Agreement on data processing within the framework of the TWINT “QR code sticker with payment information” additional function

1. Scope and definitions

1.1. Scope

This document shall apply as a supplement to the “Payment Contract for the Acceptance of TWINT” between TWINT Acquiring AG (hereinafter referred to as “TWINT” or the “Processor”) and the contractual partner (hereinafter referred to as the “Data Owner”). The Agreement shall apply for personal data that is processed by TWINT and any sub-processors in connection with the provision of the “QR code sticker with payment information” additional function. The Agreement shall not apply to any other transactions within the TWINT system in which the aforementioned additional function is not used, as no personal data is processed in such transactions.

Annexes 1 and 2 form an integral part of this Agreement. The agreed object, the nature and purpose of the processing, the type of personal data, the category of the affected persons, the sub-processors involved (Annex 1) and the technical and organisational measures are defined in the annexes.

1.2. Definitions

Unless a different definition is provided in this document, all of the terms shall be deemed to have the same meaning as in the new Federal Act on Data Protection (nFADP). A reference to the nFADP shall also always include a reference to the Ordinance on Data Protection (DPO) and every provision within substantial Swiss data protection legislation.

Pursuant to this Agreement, TWINT is the Processor and the the contractual partner is the Data Owner.

For the purposes of this Agreement, the following definitions shall apply:

Personal data	Any information related to an identified or identifiable natural person that is entered in the field by the customer within the “QR code sticker with payment information” additional function, such as name, telephone number and e-mail address, shall fall under the protection of data protection legislation.
Data Owner	The natural person or legal entity that decides upon the purpose and method of processing of the personal data (here: contractual partner).
Processor	The natural person or legal entity that processes the personal data on behalf of the Data Owner (here: TWINT Acquiring AG).
Sub-processor	Commissioned by the Processor, the (sub-)processor (an affiliated company or third-party provider) receives personal data from the Processor that is solely intended to be processed after its transmission on behalf of the Data Owner in accordance with the Data Owner's instructions and the terms of the sub-contract.
Third country	Every country that is not recognised by the Federal Council as a safe country with an appropriate level of data protection.
Data subject	An identified or identifiable person whose personal data is being processed.

2. Obligations and responsibility of the Data Owner

The Data Owner shall independently take the appropriate technical and organisational measures to protect personal data in their area of responsibility (e.g. in their own systems, buildings, applications/environments for which they are operationally responsible).

3. Obligations of the Processor

3.1. Instructions from the Data Owner

TWINT shall undertake to and guarantee that it shall process all personal data that it receives from the Data Owner, has been made available to it or that can be deduced from this data exclusively on behalf of and for the purposes intended by the Data Owner, as illustrated in Annex 1.

3.2. Duty to provide information in the event of a breach

TWINT shall inform the Data Owner immediately and work together with them as soon as TWINT gains knowledge of a breach of the security protecting the personal data of the Data Owner or if a public authority or government agency conducts an enquiry into TWINT or takes measures against TWINT, as well as if any other relevant investigations are carried out by such authorities. No admission of fault or liability on the part of TWINT may be derived from notifications of this type.

3.3. Collaboration

Upon the request of the Data Owner, TWINT shall provide the Data Owner with a commensurate level of support in the processing of enquiries from individual data subjects or supervisory authorities in connection with the processing of personal data by TWINT or a breach of the protection of the personal data.

TWINT Acquiring AG
Stauffacherstrasse 41
CH-8004 Zurich

3.4. Access by employees and sub-processors

TWINT shall take the appropriate measures to guarantee the reliability of all employees, authorised representatives and sub-processors that could have access to the personal data. TWINT shall guarantee that the persons concerned are prohibited from processing the data outside of or contrary to the instructions of the Data Owner. TWINT shall also guarantee that these persons receive appropriate training on the protection of personal data.

3.5. Technical and organisational measures

Prior to the processing of the data, TWINT shall take suitable technical and organisational measures within the meaning of nFADP to protect personal data against unauthorised processing, including processing not explicitly permitted by this Agreement, as well as against the accidental loss, destruction or damage of personal data. TWINT shall take organisational measures that guarantee the confidentiality, integrity, availability and robustness of the systems and services in connection with the processing. In so doing, the state of the art, the implementation costs and the nature, scope and purposes of the processing, as well as the varying levels of probability and severity of the risk vis-à-vis the rights and freedoms of the Data Subjects must be taken into consideration.

TWINT shall be entitled to change any of the technical and organisational measures set out in Annex 2 at any time and without making an announcement, provided that the level of protection contractually agreed to is maintained.

3.6. Deletion

TWINT shall undertake to delete personal data if the Data Owner instructs it to do so. If it is not possible to delete the data in a manner that is compliant with data protection legislation or to limit the data processing appropriately, TWINT shall undertake to anonymise the personal data in an irrevocable fashion.

4. Sub-processing

TWINT shall not commission any sub-processors with the processing of the personal data unless it is necessary and the Data Owner has consented to this.

Before selecting a sub-processor, TWINT shall check the measures the sub-processor implements in terms of security, data protection and confidentiality in order to guarantee the protection of the personal data and it shall conclude a written contract with them (an electronic version shall have the equivalent effect).

See Annex 1 for a corresponding list.

5. Cross-border transfers

TWINT shall not transfer any personal data to or within countries outside of the EU and/or the European Economic Area (EEA) without the prior consent of the Data Owner.

Should personal data that is processed within the framework of this Agreement be transferred from a country within the European Economic Area to a country outside of the European Economic Area, the Processor shall ensure that the personal data is provided with an appropriate level of protection. For this purpose, the Data Owner shall use the standard contractual clauses of the European Union regarding the transfer of personal data that have been modified in accordance with the nFADP.

6. Rights of the Data Subjects

The Data Owner shall be responsible for the data subjects being aware of their right to information, amendment, blocking, restriction of processing, deletion and transmission of their data in accordance with the nFADP. The Processor shall work together with the Data Owner fully and without delay and provide the Data Owner with the services required to fulfil the proposal and enquires made by the data subjects. The Processor shall pass on all proposals and enquiries that it directly receives to the Data Owner immediately without actually responding to them.

7. Miscellaneous

Upon the conclusion of a payment agreement and the use of the relevant additional function, this Agreement shall automatically become binding. It shall end automatically upon the fulfilment of the services rendered by TWINT for which this Agreement has been concluded. The Data Owner may suspend the transfer of personal data and/or its processing at any time. The rights and obligations of the contractual parties in this Agreement shall apply notwithstanding and without prejudice to any other rights and obligations that the contractual parties have or do not have based on other existing agreements. This Agreement shall not govern the consequences that may arise within the framework of an existing agreement between the contractual parties as a result of the exercising of a right or the fulfilment of an obligation set out in this Agreement.

This Agreement shall be subject to and construed in accordance with Swiss substantive law. Any disputes that arise out of or in connection with this Agreement or a breach thereof shall be decided exclusively by the ordinary courts of the city of Zurich, Switzerland.

TWINT Acquiring AG
Stauffacherstrasse 41
CH-8004 Zurich

Annex 1: The processing object

1. Purpose of the processing

The mandate of the Data Owner to TWINT comprises the following services:

- Provision of transactions with additional information

2. Categories of personal data

The following categories of personal data are regularly the processing object:

- Personal information (first name and last name)
- Address details (street name and building number, postcode, town/city)
- Contact details (e-mail address, telephone number)
- Payment purpose (e.g. membership number, invoice number)

3. Categories of data subjects

Group of people whose data is to be processed:

- Customers of merchants

4. List of sub-processors

In order to process data on behalf of the Data Owner, TWINT shall utilise the services of third parties that process data on behalf of TWINT (sub-processors).

The third parties with whom we work are the following companies:

- Swisscom (Switzerland) Ltd, Alte Tiefenaustrasse 6, 3050 Bern
- sumIT AG, Täfernstrasse 28, 5400 Baden (only access to TWINT systems)

Annex 2: Technical and organisational measures

TWINT AG has implemented and shall maintain a commercially reasonable data and information security program in accordance with industry best practices, which shall include technical and organisational measures to ensure an appropriate level of security for (customer) personal data taking into account the risks presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to (customer) personal data, and the nature of the (customer) personal data to be protected having regard to the state of the art and the cost of implementation.

The security program of TWINT AG shall include the following measures.

Security Program

a. **ISO27001-based Information Security Management System (ISMS)**: TWINT AG shall maintain an ISMS riskbased security program to systematically manage and protect the organization's business information and the information of its customers and partners.

b. **Security Governance Board**: TWINT AG shall maintain a security governance board comprised of the issuer banks and acquirer(s) representing the shareholders of TWINT that oversees the company's security program. This committee shall meet monthly to review the operational status of the ISMS (including audit findings, risks, threats, remediation actions, and other security-related issues) and drive continuous security improvement throughout the business.

c. **Security incident response policy**: TWINT AG shall maintain policies and procedures to (1) investigate and respond to security incidents, including procedures to assess the threat of relevant vulnerabilities or security incidents using defined incident classifications and categorizations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.

d. **Policy maintenance**: All security and privacy related policies shall be documented, regularly reviewed, updated and approved by management to ensure they remain consistent with best practices, legal and regulatory requirements and industry standards.

e. **Communication and commitment**: Security and privacy policies and procedures shall be published and effectively communicated to all personnel and relevant subcontractors. Security shall be addressed at the highest levels of the company with executive management regularly discussing security issues and leading company-wide security initiatives.

Personnel Security

a. **Background screening**: Personnel who have access to (customer) personal data or the equipment on which it is stored shall be subject to background screening (as allowed by local laws and regulations).

b. **Confidentiality obligations**: Personnel who have access to (customer) personal data shall be subject to a binding contractual obligation with TWINT AG to keep the (customer) personal data confidential.

c. **Security awareness training**: Personnel shall receive training upon hire and regularly thereafter covering security best practices and privacy principles.

d. **Code of conduct**: TWINT AG shall maintain a code of business conduct policy and compliance program to ensure ethical behavior and compliance with applicable laws and regulations.

Third-Party Security

a. **Screening**: TWINT shall maintain policies and procedures to ensure that all new suppliers, SaaS applications, IT Software, and IT service solutions are subject to reasonable due diligence to confirm their ability to meet corporate security and compliance requirements as well as business objectives.

b. **Contractual obligations**: TWINT AG shall ensure that contractual agreements with suppliers include confidentiality and privacy provisions as appropriate to protect TWINT AG's interests and to ensure TWINT can meet its security and privacy obligations to customers, partners, employees, regulators and other stakeholders.

c. **Monitoring**: TWINT AG shall periodically review existing third-party suppliers to ensure the supplier complies with contractual terms, including any security and availability requirements.

Physical Security

a. **Corporate facility security**: TWINT AG maintains a facility security program that manages building entrances, CCTVs, and overall security of its offices, including a security perimeter.

b. **Corporate data center security**: Systems installed on TWINT AG's premises shall be protected in such a manner that unauthorized logical or physical access is effectively prevented.

c. **Data center security**: TWINT AG leverages Infrastructure as a Service (IaaS) data centers for hosting infrastructure services. TWINT AG regularly assesses the security and compliance measures of the applicable data center provider, and the provider follows industry best practices and comply with numerous standards.

Solution Security

c. **Software development life cycle (SDLC)**: TWINT AG maintains a software development life cycle policy that defines the process by which personnel create secure products and services and the activities that personnel must perform at various stages of development (requirements, design, implementation, verification, documentation and delivery).

d. **Secure development**: Product management, development, test and deployment teams follow secure application development policies and procedures that are aligned to industry-standard practices.

e. **Vulnerability assessment**: TWINT AG shall regularly conduct security assessments, vulnerability scans and penetration tests. Identified product solution issues shall be scored on risk impact level and the likelihood and potential consequences of an issue occurring. Vulnerabilities are remediated on the basis of assessed risk.

Operational Security

a. **Access controls**: TWINT AG shall maintain policies, procedures, and logical controls to establish access authorizations for employees and third parties to limit access to properly authorized personnel and to prevent unauthorized access.

b. **Least privilege**: TWINT AG shall ensure that personnel only have access to systems and data as required for the performance of their roles; only authorized personnel have physical access to infrastructure and equipment; access to production resources is restricted to employees requiring access and access rights are reviewed and certified regularly to ensure access is appropriate.

c. **Malware**: TWINT AG shall utilize industry-standard measures to detect and remediate malware, viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorized access to information or systems.

d. **Encryption**: TWINT AG shall use industry-standard strong encryption methods to protect data in transit and at rest as appropriate to the sensitivity of the data and the risks associated with loss; all laptops and other removable media, including backups shall be encrypted.

e. **Business continuity and disaster recovery (BCDR)**: TWINT AG shall maintain formal BCDR plans that are regularly reviewed and updated to ensure TWINT's systems and services remain resilient in the event of a failure, including natural disasters or system failures.

f. **Data backups**: TWINT AG shall backup data and systems using alternative site storage available for restore in case of failure of the primary system. All backups shall use strong encryption in transit and at rest.

g. **Change management**: TWINT AG shall maintain change management policies and procedures to plan, test, schedule, communicate, and execute changes to TWINT's infrastructure, systems, networks, and applications.

h. **Network security**: TWINT AG shall implement industry standard technologies and controls to protect network security, including firewalls, network segmentation and wireless security. Networks shall be designed and configured to restrict connections between trusted and untrusted networks, and network designs and controls shall be reviewed at least annually.

i. **Data segregation**: TWINT AG shall ensure that production and non-production data and systems are strictly separated.