# Auftragsverarbeitungsvertrag

## zur Nutzung der Software „Getränkewart 2.0”

Version 1.0

Stand: 18. September 2026

zwischen

dem Kunden gemäß dem zwischen den Parteien geschlossenen Nutzungs-, Abonnement- oder Softwaremietvertrag über die Software „Getränkewart 2.0”

– nachfolgend „Verantwortlicher” genannt –

und

sparse creations GmbH
Düsseldorfer Straße 60
33647 Bielefeld
Deutschland

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

– nachfolgend „Auftragsverarbeiter” genannt –

gemeinsam auch „Parteien”.

## 1. Gegenstand und Anwendungsbereich

1. Dieser Auftragsverarbeitungsvertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen gemäß Art. 28 der Datenschutz-Grundverordnung.

2. Der Vertrag gilt für die Bereitstellung, den Betrieb, die Wartung und den Support der Software „Getränkewart 2.0” (nachfolgend „Software”), einschließlich der mobilen Anwendungen, zentraler Tablet-Anwendungen, administrativer Funktionen und gegebenenfalls ergänzender Webdienste.

3. Der Verantwortliche ist die Organisation, die die Software für eigene organisatorische Zwecke einsetzt. Ist die Organisation keine rechtsfähige Person oder Personenvereinigung, ist Verantwortlicher der Administrator, der die Organisation in der Software eingerichtet hat oder für sie handelt.

4. Dieser Vertrag ergänzt den zwischen den Parteien bestehenden Hauptvertrag. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die datenschutzrechtlichen Regelungen dieses Vertrags vor.

## 2. Dauer der Verarbeitung

1. Die Verarbeitung beginnt mit der Bereitstellung oder Freischaltung der Organisation in der Software.

2. Sie erfolgt für die Dauer des Hauptvertrags beziehungsweise für die Dauer der Nutzung der Software durch den Verantwortlichen.

3. Nach Beendigung des Hauptvertrags werden die personenbezogenen Daten nach Maßgabe von Ziffer 12 gelöscht oder auf Weisung des Verantwortlichen zurückgegeben, soweit keine gesetzlichen Aufbewahrungspflichten oder sonstigen rechtlichen Gründe entgegenstehen.

## 3. Art und Zweck der Verarbeitung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich, soweit dies zur Bereitstellung und zum Betrieb der Software sowie zur Erfüllung dokumentierter Weisungen des Verantwortlichen erforderlich ist.

2. Die Verarbeitung kann insbesondere folgende Vorgänge umfassen:

- Erheben und Erfassen,
- Speichern,
- Ordnen und Organisieren,
- Ändern und Berichtigen,
- Auslesen und Abfragen,
- Bereitstellen und Anzeigen,
- Zuordnen und Verknüpfen,
- Übermitteln und Versenden,
- Auswerten,
- Einschränken,
- Exportieren,
- Löschen und Vernichten.

3. Die Verarbeitung erfolgt insbesondere zu folgenden Zwecken:

- Einrichtung und Verwaltung einer Organisation in der Software,
- Registrierung und Authentifizierung von Benutzern,
- Zuordnung von Benutzern zu einer Organisation,
- Verwaltung von Mitgliedern, Mitarbeitern, Rollen und Berechtigungen,
- Bestätigung oder Freischaltung neuer Benutzer durch Administratoren,
- Verwaltung von Produkten, Preisen und Verfügbarkeiten,
- Erfassung von Verzehrs- und sonstigen Produktbuchungen,
- Führung persönlicher und gemeinschaftlicher Konten oder „Deckel”,
- Erfassung und Zuordnung von Einzahlungen, Überweisungen, Korrekturen und sonstigen Kontobewegungen,
- Erstellung und Verwaltung von Umlagen,
- Darstellung von Kontoständen und Buchungshistorien,
- Erstellung von Abrechnungen, Übersichten und Auswertungen,
- Identifikation und Autorisierung an zentralen Tablets mittels PIN oder NFC-Kennung,

- Versand und Anzeige organisationsinterner Nachrichten und Benachrichtigungen,
- Versand technischer Push-Mitteilungen,
- Administration zentraler Tablets,
- technischer Betrieb, Datensicherung und Wiederherstellung,
- Fehleranalyse, Systemsicherheit und Missbrauchsprävention,
- Bearbeitung von Supportanfragen,
- Erfüllung von Lösch-, Berichtigungs-, Auskunfts- und sonstigen Weisungen des Verantwortlichen.

4. Eine Verarbeitung für eigene, mit diesen Zwecken nicht vereinbare Zwecke des Auftragsverarbeiters findet nicht statt. Verarbeitungen, bei denen der Auftragsverarbeiter selbst über Zwecke und Mittel entscheidet, insbesondere die Verwaltung des Vertragsverhältnisses und die Abrechnung eigener Leistungen gegenüber dem Verantwortlichen, sind nicht Gegenstand dieses Auftragsverarbeitungsvertrags.

## 4. Kategorien betroffener Personen

Von der Verarbeitung können insbesondere folgende Personen betroffen sein:

- Mitglieder und sonstige Angehörige der Organisation,
- Mitarbeiter und Beschäftigte,
- ehrenamtlich Tätige,
- Administratoren und sonstige Funktionsträger,
- Gäste und vorübergehend angelegte Benutzer,
- Benutzer zentraler Tablets,
- ehemalige Mitglieder oder Mitarbeiter, soweit Daten aufgrund offener Vorgänge oder Aufbewahrungspflichten weiterhin verarbeitet werden,
- Ansprechpartner des Verantwortlichen,
- sonstige Personen, für die der Verantwortliche ein Benutzer- oder Abrechnungskonto anlegt.

## 5. Kategorien personenbezogener Daten

Abhängig von der Konfiguration und Nutzung der Software können insbesondere folgende Daten verarbeitet werden:

### 5.1 Stamm- und Kontaktdaten

- Vorname,
- Nachname,
- gegebenenfalls weitere Namensbestandteile oder Titel,
- E-Mail-Adresse,
- Benutzerkennung,
- Organisationszugehörigkeit,
- Einladungscode beziehungsweise Zuordnungscode,

- gegebenenfalls Geburtsdatum,
- Profilbild.

### 5.2 Organisations-, Rollen- und Berechtigungsdaten

- Name und Kennung der Organisation,
- Mitglieds- oder Beschäftigtenstatus,
- Benutzerrolle,
- Administratorenstatus,
- Berechtigungen,
- Freischaltungs- und Bestätigungsstatus,
- Zuordnung zu Gruppen, Konten oder Abteilungen.

### 5.3 Authentifizierungs- und Identifikationsdaten

- technische Benutzer-ID,
- E-Mail-Bestätigungsstatus,
- Passwort in technisch gesicherter beziehungsweise durch den eingesetzten Authentifizierungsdienst verwalteter Form,
- PIN für die Nutzung zentraler Tablets,
- NFC-Kennung oder eine daraus abgeleitete technische Referenz,
- Sitzungs- und Anmeldeinformationen.

Passwörter werden dem Auftragsverarbeiter nicht im Klartext angezeigt oder zur freien Verwendung bereitgestellt.

### 5.4 Verzehrs-, Produkt- und Buchungsdaten

- gebuchte Produkte,
- Produktmenge,
- Produktpreis,
- Buchungsdatum und Buchungszeit,
- buchender Benutzer,
- betroffener Benutzer,
- verwendetes Konto oder Gemeinschaftskonto,
- Buchungsart,
- Stornierungen und Korrekturen,
- Buchungsstatus,
- gegebenenfalls verwendetes zentrales Tablet.

### 5.5 Konto-, Zahlungs- und Abrechnungsdaten

- persönlicher Kontostand,

- Einzahlungen,
- Überweisungen,
- Gutschriften,
- Belastungen,
- Umlagen,
- offene und ausgeglichene Beträge,
- Zahlungs- oder Buchungsstatus,
- Verwendungszwecke und interne Bemerkungen,
- Abrechnungszeiträume,
- buchhalterische Zuordnungen,
- Export- und Auswertungsdaten.

Bankkontodaten, SEPA-Mandatsdaten oder Kreditkartendaten sind nur dann Gegenstand der Verarbeitung, wenn eine entsprechende Funktion ausdrücklich bereitgestellt, vom Verantwortlichen aktiviert und in einer ergänzenden Vereinbarung beschrieben wird.

### 5.6 Kommunikationsdaten

- organisationsinterne Nachrichten,
- Betreff und Inhalt von Mitteilungen,
- Absender,
- Empfänger oder Empfängergruppen,
- Versand- und Erstellungszeitpunkt,
- Zustellstatus,
- Push-Benachrichtigungskennungen.

### 5.7 Technische und Protokolldaten

- Geräte- und Appinformationen,
- Betriebssystem und Appversion,
- technische Benutzer- und Gerätekennungen,
- IP-Adresse, soweit sie technisch verarbeitet oder protokolliert wird,
- Zugriffszeitpunkte,
- Fehler- und Absturzinformationen,
- Sicherheits- und Auditprotokolle,
- administrative Änderungen,
- Support- und Diagnosedaten.

### 5.8 Besondere Kategorien personenbezogener Daten

Die planmäßige Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist nicht Gegenstand der Leistungen.

Der Verantwortliche verpflichtet sich, keine Gesundheitsdaten, Angaben zur ethnischen Herkunft, politischen Meinung, Religion, Gewerkschaftszugehörigkeit, sexuellen Orientierung oder vergleichbare besonders geschützte Daten in Freitextfelder, Nachrichten, Profilbilder oder sonstige Inhalte einzustellen, sofern dies nicht zuvor ausdrücklich mit dem Auftragsverarbeiter vereinbart und datenschutzrechtlich abgesichert wurde.

## 6. Weisungsgebundenheit

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Europäischen Union oder eines Mitgliedstaats zu einer anderweitigen Verarbeitung verpflichtet ist.

2. Weisungen werden insbesondere erteilt durch:

- die Auswahl und Konfiguration der Funktionen der Software,
- Handlungen berechtigter Administratoren,
- das Anlegen, Ändern, Sperren oder Löschen von Benutzern,
- die Vergabe von Rollen und Berechtigungen,
- die Erfassung und Korrektur von Buchungen,
- Mitteilungen per E-Mail oder über vereinbarte Supportkanäle.

3. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

4. Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtswidrig, informiert er den Verantwortlichen unverzüglich. Er ist berechtigt, die Ausführung der Weisung bis zu ihrer Bestätigung oder Änderung auszusetzen.

5. Weisungen, die über die vertraglich vereinbarten Leistungen hinausgehen, können gesondert vergütet werden. Dies gilt nicht, soweit die Unterstützung bereits gesetzlich geschuldet oder im Hauptvertrag enthalten ist.

## 7. Pflichten des Verantwortlichen

1. Der Verantwortliche entscheidet über Zwecke und wesentliche Mittel der Verarbeitung und bleibt für die Rechtmäßigkeit der Verarbeitung verantwortlich.

2. Der Verantwortliche ist insbesondere verpflichtet,

- eine geeignete Rechtsgrundlage für die Verarbeitung sicherzustellen,
- die betroffenen Personen ordnungsgemäß zu informieren,
- nur erforderliche und sachlich richtige Daten zu verarbeiten,
- angemessene Lösch- und Aufbewahrungsfristen festzulegen,
- Benutzerrollen und Berechtigungen sachgerecht zu vergeben,
- Administratorrechte auf vertrauenswürdige Personen zu beschränken,
- Zugangsdaten, PINs, NFC-Tags und zentrale Tablets vor unbefugtem Zugriff zu schützen,
- unberechtigte Benutzer unverzüglich zu sperren oder zu entfernen,
- die Zulässigkeit von Nachrichten, Bildern und Freitextinhalten sicherzustellen,
- Anfragen betroffener Personen zu prüfen und zu beantworten,

- gesetzliche Aufbewahrungspflichten für abrechnungsrelevante Daten zu beurteilen,
- den Auftragsverarbeiter über Änderungen der Weisungs- oder Ansprechpartner zu informieren.

3. Der Verantwortliche stellt sicher, dass seine Administratoren zur Abgabe von Weisungen und zum Abschluss beziehungsweise zur Annahme dieses Vertrags berechtigt sind.

## 8. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich insbesondere,

1. personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten;

2. sicherzustellen, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

3. die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen einzuhalten;

4. den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Betroffenenrechten zu unterstützen;

5. den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß Art. 32 bis 36 DSGVO zu unterstützen, soweit dies unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen möglich ist;

6. Datenschutzverletzungen nach Maßgabe von Ziffer 10 mitzuteilen;

7. die Einhaltung dieses Vertrags nach Maßgabe von Ziffer 11 nachzuweisen;

8. Daten nach Beendigung der Verarbeitung gemäß Ziffer 12 zu löschen oder zurückzugeben;

9. ein Verzeichnis der für den Verantwortlichen durchgeführten Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich erforderlich ist;

10. mit zuständigen Datenschutzaufsichtsbehörden zusammenzuarbeiten, soweit dies gesetzlich erforderlich ist.

## 9. Unterauftragsverarbeiter

1. Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen.

2. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt.

3. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern, indem er eine neue Version dieses Vertrags gemäß Ziffer 15 bereitstellt, die vor der Umsetzung der Änderung erneut angenommen werden muss.

4. Der Verantwortliche kann einer Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen nach der Information widersprechen.

5. Können die Parteien keine angemessene Lösung finden, kann jede Partei die von der Änderung betroffene Leistung oder, sofern eine Fortsetzung nicht zumutbar ist, den Hauptvertrag außerordentlich kündigen.

6. Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter durch einen Vertrag, der im Wesentlichen dieselben Datenschutzpflichten enthält, die in diesem Vertrag festgelegt sind.

7. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Erfüllung der Pflichten seiner Unterauftragsverarbeiter verantwortlich.

8. Soweit ein Unterauftragsverarbeiter personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums verarbeitet, stellt der Auftragsverarbeiter sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Hierzu können insbesondere ein Angemessenheitsbeschluss, das EU-U.S. Data Privacy Framework oder die Standardvertragsklauseln der Europäischen Kommission herangezogen werden.

## 10. Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, die Daten des Verantwortlichen betrifft.

2. Die Mitteilung enthält, soweit zu diesem Zeitpunkt verfügbar:

- eine Beschreibung der Art der Verletzung,
- die betroffenen Datenkategorien,
- die Kategorien und ungefähre Anzahl betroffener Personen,
- die ungefähre Anzahl betroffener Datensätze,
- die wahrscheinlichen Folgen der Verletzung,
- die ergriffenen oder vorgeschlagenen Gegenmaßnahmen,
- einen Ansprechpartner für Rückfragen.

3. Können nicht alle Informationen gleichzeitig bereitgestellt werden, werden sie schrittweise ohne unangemessene Verzögerung ergänzt.

4. Die Bewertung einer Melde- oder Benachrichtigungspflicht gegenüber einer Aufsichtsbehörde oder betroffenen Personen obliegt dem Verantwortlichen.

5. Der Auftragsverarbeiter unterstützt den Verantwortlichen im angemessenen Umfang bei der Untersuchung, Eindämmung, Dokumentation und Meldung des Vorfalls.

## 11. Nachweise und Kontrollen

1. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen.

2. Nachweise können insbesondere erbracht werden durch:

- eine aktuelle Beschreibung der technischen und organisatorischen Maßnahmen,
- geeignete Zertifikate oder Prüfberichte,
- dokumentierte Sicherheits- und Datenschutzprozesse,
- Auskünfte zu Unterauftragsverarbeitern,
- schriftliche Selbstauskünfte.

3. Der Verantwortliche ist berechtigt, nach vorheriger angemessener Ankündigung Kontrollen durchzuführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen zu lassen.

4. Kontrollen sind während der üblichen Geschäftszeiten durchzuführen und so zu gestalten, dass der Geschäftsbetrieb und die Sicherheit anderer Kunden nicht beeinträchtigt werden.

5. Vor-Ort-Prüfungen sind nur zulässig, soweit andere Nachweise nicht ausreichen oder konkrete Anhaltspunkte für einen erheblichen Verstoß bestehen.

6. Der Verantwortliche trägt die angemessenen Kosten einer von ihm veranlassten Prüfung, sofern die Prüfung keinen wesentlichen Verstoß des Auftragsverarbeiters ergibt.

7. Betriebs- und Geschäftsgeheimnisse, Sicherheitskonzepte sowie personenbezogene Daten anderer Kunden sind zu schützen.

## 12. Löschung und Rückgabe

1. Der Verantwortliche kann während der Vertragslaufzeit im Rahmen der bereitgestellten Funktionen Daten selbst berichtigen, sperren oder löschen.

2. Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter die im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie dem Verantwortlichen zurück, sofern der Verantwortliche dies vor der Löschung verlangt und die Rückgabe technisch möglich sowie vertraglich vorgesehen ist.

3. Der Verantwortliche muss einen gewünschten Datenexport spätestens innerhalb von 30 Tagen nach Vertragsende anfordern.

4. Produktivdaten werden grundsätzlich innerhalb von 90 Tagen nach Vertragsende gelöscht, sofern keine abweichende Weisung, gesetzliche Aufbewahrungspflicht oder berechtigte technische Notwendigkeit entgegensteht.

5. 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.

6. Soweit einzelne Daten wegen gesetzlicher Aufbewahrungspflichten nicht gelöscht werden dürfen, werden sie gesperrt und nur noch zu diesem Zweck verarbeitet.

7. Die Löschung eines individuellen Benutzerkontos kann von der Löschung der organisationsbezogenen Buchungs- und Abrechnungsdaten getrennt sein. Der Verantwortliche entscheidet, ob Buchungsdaten gelöscht, anonymisiert oder aufgrund gesetzlicher beziehungsweise organisatorischer Nachweispflichten weiter aufbewahrt werden müssen.

8. Die Löschung kann auf Verlangen des Verantwortlichen in geeigneter Form bestätigt werden.

## 13. Betroffenenrechte

1. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter und betrifft die Anfrage Daten, die im Auftrag des Verantwortlichen verarbeitet werden, leitet der Auftragsverarbeiter die Anfrage grundsätzlich an den Verantwortlichen weiter.

2. Der Auftragsverarbeiter beantwortet solche Anfragen nicht eigenständig, sofern er nicht hierzu vom Verantwortlichen angewiesen oder gesetzlich verpflichtet ist.

3. Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit bei:

- Auskunft,
- Berichtigung,
- Löschung,
- Einschränkung der Verarbeitung,
- Datenübertragbarkeit,
- Widerspruch,
- Nachweis der Bearbeitung einer Anfrage.

4. Der Verantwortliche bleibt für die Prüfung der Identität der betroffenen Person, die rechtliche Bewertung und die fristgerechte Beantwortung verantwortlich.

## 14. Technische Identifikationsmittel und zentrale Tablets

1. Die Software kann die Identifikation an zentralen Tablets mittels persönlicher PIN oder NFC-Kennung ermöglichen.

2. Der Verantwortliche entscheidet, ob diese Funktionen aktiviert werden.

3. Der Verantwortliche ist verpflichtet,

- zentrale Tablets vor unbefugtem Zugriff zu schützen,
- den physischen Zugang angemessen zu beschränken,
- PINs und NFC-Tags nur berechtigten Personen zuzuordnen,
- verlorene oder kompromittierte NFC-Tags unverzüglich zu sperren oder neu zuzuordnen,
- Administratorzugänge nicht auf allgemein zugänglichen Geräten dauerhaft angemeldet zu lassen.

4. NFC-Kennungen werden ausschließlich zur technischen Zuordnung und Autorisierung verwendet. Eine biometrische Verarbeitung findet dadurch nicht statt.

## 15. Digitale Annahme und Nachweis

1. Dieser Vertrag wird ausschließlich elektronisch innerhalb der jeweiligen App angenommen.

2. Administratoren müssen den Vertrag beim Login in der jeweiligen App ausdrücklich bestätigen, sofern noch keine gültige Zustimmung zur aktuellen Vertragsversion vorliegt. Ohne Bestätigung ist die weitere Nutzung der Adminfunktionen nicht möglich.

3. Die Zustimmung erfolgt durch Aktivierung einer Checkbox durch eine Person, die erklärt, im Namen des Verantwortlichen zu handeln und hierzu berechtigt zu sein.

4. Der Auftragsverarbeiter protokolliert die Zustimmung mit Organisation, Benutzer beziehungsweise Administrator, Zeitpunkt und Vertragsversion und stellt die Zustimmungshistorie im Administrationsbereich bereit.

5. Bei neuen Vertragsversionen kann der Auftragsverarbeiter eine erneute Zustimmung verlangen und die Nutzung der jeweiligen App bis zur Zustimmung aussetzen.

## 16. Haftung

Für die Haftung gelten Art. 82 DSGVO sowie die Haftungsregelungen des Hauptvertrags.

Eine Haftungsbeschränkung gilt nicht, soweit sie nach zwingendem Datenschutzrecht unzulässig ist.

## 17. Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrags bedürfen mindestens der Textform. Dies gilt auch für eine Änderung dieses Formerfordernisses.

2. Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

3. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts.

4. Gerichtsstand ist, soweit gesetzlich zulässig, Bielefeld.

5. Die Anlagen sind Bestandteil dieses Vertrags.

## Anlage 1

### Beschreibung der Auftragsverarbeitung

### Gegenstand

Bereitstellung, Betrieb, Wartung und Support der Software „Getränkewart 2.0” zur organisationsinternen Verwaltung von Benutzern, Produkten, Verzehr, Konten, Einzahlungen, Umlagen, Abrechnungen, Nachrichten und zentralen Tablets.

### Dauer

Dauer des Hauptvertrags zuzüglich der in Ziffer 12 geregelten Rückgabe-, Lösch- und Sicherungsfristen.

### Art der Verarbeitung

Erheben, Erfassen, Speichern, Ordnen, Ändern, Auslesen, Abfragen, Anzeigen, Zuordnen, Übermitteln, Auswerten, Exportieren, Einschränken und Löschen.

### Zweck

Organisationsinterne Verwaltung und Abrechnung von Produktverbräuchen und sonstigen Buchungen sowie Benutzer-, Rollen-, Kommunikations- und Administrationsfunktionen.

### Kategorien betroffener Personen

Mitglieder, Mitarbeiter, Ehrenamtliche, Administratoren, Gäste, Ansprechpartner und sonstige Benutzer der Organisation.

### Datenkategorien

Stamm- und Kontaktdaten, Benutzer- und Rollendaten, Authentifizierungsdaten, PIN-/NFC-Zuordnungen, Profilinformationen, Verzehrs- und Buchungsdaten, Konto- und Abrechnungsdaten, Nachrichten, Push-Kennungen sowie technische Protokoll- und Supportdaten.

## Anlage 2

### Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen angemessene technische und organisatorische Maßnahmen.

### 1. Zutrittskontrolle

Maßnahmen zur Verhinderung des unbefugten physischen Zutritts zu Datenverarbeitungsanlagen, insbesondere:

- Nutzung professionell betriebener Rechenzentren,
- physische Sicherungsmaßnahmen der Hostinganbieter,
- beschränkter Zugang zu internen Arbeitsmitteln,
- Schutz dienstlicher Endgeräte.

### 2. Zugangskontrolle

Maßnahmen zur Verhinderung der unbefugten Nutzung von Datenverarbeitungssystemen:

- Benutzerkonten mit individueller Authentifizierung,
- Passwortschutz,
- rollenbasierte Zugänge,
- beschränkte administrative Berechtigungen,
- Sperrung oder Entfernung ausgeschiedener Benutzer,
- sichere Verwaltung technischer Zugangsschlüssel.

### 3. Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass Benutzer nur auf die ihrer Berechtigung unterliegenden Daten zugreifen können:

- Mandantentrennung nach Organisationen,
- Rollen- und Berechtigungskonzept,
- gesonderte Administratorrechte,
- beschränkter Zugriff auf Verwaltungsfunktionen,
- serverseitige beziehungsweise datenbankseitige Berechtigungsprüfungen,

- Schutz von Export- und Abrechnungsfunktionen.

## 4. Weitergabekontrolle

Maßnahmen zum Schutz personenbezogener Daten bei Übertragung und Weitergabe:

- verschlüsselte Datenübertragung mittels TLS,
- kontrollierte Schnittstellen,
- Zugriffsbeschränkungen für Exporte,
- vertragliche Verpflichtung von Unterauftragsverarbeitern,
- dokumentierte Regelungen für Drittlandübermittlungen.

## 5. Eingabekontrolle

Maßnahmen zur Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen:

- Zuordnung von Buchungen zu Benutzern,
- Zeitstempel für wesentliche Vorgänge,
- Protokollierung administrativer und sicherheitsrelevanter Aktionen, soweit erforderlich,
- Nachvollziehbarkeit von Korrektur- und Stornobuchungen.

## 6. Auftragskontrolle

Maßnahmen zur Sicherstellung der weisungsgemäßen Verarbeitung:

- Abschluss von Auftragsverarbeitungsverträgen,
- dokumentierte Weisungswege,
- Auswahl und Kontrolle von Unterauftragsverarbeitern,
- Vertraulichkeitsverpflichtungen,
- geregelte Support- und Administrationsprozesse.

## 7. Verfügbarkeitskontrolle

Maßnahmen zum Schutz gegen Verlust oder Zerstörung:

- regelmäßige Datensicherungen,
- redundante oder hochverfügbare Cloud-Infrastruktur, soweit vom Dienstleister bereitgestellt,
- Wiederherstellungsprozesse,
- Überwachung technischer Fehler,
- Sicherheitsupdates,
- Incident-Response-Verfahren.

## 8. Trennungsgebot

Maßnahmen zur getrennten Verarbeitung für unterschiedliche Zwecke oder Kunden:

- logische Trennung der Organisationen,

- organisationsbezogene Datenkennungen,
- rollenbasierte Sichtbarkeit,
- getrennte Produktiv-, Entwicklungs- und Testumgebungen, soweit technisch vorgesehen,
- keine Verwendung realer Produktivdaten in Tests, soweit nicht erforderlich und angemessen abgesichert.

### 9. Datenschutzfreundliche Voreinstellungen

- Beschränkung auf erforderliche Datenfelder,
- optionale Eingabe nicht zwingend erforderlicher Profilinformationen,
- konfigurierbare Rollen,
- Lösch- und Sperrmöglichkeiten,
- Beschränkung zentraler Tablet-Funktionen auf den erforderlichen Umfang.

### 10. Kontrolle und Weiterentwicklung

- regelmäßige Überprüfung der Schutzmaßnahmen,
- Aktualisierung eingesetzter Softwarekomponenten,
- Prüfung bekannt gewordener Sicherheitslücken,
- Anpassung der Maßnahmen an technische und organisatorische Veränderungen.

## Anlage 3

### Genehmigte Unterauftragsverarbeiter

Die nachfolgend aufgeführten Dienste werden entsprechend der aktuellen Produktivkonfiguration eingesetzt.

### 1. Google (Firebase / Google Cloud)

Anbieter: Google Cloud EMEA Limited beziehungsweise die jeweils vertragsführende Google-Gesellschaft

Leistung: Authentifizierung einschließlich systemseitiger Registrierungs-, Bestätigungs- und Passwort-E-Mails, Hosting, Datenbank, Cloud Functions, Dateispeicherung, technische Infrastruktur und Push-Zustellung über Firebase Cloud Messaging (FCM)

Mögliche Daten: Benutzer-, Organisations-, Buchungs-, Kommunikations-, Authentifizierungs-, Geräte-, Push- und Protokolldaten

Verarbeitungsort: Europäische Union und gegebenenfalls weitere vertraglich beziehungsweise rechtlich abgesicherte Standorte

Transfergrundlage: Angemessenheitsbeschluss, EU-U.S. Data Privacy Framework oder Standardvertragsklauseln, soweit erforderlich

### 2. Google Firebase Crashlytics

Anbieter: Google

Leistung: Fehler- und Crash-Reporting

Mögliche Daten: Geräteinformationen, Appversion, Fehlerprotokolle, technische Kennungen und gegebenenfalls Benutzerreferenzen

Verarbeitungsort: gemäß den vertraglichen Bedingungen von Google

### 3. Google Firebase Analytics

Anbieter: Google

Leistung: Nutzungsanalyse, soweit die Funktion aktiviert ist

Mögliche Daten: Geräte- und Nutzungsinformationen, technische Kennungen und Ereignisdaten

Verarbeitungsort: gemäß den vertraglichen Bedingungen von Google

### 4. Apple Push Notification Service (APNs)

Anbieter: Apple

Leistung: Zustellung von Push-Benachrichtigungen an Apple-Geräte

Mögliche Daten: Geräte- beziehungsweise Push-Token und technische Nachrichteninformationen

Verarbeitungsort: gemäß den vertraglichen Bedingungen von Apple

### 5. Google Play / Apple App Store

Anbieter: Google beziehungsweise Apple

Leistung: Bereitstellung der App und Abwicklung von In-App-Käufen, zum Beispiel zum Entfernen von Werbung

Mögliche Daten: App-Store-Konto, Kaufstatus, Transaktions- und technische Gerätedaten nach Maßgabe des jeweiligen Plattformbetreibers

Verarbeitungsort: gemäß den vertraglichen Bedingungen des jeweiligen Plattformbetreibers

Änderungen der Unterauftragsverarbeiterliste werden durch Bereitstellung einer neuen Vertragsversion nach Maßgabe von Ziffer 15 bekannt gemacht und bedürfen der erneuten Zustimmung.

Für Tracking- und Werbedienste kann eine gemeinsame Verantwortlichkeit oder eigene Verantwortlichkeit des jeweiligen Anbieters vorliegen.

Sofern Daten in Drittländer, zum Beispiel in die USA, übermittelt werden, erfolgt dies auf Grundlage der Standardvertragsklauseln der Europäischen Kommission sowie gegebenenfalls des EU-U.S. Data Privacy Framework.