Vereinbarung über die Datenbearbeitung im Rahmen der TWINT Zusatzfunktion «QR-Code-Sticker mit Information zur Zahlung»

1. Geltungsbereich und Definitionen

1.1. Geltungsbereich

Dieses Dokument gilt ergänzend zum «Payment-Vertrags für die Akzeptanz von TWINT» zwischen der TWINT Acquiring AG (nachfolgend «TWINT» oder «Auftragsbearbeiter») und dem Vertragspartner (nachfolgend «Datenverantwortlicher»). Die Vereinbarung gilt für personenbezogene Daten, die durch TWINT und allfällige Unterauftragsbearbeiter im Zusammenhang mit der Bereitstellung der Zusatzfunktion «QR-Code-Sticker mit Information zur Zahlung» bearbeitet werden. Sie findet keine Anwendung auf alle übrigen Transaktionen im TWINT Zahlungssystem, bei denen die Zusatzfunktion nicht genutzt wird, da dort keine personenbezogenen Daten bearbeitet werden.

Die Anhänge 1 und 2 sind Bestandteile dieser Vereinbarung. Darin werden der vereinbarte Gegenstand, die Art und der Zweck der Bearbeitung, die Art der personenbezogenen Daten, die Kategorie der betroffenen Personen, die beigezogenen Unterauftragsbearbeiter (Anhang 1) sowie die technischen und organisatorischen Massnahmen (Anhang 2) festgelegt.

1.2. Definitionen

Sofern hier nicht anders definiert, haben alle Begriffe die gleiche Bedeutung wie im Schweizer Datenschutzgesetz (DSG). Ein Verweis auf das DSG schliesst immer auch einen Verweis auf die Verordnung zum DSG (DSV) und jede andere Bestimmung des materiellen schweizerischen Datenschutzrechts ein.

Unter der vorliegenden Vereinbarung ist TWINT Auftragsbearbeiter und der Vertragspartner ist Datenverantwortlicher.

Für die Zwecke dieses Vertrags gelten folgende Bedeutungen:

Personenbezogene Daten	Alle Informationen über eine bestimmte oder bestimmbare natürliche Person, die von den Kundinnen und Kunden des Vertragspartners im Feld der Zusatzfunktion «QR-Code-Sticker mit Information zur Zahlung» eingegeben werden, wie bspw. Name, Telefonnummer, E-Mail-Adresse, und die unter den Schutz des Datenschutzrechts fallen.
Datenverantwortlicher	Natürliche oder juristische Person, die über den Zweck und die Mittel der Bearbeitung der personenbezogenen Daten bestimmt (hier: Vertragspartner).
Auftragsbearbeiter	Natürliche oder juristische Person, die im Auftrag des Datenverantwortlichen personenbezogene Daten bearbeitet (hier: TWINT Acquiring AG).
Unterauftragsbearbeiter	Vom Auftragsbearbeiter beauftragter (Unter-)Auftragsbearbeiter (verbundene Unternehmen oder Drittanbieter), der vom Auftragsbearbeiter personenbezogene Daten erhält, die ausschliesslich dazu bestimmt sind, nach der Übermittlung im Namen des Datenverantwortlichen gemäss dessen Anweisungen und den Bedingungen des Untervertrags bearbeitet zu werden.
Drittland	Jedes Land, welches vom Bundesrat nicht als sicheres Land mit angemessenem Datenschutzniveau anerkannt wird.
Betroffene Person	Bestimmte oder bestimmbare natürliche Person, über die personenbezogene Daten bearbeitet werden.

2. Pflichten und Verantwortung des Datenverantwortlichen

Der Datenverantwortliche ergreift eigenständig angemessene technische und organisatorische Massnahmen zum Schutz der personenbezogenen Daten in seinem Verantwortungsbereich (z. B. in seinen eigenen Systemen, Gebäuden, Anwendungen/Umgebungen, für die er operativ verantwortlich ist).

3. Pflichten des Auftragsbearbeiters

3.1. Weisungen des Datenverantwortlichen

TWINT verpflichtet sich und gewährleistet, dass er alle und jegliche personenbezogenen Daten, die er vom Datenverantwortlichen erhalten oder zur Verfügung gestellt bekommen hat oder die von diesen Daten abgeleitet wurden, ausschliesslich im Auftrag und ausschliesslich für die Zwecke des Datenverantwortlichen, wie Anhang 1 dargelegt, bearbeiten wird.

3.2. Informationspflicht bei Verletzung

TWINT wird den Datenverantwortlichen unverzüglich informieren und mit ihm zusammenarbeiten, sobald TWINT Kenntnis von einer Verletzung des Schutzes der personenbezogenen Daten des Datenverantwortlichen erlangt oder wenn eine staatliche Behöre Ermittlungen gegen TWINT durchführt oder Massnahmen gegen TWINT anordnet, sowie bei allen anderen einschlägigen Untersuchungen durch solche Behörden. Aus Benachrichtigungen dieser Art dürfen keine Fehlereingeständnisse oder Haftungen von Seiten TWINT abgeleitet werden.

3.3. Zusammenarbeit

Auf Wunsch des Datenverantwortlichen unterstützt TWINT diesen in angemessenem Umfang bei der Bearbeitung von Anfragen

TWINT Acquiring AG
Stauffacherstrasse 41
CH-8004 Zürich

einzelner betroffenen Personen oder Aufsichtsbehörden in Bezug auf die Bearbeitung personenbezogener Daten durch TWINT oder einer Verletzung des Schutzes der personenbezogenen Daten.

3.4. Zugriff durch Mitarbeitende und Unterauftragsbearbeiter

TWINT ergreift angemessene Massnahmen, um die Zuverlässigkeit aller Mitarbeitenden, Beauftragten oder Unterauftragsbearbeiter zu gewährleisten, die Zugang zu den personenbezogenen Daten haben könnten. TWINT gewährleistet, dass es den betreffenden Personen untersagt ist, die Daten ausserhalb oder entgegen den Anweisungen des Datenverantwortlichen zu bearbeiten. TWINT gewährleistet ferner, dass diese Personen eine angemessene Schulung zum Schutz der personenbezogenen Daten erhalten.

3.5. Technische und organisatorische Massnahmen

TWINT trifft vor der Bearbeitung geeignete technische und organisatorische Massnahmen im Sinne des DSG, um die personenbezogenen Daten vor unbefugten Bearbeitungen, einschliesslich nicht ausdrücklich durch diesen Vertrag zugelassener Bearbeitungen, vor versehentlichem Verlust oder Zerstörung oder Beschädigung der personenbezogenen Daten zu schützen. TWINT trifft organisatorische Massnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Bearbeitung gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Bearbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen zu berücksichtigen.

TWINT ist berechtigt, die gemäss Anhang 2 getroffenen technischen und organisatorischen Massnahmen jederzeit unangekündigt zu ändern, unter der Voraussetzung, dass das vertraglich vereinbarte Schutzniveau eingehalten wird.

3.6. Löschung

TWINT verpflichtet sich, die personenbezogenen Daten zu löschen, wenn der Datenverantwortliche dies anordnet. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenbearbeitung nicht möglich, verpflichtet sich TWINT, die personenbezogenen Daten unwiderruflich zu anonymisieren.

4. Unterauftragsbearbeitung

TWINT beauftragt keine Unterauftragsbearbeiter mit der Bearbeitung der personenbezogenen Daten, es sei denn dies sei notwendig oder erfolgt mit Zustimmung des Datenverantwortlichen.

TWINT prüft vor der Auswahl eines Unterauftragsbearbeiters dessen Massnahmen zur Wahrung der Sicherheit, des Datenschutzes und der Vertraulichkeit, um den Schutz der personenbezogenen Daten zu gewährleisten und schliesst mit ihnen einen schriftlichen Vertrag (elektronische Form gilt äquivalent).

Eine entsprechende Liste findet sich in Anhang 1.

5. Grenzüberschreitender Transfer

TWINT übermittelt keine personenbezogenen Daten in Länder ausserhalb der EU und/oder des Europäischen Wirtschaftsraums (EWR) ohne die vorherige Zustimmung des Datenverantwortlichen.

Werden personenbezogene Daten, die im Rahmen dieser Vereinbarung bearbeitet werden, von einem Land innerhalb des Europäischen Wirtschaftsraums in ein Land ausserhalb des Europäischen Wirtschaftsraums übermittelt, stellt der Auftragsbearbeiter sicher, dass die personenbezogenen Daten angemessen geschützt sind. Zu diesem Zweck verwendet der Auftragsbearbeiter die gemäss dem DSG modifizierten EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten.

6. Rechte der betroffenen Personen

Der Datenverantwortliche ist dafür verantwortlich, dass die betroffenen Personen ihr Recht auf Auskunft, Berichtigung, Sperrung, Einschränkung der Bearbeitung, Löschung oder Datenübertragung nach Massgabe des DSG wahrnehmen können. Der Auftragsbearbeiter wird mit dem Datenverantwortlichen in vollem Umfang und ohne Verzögerung zusammenarbeiten und dem Datenverantwortlichen die erforderlichen Dienstleistungen zur Verfügung stellen, um Anträge oder Anfragen der betroffenen Personen zu erfüllen. Der Auftragsbearbeiter verweist alle Anträge oder Anfragen, die er direkt erhält, unverzüglich an den Datenverantwortlichen weiter, ohne sie in der Sache zu beantworten.

7. Varia

Diese Vereinbarung ist mit Abschluss eines Payment-Vertrages und der Nutzung der entsprechenden Zusatzfunktion automatisch verbindlich. Sie endet automatisch mit der Beendigung der von TWINT erbrachten Dienstleistungen, für die diese Vereinbarung geschlossen wurde. Der Datenverantwortliche kann den Transfer von personenbezogenen Daten und/oder deren Bearbeitung jederzeit aussetzen. Die Rechte und Pflichten der Vertragsparteien aus dieser Vereinbarung gelten unbeschadet und ungeachtet anderer Rechte und Pflichten, die die Vertragsparteien aufgrund anderer bestehender Vereinbarungen haben oder nicht haben. Dieser Vertrag regelt nicht die Folgen, die die Ausübung eines Rechts und die Erfüllung einer Verpflichtung aus diesem Vertrag im Rahmen einer bestehenden Vereinbarung zwischen den Vertragsparteien haben können.

Dieser Vertrag unterliegt dem materiellen Recht der Schweiz und wird in Übereinstimmung mit diesem ausgelegt. Alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem oder einer Verletzung desselben ergeben, werden ausschliesslich von den ordentlichen Gerichten in Zürich, Schweiz, entschieden.

TWINT Acquiring AG
Stauffacherstrasse 41
CH-8004 Zürich

Anhang 1: Gegenstand der Auftragsbearbeitung

1. Zweck der Bearbeitung

Der Auftrag des Datenverantwortlichen an TWINT umfasst folgende Leistungen:

- Anreicherung von Transaktionen mit Zusatzinformationen

2. Kategorien der personenbezogenen Daten

Folgende Kategorien von personenbezogenen Daten sind regelmässig Gegenstand der Bearbeitung:

- Angabe zur Person (Vorname, Nachname)
- Adressdaten (Strasse und Hausnummer, Postleitzahl, Ort)
- Kontaktdaten (E-Mail-Adresse, Telefonnummer)
- Zahlungszweck (z.B. Mitgliedschaftsnummer, Rechnungsnummer etc.)

3. Kategorien der betroffenen Personen

Kreis der von der Datenbearbeitung betroffenen Personen:

- Kundinnen und Kunden der Händler

4. Liste der Unterauftragsbearbeiter

TWINT nimmt für die Bearbeitung von Daten im Auftrag des Datenverantwortlichen Leistungen von Dritten in Anspruch, die im Auftrag von TWINT Daten bearbeiten (Unterauftragsbearbeiter).

Dabei handelt es sich um nachfolgende Unternehmen:

- Swisscom (Schweiz) AG, Alte Tiefenaustrasse 6, 3050 Bern
- sumIT AG, Täfernstrasse 28, 5400 Baden (nur Zugriff auf TWINT Systeme)

TWINT Acquiring AG
Stauffacherstrasse 41
CH-8004 Zürich

Anhang 2: Technische und organisatorische Massnahmen

TWINT AG unterhält ein wirtschaftlich angemessenes Daten- und Informationssicherheitsprogramm in Übereinstimmung mit den Best Practices der Branche. Dieses umfasst technische und organisatorische Massnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus für personenbezogene (Kunden-)Daten unter Berücksichtigung der mit der Verarbeitung verbundenen Risiken, insbesondere der versehentlichen oder unrechtmässigen Zerstörung, des Verlusts, der Änderung oder der unbefugten Weitergabe von personenbezogenen (Kunden-)Daten oder des unbefugten Zugriffs auf personenbezogene (Kunden-)Daten, sowie unter Berücksichtigung der Art der zu schützenden personenbezogenen (Kunden-)Daten in Hinblick auf den Stand der Technik und die Implementierungskosten.

Das Sicherheitsprogramm von TWINT AG umfasst die folgenden Massnahmen:

Sicherheitsprogramm

a. **Informationssicherheitsmanagementsystem (ISMS) gemäss ISO 27001:** TWINT AG unterhält ein risikobasiertes ISMS-Sicherheitsprogramm, um ihre Geschäftsinformationen sowie die Informationen ihrer Kundschaft und Partnerorganisationen systematisch zu verwalten und zu schützen.

b. **Security-Governance-Ausschuss:** TWINT AG führt einen Security-Governance-Ausschuss bestehend aus den Issuer-Banken und dem Käuferkreis, der die Shareholder der TWINT AG repräsentiert und das Sicherheitsprogramm des Unternehmens überwacht. Dieser Ausschuss tritt einmal monatlich zusammen, um den Betriebsstatus des ISMS (einschliesslich Auditergebnissen, Risiken, Bedrohungen, Sanierungsmassnahmen und anderer sicherheitsrelevanter Fragen) zu überprüfen und die laufende Verbesserung der Sicherheit im gesamten Unternehmen voranzutreiben.

c. **Richtlinie zur Reaktion auf sicherheitsrelevante Vorfälle:** TWINT AG unterhält Richtlinien und Verfahren, um (1) sicherheitsrelevante Vorfälle zu untersuchen und darauf zu reagieren, einschliesslich Verfahren zur Beurteilung der Bedrohung durch relevante Schwachstellen oder Sicherheitsvorfälle unter Anwendung definierter Vorfallsklassifizierungen und -kategorien, und um (2) Abhilfe- und Schadensbegrenzungsmassnahmen für Vorfälle festzulegen, einschliesslich Massnahmen zur Sammlung von Abweichungen und Beweisen sowie definierter Schritte zur Behebung.

d. **Pflege der Richtlinien:** Alle sicherheits- und datenschutzbezogenen Richtlinien sind zu dokumentieren, regelmässig zu überprüfen, zu aktualisieren und von der Geschäftsleitung zu genehmigen, um sicherzustellen, dass sie den Best Practices, den rechtlichen und regulatorischen Anforderungen sowie den Branchenstandards entsprechen.

e. **Kommunikation und Engagement:** Sicherheits- und Datenschutzbestimmungen und -verfahren sind zu veröffentlichen und allen Mitarbeitenden und relevanten Subunternehmen wirksam zu kommunizieren. Die Sicherheit fällt in die Zuständigkeit der obersten Unternehmensebene, wobei die Geschäftsleitung Sicherheitsprobleme regelmässig erörtert und die Leitung der unternehmensweiten Sicherheitsinitiativen innehat.

Personalsicherheit

a. Sicherheits**überprüfung:** Mitarbeitende mit Zugriff auf personenbezogene (Kunden-)Daten oder auf die Anlagen und Geräte, auf denen diese gespeichert sind, werden (im Rahmen der lokalen Gesetze und Bestimmungen) einer Sicherheitsüberprüfung unterzogen.

b. **Geheimhaltungspflicht:** Mitarbeitende mit Zugriff auf personenbezogene (Kunden-)Daten unterliegen gemäss Vertrag mit TWINT AG einer verbindliche Geheimhaltungspflicht in Bezug auf die personenbezogenen (Kunden-)Daten.

c. **Schulungen zum Sicherheitsbewusstsein:** Bei Eintritt in das Unternehmen und in regelmässigen Abständen werden die Mitarbeitenden während der Anstellungsdauer in bewährten Sicherheitsverfahren und Datenschutzgrundsätzen geschult.

d. **Verhaltenskodex (Code of Conduct):** TWINT AG pflegt einen Verhaltenskodex und ein Compliance-Programm, um eine ethische Verhaltensweise sowie die Einhaltung der geltenden Gesetze und Vorschriften zu gewährleisten.

Sicherheit Dritter

a. **Screening:** TWINT AG stellt mittels Richtlinien und Verfahren sicher, dass alle neuen Lieferanten, SaaS-Anwendungen, IT-Softwares und IT-Servicelösungen einer angemessenen Due-Diligence-Prüfung unterzogen werden, die bestätigt, dass sie in der Lage sind, die Geschäftsziele sowie die Anforderungen an die Unternehmenssicherheit und die Compliance einzuhalten.

b. **Vertragspflichten:** TWINT AG stellt sicher, dass die Verträge mit Lieferanten angemessene Bestimmungen zu Geheimhaltung und Datenschutz beinhalten, um die Interessen von TWINT AG zu schützen und sicherzustellen, dass TWINT AG ihre Sicherheits- und Datenschutzpflichten gegenüber der Kundschaft, Partnern, Mitarbeitenden, Regulierungsbehörden und anderen Stakeholdern einhalten kann.

c. **Monitoring:** TWINT AG überprüft bestehende Drittanbieter regelmässig, um sicherzustellen, dass die Lieferanten die Vertragsbedingungen, einschliesslich der Anforderungen an Sicherheit und Verfügbarkeit, einhalten.

TWINT Acquiring AG
Stauffacherstrasse 41
CH-8004 Zürich

Physische Sicherheit

a. **Sicherheit der Betriebsgebäude:** TWINT AG unterhält ein Sicherheitsprogramm, das die Gebäudeeingänge, die Videoüberwachungsanlagen und die allgemeine Sicherheit der Büros, einschliesslich eines Sicherheitsperimeters, betrifft.

b. **Sicherheit des unternehmenseigenen Rechenszentrums:** Systeme, die sich auf dem Gelände von TWINT AG befinden, sind mit Massnahmen zu schützen, die unbefugte logische (elektronische) oder physische Zugriffe wirksam verhindern.

c. **Sicherheit des Rechenzentrums:** TWINT AG nutzt Infrastructure-as-a-Service (IaaS)-Rechenzentren für Hosting-Infrastrukturdienste. TWINT AG beurteilt regelmässig die Sicherheits- und Compliance-Massnahmen des jeweiligen Rechenzentrumbetreibers in regelmässigen Abständen; der Betreiber hält die Best Practices der Branche und die zahlreichen Standards ein.

Lösungssicherheit

c. Lebenszyklus bei **Softwareentwicklung (Software Development Life Cycle, SDLC):** TWINT AG unterhält eine Richtlinie für den Lebenszyklus bei Softwareentwicklung, die den Prozess für die Schaffung von sicheren Produkten und Diensten durch die Mitarbeitenden sowie die Aktivitäten festlegt, die die Mitarbeitenden während der einzelnen Entwicklungsschritte (Anforderungen, Design, Implementierung, Verifizierung, Dokumentierung und Lieferung) aus- bzw. durchzuführen haben.

d. **Sichere Entwicklung:** Die Teams Produktmanagement, Produktentwicklung, Produkttest und Produktbereitstellung befolgen Richtlinien und Verfahren für die sichere Anwendungsentwicklung, die dem Branchenstandard entsprechen.

e. **Schwachstellenbewertung:** TWINT AG führt regelmässig Sicherheitsbewertungen, Schwachstellenscans und Penetrationstests durch. Identifizierte Probleme bei Lösungsprodukten werden gemäss Umfang des potenziellen Risikos und seiner Auswirkungen sowie gemäss Wahrscheinlichkeit und der Folgenabschätzung des betreffenden Problems bewertet. Schwachstellen werden anhand der Risikobewertung behoben.

Operative Sicherheit

a. **Zugriffskontrollen:** TWINT AG unterhält Richtlinien, Verfahren und logische Kontrollen, um Zugriffsberechtigungen für Mitarbeitende und Dritte festzulegen, den Zugriff auf ordnungsgemäss befugte Mitarbeitende zu beschränken und unbefugte Zugriffe zu verhindern.

b. **Least Privilege:** TWINT AG stellt sicher, dass die Mitarbeitenden nur in dem Ausmass Zugriff auf Systeme und Daten haben, wie es für die Erfüllung ihrer Aufgaben erforderlich ist. Nur entsprechen befugte Mitarbeitende haben physischen Zugang zu Infrastruktur und Anlagen. Der Zugriff auf Produktionsressourcen ist auf Mitarbeitende beschränkt, die Zugriff benötigen; die Zugangsrechte werden regelmässig überprüft und zertifiziert, um sicherzustellen, dass der Zugriff angemessen ist.

c. **Malware:** TWINT AG setzt branchenübliche Massnahmen zur Erkennung und Beseitigung von Malware, Viren, Ransomware, Spyware und anderen absichtlich schädlichen Programmen ein, die dazu verwendet werden können, unbefugten Zugriff auf Informationen oder Systeme zu erlangen.

d. **Verschlüsselung:** TWINT AG trägt der Sensibilität der Daten und den mit einem Verlust verbundenen Risiken Rechnung und verwendet starke, dem Branchenstandard entsprechende Verschlüsselungsmethoden, um Daten während der Übertragung und im Ruhezustand zu schützen. Sämtliche Laptops und andere Wechselmedien, einschliesslich Backups, sind zu verschlüsseln.

e. **Geschäftskontinuität und Notfallwiederherstellung (Business Continuity and Disaster Recovery, BCDR):** TWINT AG unterhält formelle BCDR-Pläne, die regelmässig überprüft und aktualisiert werden, um sicherzustellen, dass die Systeme und Dienste von TWINT während eines Ausfalls, einschliesslich Ausfällen aufgrund von Naturkatastrophen oder Systemstörungen, verfügbar bleiben.

f. **Daten-Backups:** TWINT AG sichert Daten und Systeme an einem alternativen Speicherort, sodass sie bei einem Ausfall des Primärsystems wiederhergestellt werden können. Alle Backups müssen während der Datenübertragung und im Ruhezustand starke Verschlüsselungen aufweisen.

g. **Änderungsmanagement:** TWINT AG unterhält Richtlinien und Verfahren für das Änderungsmanagement, um Änderungen an der Infrastruktur, den Systemen, den Netzwerken und den Anwendungen von TWINT zu planen, zu testen, zu terminieren, zu kommunizieren und auszuführen.

h. **Netzwerksicherheit:** TWINT AG setzt Technologien und -Kontrollen gemäss den in der Branche üblichen Standards ein, um die Netzwerksicherheit, einschliesslich Firewalls, Netzsegmentierung und drahtloser Netzwerksicherheit, zu schützen. Die Netzwerke sind so zu gestalten und zu konfigurieren, dass Verbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken eingeschränkt werden; die Netzwerkgestaltung und -kontrolle ist mindestens einmal jährlich zu überprüfen.

i. **Datentrennung:** TWINT AG stellt sicher, dass produktive und nicht produktive Daten und Systeme strikt getrennt werden.

TWINT Acquiring AG
Stauffacherstrasse 41
CH-8004 Zürich