Accordo sul trattamento dei dati nell'ambito della funzione supplementare di TWINT «Adesivo con codice QR con informazioni sul pagamento»

1. Ambito di validità e definizioni

1.1. Ambito di validità

Il presente documento è un'integrazione al «Contratto Payment per l'accettazione di TWINT» tra TWINT Acquiring SA (di seguito «TWINT» o «Responsabile del trattamento») e il contraente (di seguito «titolare del trattamento»). L'accordo si applica ai dati personali trattati da TWINT e da eventuali sub-Responsabili del trattamento in relazione alla messa a disposizione della funzione supplementare «Adesivo con codice QR con informazioni sul pagamento». L'accordo non trova applicazione per tutte le altre transazioni all'interno del sistema di pagamento TWINT per le quali la funzione supplementare non viene utilizzata, in quanto per tali transazioni non avviene alcun trattamento di dati personali.

Gli Allegati 1 e 2 sono parte integrante del presente accordo. Essi definiscono l'oggetto concordato, la tipologia e la finalità del trattamento, la tipologia dei dati personali, la categoria di interessati, i sub-Responsabili del trattamento impiegati (Allegato 1) nonché le misure tecniche e organizzative (Allegato 2).

1.2. Definizioni

Se non diversamente specificato nel presente documento, tutti i termini hanno il medesimo significato specificato nella Legge svizzera sulla protezione dei dati (LPD). I rimandi alla LPD implicano sempre anche un rimando all'Ordinanza sulla protezione dei dati (OPDa) e a qualsiasi altra disposizione del diritto sostanziale svizzero in materia di protezione dei dati.

Ai sensi del presente accordo, TWINT è Responsabile del trattamento e il contraente è il titolare del trattamento.

Per le finalità del presente accordo si applicano le seguenti definizioni:

Dati personali	Tutte le informazioni riguardanti una persona fisica determinata o determinabile, inserite dalle clienti e dai clienti del contraente nel campo della funzione supplementare «Adesivo con codice QR con informazioni sul pagamento» – come, ad esempio, nome e cognome, numero di telefono, indirizzo e-mail – e che rientrano nell'ambito di protezione del diritto in materia di protezione dei dati.
Titolare del trattamento	Persona fisica o giuridica che stabilisce la finalità e i mezzi del trattamento dei dati personali (qui: contraente).
Responsabile del trattamento	Persona fisica o giuridica che tratta i dati personali su incarico del titolare del trattamento (qui: TWINT Acquiring SA).
Sub-Responsabile del trattamento	(Sub)Responsabile del trattamento (azienda collegata o fornitore terzo) incaricato dal Responsabile del trattamento. Il sub-Responsabile del trattamento riceve dal Responsabile del trattamento i dati personali che, dopo la trasmissione, sono destinati a essere trattati esclusivamente a nome del titolare del trattamento in conformità alle istruzioni impartite da quest'ultimo e alle condizioni del sub-contratto.
Paese terzo	Ogni Paese che il Consiglio federale non considera un Paese sicuro con un livello di protezione dei dati adeguato.
Persona interessata o Interessato	Persona fisica determinata o determinabile i cui dati personali sono oggetto di trattamento.

2. Obblighi e responsabilità del titolare del trattamento

Il titolare del trattamento adotta autonomamente misure tecniche e organizzative adeguate per la protezione dei dati personali nella propria sfera di responsabilità – ad esempio all'interno dei propri sistemi, edifici, applicazioni/ambienti per i quali detiene la responsabilità operativa.

3. Obblighi del Responsabile del trattamento

3.1. Istruzioni del titolare del trattamento

TWINT si impegna e garantisce che tutti i dati personali ricevuti o messi a sua disposizione dal titolare del trattamento o derivati da tali dati vengano trattati esclusivamente su incarico ed esclusivamente per le finalità del titolare del trattamento così come definito nell'Allegato 1.

3.2. Obbligo di informazione in caso di violazione

TWINT informerà tempestivamente il titolare del trattamento e collaborerà con quest'ultimo qualora TWINT venga a conoscenza di una violazione della protezione dei dati personali del titolare del trattamento o nel caso in cui un'autorità statale avvii indagini contro TWINT o disponga misure contro TWINT nonché in qualsiasi altra circostanza in cui vengano effettuati accertamenti pertinenti da parte di tali autorità. Da questo tipo di notifiche non possono essere dedotte ammissioni di colpa o responsabilità da parte di TWINT.

3.3. Collaborazione

Su richiesta del titolare del trattamento, TWINT fornisce supporto a quest'ultimo in misura adeguata per l'elaborazione di richieste da parte di singole persone interessate o autorità di vigilanza in riferimento al trattamento di dati personali a cura di TWINT o a eventuali violazioni della protezione dei dati personali.

3.4. Accesso ai dati da parte di collaboratrici, collaboratori e sub-Responsabili del trattamento

TWINT adotta misure idonee a garantire l'affidabilità di tutte le collaboratrici, tutti i collaboratori, Responsabili e sub-Responsabili del trattamento che potrebbero avere accesso ai dati personali. TWINT garantisce che alle persone interessate summenzionate è proibito trattare i dati per finalità che esulano dalle istruzioni impartite dal titolare del trattamento o che costituiscono una violazione delle stesse. TWINT garantisce altresì di avere adeguatamente formato tali persone sulla protezione dei dati personali.

3.5. Misure tecniche e organizzative

Prima di procedere al trattamento, TWINT adotta misure tecniche e organizzative adeguate ai sensi della LPD al fine di proteggere i dati personali da trattamenti non autorizzati – ivi inclusi trattamenti non espressamente consentiti in virtù del presente accordo – da perdita o distruzione oppure danneggiamento accidentale. TWINT adotta misure organizzative a garanzia dell'affidabilità, dell'integrità, della disponibilità e della resilienza dei sistemi e dei servizi in relazione al trattamento dei dati. A tale riguardo è necessario tenere conto del livello tecnico, dei costi di implementazione, della tipologia, dell'entità e delle finalità del trattamento nonché della diversa probabilità e gravità del rischio per i diritti e le libertà degli interessati.

TWINT è autorizzata a modificare, in qualunque momento e senza preavviso, le misure tecniche e organizzative adottate in conformità all'Allegato 2, a condizione che venga mantenuto il livello di protezione concordato contrattualmente.

3.6. Cancellazione

TWINT si impegna a cancellare i dati personali qualora il titolare del trattamento lo richieda. Ove non sia possibile procedere a una cancellazione conforme alle norme in materia di protezione dei dati o a un'adeguata limitazione del trattamento dei dati, TWINT si impegna ad anonimizzare irreversibilmente i dati personali.

4. Trattamento in subappaltato

TWINT non affida il trattamento dei dati personali ad alcun sub-Responsabile del trattamento, eccetto nel caso in cui ciò risulti necessario o avvenga con il consenso del titolare del trattamento.

Prima di scegliere un sub-Responsabile del trattamento, TWINT ne verifica le misure adottate ai fini della sicurezza, della protezione dei dati e della riservatezza, al fine di garantire la protezione dei dati personali – e stipula con esso un contratto scritto (la forma elettronica si considera equivalente).

Un elenco dei sub-Responsabili del trattamento è disponibile nell'Allegato 1.

5. Trasferimento transfrontaliero

TWINT non trasferisce dati personali in Paesi al di fuori dell'UE e/o dello Spazio Economico Europeo (SEE) senza il preventivo consenso del titolare del trattamento.

Nel caso in cui si verifichi il trasferimento di dati personali trattati nell'ambito del presente accordo da un Paese dello Spazio Economico Europeo verso un Paese al di fuori dello Spazio Economico Europeo, il Responsabile del trattamento si accerta che i dati personali siano adeguatamente protetti. A tale scopo, per il trasferimento dei dati personali il Responsabile del trattamento impiega le clausole contrattuali standard UE modificate ai sensi della LPD.

6. Diritti delle persone interessate

Il titolare del trattamento è responsabile di garantire che le persone interessate possano esercitare il proprio diritto di informazione, rettifica, blocco, limitazione del trattamento, cancellazione o trasferimento dei dati come previsto dalla LPD. Il Responsabile del trattamento collaborerà appieno e senza indugio con il titolare del trattamento e metterà a disposizione del titolare del trattamento i servizi necessari per soddisfare le richieste delle persone interessate. Il Responsabile del trattamento inoltra prontamente al titolare del trattamento tutte le richieste ricevute direttamente, senza rispondere nel merito.

7. Disposizioni varie

Il presente accordo diventa automaticamente vincolante alla sottoscrizione di un contratto Payment e con l'utilizzo della relativa funzione supplementare. Termina automaticamente alla cessazione dei servizi erogati da TWINT per i quali è stato stipulato il presente accordo. Il titolare del trattamento può sospendere, in qualsiasi momento, il trasferimento di dati personali e/o il relativo trattamento. I diritti e gli obblighi dei contraenti derivanti dal presente accordo valgono a prescindere e fatti salvi altri diritti e doveri che i contraenti hanno o non hanno in virtù di altri accordi in essere. Il presente accordo non disciplina le conseguenze che possono scaturire dall'esercizio di un diritto e dall'adempimento di un obbligo derivanti dal presente accordo nel quadro di un accordo in essere tra i contraenti.

Il presente accordo è disciplinato dal diritto sostanziale svizzero ed è redatto in conformità a esso. Per qualsiasi controversia derivante dal presente accordo o correlata al presente accordo nonché qualsiasi violazione del presente accordo sono competenti esclusivamente i tribunali ordinari di Zurigo in Svizzera.

Allegato 1: Oggetto del trattamento

1. Finalità del trattamento

L'incarico assegnato dal titolare del trattamento a TWINT comprende le prestazioni seguenti:

- Integrazione delle transazioni con informazioni supplementari

2. Categorie di dati personali

Le seguenti categorie di dati personali sono regolarmente oggetto di trattamento:

- Dati sulla persona (nome e cognome)
- Dati relativi all'indirizzo (Via e N° civico, NPA, Località)
- Dati di contatto (indirizzo e-mail, numero di telefono)
- Causale (ad esempio numero di adesione, numero della fattura ecc.)

3. Categorie di persone interessate

Cerchia delle persone interessate dal trattamento dei dati:

- Clienti dei rivenditori

4. Elenco dei sub-Responsabili del trattamento

Per il trattamento dei dati richiesto dal titolare del trattamento, TWINT si avvale di servizi di terze parti che trattano i dati su incarico di TWINT (sub-Responsabili del trattamento).

Si tratta delle aziende seguenti:

- Swisscom (Svizzera) SA, Alte Tiefenaustrasse 6, 3050 Berna
- sumIT AG, Täfernstrasse 28, 5400 Baden (solo accesso ai sistemi TWINT)

Allegato 2: Misure tecniche e organizzative

TWINT SA ha implementato ed è tenuta a mantenere un programma di sicurezza dei dati e delle informazioni ragionevole sotto il profilo commerciale nonché conforme alle buone prassi del settore, comprendente misure tecniche e organizzative atte a garantire un adeguato livello di sicurezza dei dati personali (dei clienti) e che tenga in considerazione i rischi correlati al trattamento, in particolare derivanti da distruzione accidentale o illecita, perdita, alterazione o divulgazione non autorizzata di dati personali (dei clienti) o accesso agli stessi nonché la natura dei dati personali (dei clienti) oggetto di protezione, il livello tecnico e il costo di implementazione.

Il programma di sicurezza di TWINT SA deve comprendere le misure di seguito specificate.

Programma di sicurezza

a. **Sistema di gestione della sicurezza delle informazioni (ISMS) basato sulla norma ISO 27001**: TWINT SA è tenuta a mantenere un programma di sicurezza basato sui rischi ISMS al fine di gestire e proteggere in modo sistematico i dati aziendali e le informazioni dei propri clienti e partner.

b. **Comitato di gestione della sicurezza**: TWINT SA è tenuta a mantenere un Comitato di gestione della sicurezza costituito dalle banche emittenti e dall'acquirente risp. dagli acquirenti in rappresentanza degli shareholder di TWINT, il cui compito è sorvegliare il programma di sicurezza dell'azienda. Il Comitato deve riunirsi a cadenza mensile per valutare lo stato operativo dell'ISMS (ivi compresi esiti di audit, rischi, minacce, azioni correttive e altre questioni relative alla sicurezza) e promuovere il miglioramento costante della sicurezza a livello aziendale.

c. **Politica di risposta a incidenti di sicurezza**: TWINT SA è tenuta a mantenere politiche e procedure volte a (1) indagare e reagire a incidenti di sicurezza, ivi comprese procedure di valutazione della minaccia di vulnerabilità rilevanti o incidenti di sicurezza impiegando classificazioni e categorizzazioni definite degli incidenti e (2) adottare azioni correttive e di mitigazione degli eventi, comprese procedure di raccolta di artefatti e prove nonché misure correttive definite.

d. **Mantenimento della politica**: Tutte le politiche correlate alla sicurezza e alla riservatezza vanno documentate, regolarmente riesaminate, aggiornate e autorizzate dal Management al fine di assicurare che siano sempre in linea con le buone prassi, i requisiti legali e normativi nonché gli standard del settore.

e. **Comunicazione e coinvolgimento**: Le politiche e le procedure di sicurezza e riservatezza vanno pubblicate e comunicate in modo efficace a tutto il personale e ai subappaltatori di competenza. La sicurezza deve essere tema di discussione ai più alti livelli aziendali e i dirigenti esecutivi devono confrontarsi regolarmente sulle questioni inerenti alla sicurezza e sulle principali iniziative di sicurezza a livello aziendale.

Sicurezza del personale

a. **Verifica dei precedenti**: Il personale che ha accesso ai dati personali (dei clienti) o ai dispositivi su cui tali dati sono conservati deve essere sottoposto a una verifica dei precedenti (nella misura consentita dalle leggi e dai Regolamenti locali).

b. **Obblighi di riservatezza**: Il personale che ha accesso ai dati personali (dei clienti) deve essere contrattualmente vincolato da TWINT SA al mantenimento della riservatezza sui dati personali (dei clienti).

c. **Sensibilizzazione alla sicurezza**: Al momento dell'assunzione e, in seguito, a intervalli di tempo regolari, il personale va sensibilizzato sul tema della sicurezza tramite corsi di formazione sulle buone prassi e sui principi di riservatezza.

d. **Codice di condotta**: TWINT SA è tenuta a mantenere un codice di condotta aziendale e un programma di conformità al fine di garantire un comportamento etico e la conformità alle leggi e ai Regolamenti applicabili.

Sicurezza di terzi

a. **Attività di controllo**: TWINT è tenuta a mantenere politiche e procedure volte a garantire che tutti i nuovi fornitori, le applicazioni SaaS, le soluzioni di software IT e servizi IT siano sottoposti a ragionevoli controlli di due diligence al fine di accertarne la capacità di soddisfare i requisiti aziendali di sicurezza e conformità nonché gli obiettivi operativi.

b. **Obblighi contrattuali**: TWINT SA è tenuta a garantire che gli accordi contrattuali con i fornitori comprendano disposizioni in materia di riservatezza e segretezza idonee a tutelare gli interessi di TWINT SA e a garantire che TWINT possa adempiere ai propri obblighi di sicurezza e riservatezza nei confronti di clienti, partner, dipendenti, organismi di regolamentazione e altri stakeholder.

c. **Monitoraggio**: TWINT SA è tenuta a riesaminare periodicamente i propri fornitori terzi al fine di accertare che rispettino le condizioni contrattuali, compresi tutti i requisiti relativi a sicurezza e disponibilità.

Sicurezza fisica

a. **Sicurezza della sede aziendale**: TWINT SA è tenuta a mantenere un programma di sicurezza della sede aziendale comprendente la gestione degli ingressi agli edifici, delle videocamere CCTV e della sicurezza generale dei propri uffici nonché di un perimetro di sicurezza.

b. **Sicurezza dei centri dati aziendali**: I sistemi installati presso i locali di TWINT SA devono essere protetti in modo tale da impedire efficacemente qualunque accesso logico o fisico non autorizzato.

c. **Sicurezza dei centri dati**: TWINT SA impiega centri dati in ambiente Infrastructure as a Service (IaaS) per l'hosting di servizi infrastrutturali. TWINT SA valuta periodicamente le misure di sicurezza e conformità del fornitore dei centri dati impiegato. A sua volta, il fornitore segue le buone prassi del settore e rispetta numerose normative.

Sicurezza delle soluzioni

c. **Ciclo di vita dello sviluppo software (SDLC)**: TWINT SA è tenuta a mantenere una politica del ciclo di vita dello sviluppo software che definisca il processo in base al quale il personale crea prodotti e servizi sicuri e le attività svolte dal personale nelle varie fasi dello sviluppo (requisiti, progettazione, implementazione, verifica, documentazione e consegna).

d. **Sviluppo sicuro**: I team incaricati della gestione, dello sviluppo, della verifica e dell'impiego del prodotto seguono politiche e procedure di sviluppo di applicazioni sicure in linea con le pratiche normalmente in uso nel settore.

e. **Valutazione della vulnerabilità**: TWINT SA è tenuta a condurre periodicamente valutazioni della sicurezza, scansioni della vulnerabilità e test di penetrazione. Le problematiche relative ai prodotti individuate vanno valutate assegnando un punteggio di rischio e stabilendo le probabilità che l'evento si verifichi nonché le sue potenziali conseguenze. Le vulnerabilità vengono corrette sulla base della valutazione del rischio.

Sicurezza operativa

a. **Controlli degli accessi**: TWINT SA è tenuta a mantenere politiche, procedure e controlli logici al fine di definire le autorizzazioni di accesso dei dipendenti e di terzi, allo scopo di limitare gli accessi soltanto al personale autorizzato e impedire gli accessi non autorizzati.

b. **Privilegio minimo**: TWINT SA è tenuta a garantire che il personale abbia accesso esclusivamente ai sistemi e ai dati necessari per lo svolgimento delle rispettive funzioni. Soltanto il personale autorizzato può accedere fisicamente alle infrastrutture e alle apparecchiature. L'accesso alle risorse di produzione è limitato ai dipendenti che ne hanno necessità. I diritti di accesso vengono periodicamente rivisti e certificati per garantirne l'adeguatezza.

c. **Malware**: TWINT SA è tenuta a impiegare misure normalmente in uso nel settore al fine di rilevare ed eliminare malware, virus, ransomware, spyware e altri programmi dannosi che possono essere utilizzati per accedere illegalmente a informazioni o sistemi.

d. **Crittografia**: TWINT SA è tenuta a impiegare metodi di crittografia forti normalmente in uso nel settore al fine di proteggere i dati in transito e i dati a riposo nella misura adeguata al livello di sensibilità dei dati e ai rischi associati alla loro perdita. Tutti i computer portatili e qualsiasi altro dispositivo amovibile, compresi i supporti di backup, devono essere crittografati.

e. **Continuità aziendale e ripristino di emergenza (BCDR)**: TWINT SA è tenuta a mantenere piani BCDR formali periodicamente riesaminati e aggiornati al fine di garantire che i sistemi e i servizi di TWINT rimangano resilienti in caso di guasti dovuti, tra l'altro, a calamità naturali o guasti di sistema.

f. **Backup dei dati**: TWINT SA è tenuta a effettuare il backup dei dati e dei sistemi utilizzando posizioni di conservazione alternative in grado di permettere un ripristino in caso di guasto del sistema primario. Tutti i backup devono utilizzare una crittografia forte dei dati in transito e a riposo.

g. **Gestione delle modifiche**: TWINT SA è tenuta a mantenere politiche e procedure di gestione delle modifiche per pianificare, verificare, programmare, comunicare ed eseguire modifiche all'infrastruttura, ai sistemi, alle reti e alle applicazioni di TWINT.

h. **Sicurezza della rete**: TWINT SA è tenuta ad adottare tecnologie e controlli normalmente in uso nel settore al fine di garantire la sicurezza della rete, ivi compresi firewall, segmentazione della rete e sicurezza wireless. Le reti devono essere progettate e configurate al fine di limitare i collegamenti tra reti attendibili e non attendibili. La struttura e i controlli delle reti vanno riesaminati almeno a cadenza annuale.

i. **Segregazione dei dati**: TWINT SA è tenuta a garantire la rigorosa separazione dei sistemi e dei dati di produzione e non produzione.