroffenen Personen stehen nach Maßgabe der gesetzlichen Voraussetzungen insbesondere folgende Rechte zu:

- Recht auf Auskunft über die verarbeiteten personenbezogenen Daten,
- Recht auf Berichtigung unrichtiger oder unvollständiger Daten,
- Recht auf Löschung,
- Recht auf Einschränkung der Verarbeitung,
- Recht auf Datenübertragbarkeit,
- Recht auf Widerspruch gegen bestimmte Verarbeitungen,
- Recht auf Widerruf einer erteilten Einwilligung mit Wirkung für die Zukunft,
- Recht auf Beschwerde bei einer Datenschutzaufsichtsbehörde.

Zur Ausübung von Rechten können Sie sich an info@getraenkewart.com wenden.

Betrifft die Anfrage Daten, die von uns ausschließlich im Auftrag einer Organisation verarbeitet werden, ist die jeweilige Organisation für die rechtliche Prüfung und Beantwortung verantwortlich. Wir leiten die Anfrage gegebenenfalls an die Organisation weiter und unterstützen sie bei der Bearbeitung.

Zur Vermeidung unbefugter Offenlegungen können wir oder die Organisation einen angemessenen Nachweis der Identität verlangen.

22. Widerspruchsrecht

Soweit personenbezogene Daten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO verarbeitet werden, besteht aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, ein Recht auf Widerspruch gegen diese Verarbeitung.

Wir verarbeiten die betreffenden Daten nach einem wirksamen Widerspruch nicht weiter, es sei denn, es bestehen zwingende schutzwürdige Gründe für die Verarbeitung, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

23. Beschwerderecht

Betroffene Personen haben das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren. Zuständig für die sparse creations GmbH ist grundsätzlich:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
https://www.ldi.nrw.de

Das Beschwerderecht kann auch bei einer anderen zuständigen Aufsichtsbehörde ausgeübt werden.

24. Änderungen dieser Datenschutzerklärung

Wir passen diese Datenschutzerklärung an, wenn sich rechtliche, technische oder organisatorische Rahmenbedingungen ändern oder neue Funktionen eingeführt werden.

Bei wesentlichen Änderungen informieren wir die Nutzer durch einen Hinweis beim nächsten Login in der App auf einem beliebigen Gerät, bei dem die Kenntnisnahme erneut abgefragt wird. Es gilt die jeweils in der Software veröffentlichte Fassung.