Convention sur le traitement des données dans le cadre de la fonction supplémentaire TWINT «Autocollant code QR avec informations de paiement»

1. Champ d'application et définitions

1.1. Champ d'application

Le présent document complète le «Contrat de paiement pour l'acceptation de TWINT» conclu entre TWINT Acquiring SA (ci-après «TWINT» ou «sous-traitant») et le partenaire contractuel (ci-après «responsable des données»). La présente Convention s'applique aux données personnelles traitées par TWINT et d'éventuels sous-traitants ultérieurs en relation avec la mise à disposition de la fonction supplémentaire «Autocollant code QR avec informations de paiement». Elle ne s'applique pas à toute autre transaction au sein du système de paiement TWINT dans le cadre desquelles la fonction supplémentaire n'est pas utilisée, étant donné qu'aucune donnée personnelle n'y est traitée.

Les annexes 1 et 2 font partie intégrante de la présente Convention. Elles définissent l'objet convenu, la nature et le but du traitement des données, le type de données personnelles, la catégorie des personnes concernées, les sous-traitants ultérieurs impliqués (Annexe 1), ainsi que les mesures techniques et organisationnelles (Annexe 2).

1.2. Définitions

Sauf mention contraire, tous les termes ont le même sens que dans la loi suisse sur la protection des données (LPD). Une référence à la LPD implique toujours une référence à l'ordonnance relative à la LPD (OPDo) et à toute autre disposition du droit matériel suisse sur la protection des données.

Dans le cadre de la présente Convention, TWINT est sous-traitante et le partenaire contractuel est responsable des données.

Les dispositions suivantes s'appliquent aux fins du présent contrat:

Données personnelles	Toute information relative à une personne physique identifiée ou identifiable saisie par les clientes et les clients du partenaire contractuel dans le champ de la fonction supplémentaire «Autocollant code QR avec informations de paiement», comme p. ex. nom, numéro de téléphone, adresse e-mail, qui sont protégées par la loi sur la protection des données.
Responsable des données	Personne physique ou morale qui définit le motif et les moyens du traitement des données personnelles (ici: partenaire contractuel).
Sous-traitant	Personne physique ou morale qui traite des données personnelles sur mandat du responsable des données (ici: TWINT Acquiring SA).
Sous-traitant ultérieur	Sous-traitant (ultérieur) mandaté par le sous-traitant (entreprises liées ou tierces) qui obtient de la part du sous-traitant des données personnelles exclusivement destinées à être traitées au nom du responsable des données, conformément à ses instructions et aux conditions du contrat de sous-traitance.
Pays tiers	Tout pays non reconnu par le Conseil fédéral comme pays garantissant un niveau suffisant de protection des données.
Personne concernée	Personne physique identifiée ou identifiable à propos de laquelle des données personnelles sont traitées.

2. Obligations et responsabilité du responsable des données

Le responsable des données prend de manière autonome des mesures appropriées d'ordre technique et organisationnel pour la protection des données personnelles relevant de son domaine de compétence (p. ex. dans ses systèmes, ses bâtiments, ses applications/environnements, pour lesquels il assume la responsabilité opérationnelle).

3. Obligations du sous-traitant

3.1. Directives du responsable des données

TWINT s'engage et garantit qu'elle traitera exclusivement sur mandat et aux fins du responsable des données toute donnée personnelle obtenue ou mise à disposition par le responsable des données ou déduite de ces données, conformément aux dispositions de l'Annexe 1.

3.2. Obligation d'information en cas de violation

TWINT informe sans délai le responsable des données et collabore avec ce dernier dès que TWINT prend connaissance d'une violation de la protection des données personnelles du responsable des données ou si une autorité étatique ouvre une enquête contre TWINT ou ordonne des mesures contre TWINT, ainsi qu'en cas de toute autre enquête menée par de telles autorités. Aucune reconnaissance de faute ou de responsabilité de la part de TWINT ne peut être déduite de notifications de ce type.

3.3. Collaboration

Sur demande du responsable des données, TWINT soutient ce dernier de manière appropriée dans le traitement de requêtes de personnes concernées ou d'autorités de surveillance relatives au

TWINT Acquiring SA
Stauffacherstrasse 41
CH-8004 Zurich

traitement de données personnelles par TWINT ou à la violation de la protection des données personnelles.

3.4. Accès par des collaboratrices et collaborateurs ainsi que par des sous-traitants ultérieurs

TWINT prend des mesures appropriées afin de garantir la fiabilité de toutes les collaboratrices et de tous les collaborateurs, des mandataires ou des sous-traitants pouvant avoir accès aux données personnelles. TWINT garantit qu'il est interdit aux personnes en question de traiter les données en dehors ou à l'encontre des instructions du responsable des données. TWINT garantit en outre que ces personnes obtiennent une formation appropriée pour la protection des données personnelles.

3.5. Mesures techniques et organisationnelles

Préalablement au traitement des données, TWINT prend des mesures techniques et organisationnelles dans le sens de la LPD afin de protéger les données personnelles de traitements illicites, y compris les traitements non autorisés expressément par le présent contrat, de perte accidentelle, d'endommagement ou de destruction. TWINT prend des mesures organisationnelles garantissant la confidentialité, l'intégrité, la disponibilité et la capacité des systèmes et des services relatifs au traitement des données. À cet égard, il est tenu compte de l'état actuel de la technique, des coûts d'implémentation et du type, de l'étendue et des motifs du traitement des données ainsi que des différentes probabilités de survenance et de la gravité du risque pour les droits et les libertés des personnes concernées.

TWINT est habilitée à modifier à tout moment et sans préavis les mesures techniques et organisationnelles prises conformément à l'Annexe 2, pour autant que le niveau de protection convenu contractuellement soit respecté.

3.6. Suppression des données

TWINT s'engage à effacer les données personnelles si le responsable des données l'ordonne. Si une suppression conforme aux principes de la protection des données ou une limitation correspondante du traitement des données n'est pas possible, TWINT s'engage à anonymiser les données personnelles de manière irréversible.

4. Sous-traitance ultérieure

TWINT ne mandate aucun sous-traitant ultérieur pour le traitement des données personnelles, sauf en cas de nécessité ou avec le consentement du responsable des données.

Avant de choisir un sous-traitant ultérieur, TWINT vérifie les mesures mises en place par ce dernier pour garantir la sécurité, la protection des données personnelles et la confidentialité, et conclut avec lui un contrat écrit (la forme électronique est considérée comme équivalente).

Une liste des sous-traitants ultérieurs figure à l'Annexe 1.

5. Transfert transfrontalier

TWINT ne transmet aucune donnée personnelle dans des pays hors de l'EU et/ou de l'Espace économique européen (EEE) sans approbation préalable du responsable des données.

Si des données personnelles traitées dans le cadre de la présente Convention sont transmises depuis un pays de l'Espace économique européen vers un pays hors de l'Espace économique européen, le sous-traitant veille à la protection appropriée de ces données. À cet effet, le sous-traitant applique les clauses contractuelles types de l'UE pour le transfert de données personnelles modifiées, conformément à la LPD.

6. Droits de la personne concernée

Le responsable des données est chargé de veiller à ce que les personnes concernées puissent exercer leur droit d'information, de rectification, de blocage, ainsi que de limitation du traitement, de suppression ou de transfert des données conformément à la LPD. Le sous-traitant collaborera pleinement et sans délai avec le responsable des données et mettra à la disposition de ce dernier les services requis afin de répondre aux requêtes ou aux demandes des personnes concernées. Le sous-traitant transmet sans délai au responsable des données toutes les requêtes ou demandes obtenues directement, sans y répondre.

7. Divers

La présente Convention est automatiquement contraignante avec la conclusion d'un Contrat de paiement et l'utilisation de la fonction supplémentaire en question. Elle prend fin automatiquement avec l'arrêt des prestations fournies par TWINT pour lesquelles la présente Convention a été conclue. Le responsable des données peut suspendre à tout moment le transfert et/ou le traitement de données personnelles. Les droits et obligations des parties contractantes dans le cadre de la présente Convention s'appliquent nonobstant et sans préjudice aux autres droits et obligations incombant ou non aux parties contractantes sur la base d'autres accords existants. Le présent contrat ne régit pas les conséquences éventuelles de l'exercice d'un droit et du respect d'une obligation découlant du présent contrat sur un accord existant entre les parties contractantes.

Le présent contrat est soumis et interprété conformément au droit matériel suisse. Tout litige découlant du présent contrat, s'y rapportant ou résultant de la violation dudit contrat sera soumis exclusivement aux tribunaux ordinaires de Zurich.

TWINT Acquiring SA
Stauffacherstrasse 41
CH-8004 Zurich

Annexe 1: Objet du traitement du mandat

1. Motif du traitement

Le mandat du responsable des données à TWINT englobe les prestations suivantes:

- Enrichissement de transactions avec des informations supplémentaires

2. Catégories des données personnelles

Les catégories de données personnelles suivantes font régulièrement l'objet d'un traitement:

- Informations sur la personne (prénom, nom)
- Informations sur l'adresse (rue et numéro, code postal, lieu)
- Coordonnées (adresse e-mail, numéro de téléphone)
- Motif de paiement (p. ex. numéro de membre, numéro de facture, etc.)

3. Catégories des personnes concernées

Cercle des personnes concernées par le traitement des données:

- Clientes et clients des commerçants

4. Liste des sous-traitants ultérieurs

Pour le traitement de données sur mandat du responsable des données, TWINT peut avoir recours à des prestations de tiers qui traitent les données sur mandat de TWINT (sous-traitants ultérieurs)

Il s'agit des entreprises suivantes:

- Swisscom (Suisse) SA, Alte Tiefenaustrasse 6, 3050 Berne
- sumIT AG, Täfernstrasse 28, 5400 Baden (uniquement accès aux systèmes TWINT)

TWINT Acquiring SA
Stauffacherstrasse 41
CH-8004 Zurich

Annexe 2: Mesures techniques et organisationnelles

TWINT SA a implémenté et entretient un programme de sécurité des données et des informations commercialement raisonnable, conforme aux meilleures pratiques du secteur. Ce programme inclut des mesures techniques et organisationnelles visant à assurer un niveau de sécurité approprié pour les données personnelles (des clientes et clients), en tenant compte des risques présentés par le traitement, notamment la destruction, la perte et l'altération accidentelles ou illicites, la divulgation non autorisée ou l'accès aux données personnelles (des clientes et clients), ainsi que par la nature des données personnelles (des clientes et clients) à protéger, eu égard à l'état actuel de la technique et aux coûts d'implémentation.

Le programme de sécurité de TWINT SA inclut les mesures suivantes:

Programme de sécurité

a. **Système de gestion de la sécurité des informations basé sur la norme ISO27001 (ISMS):** TWINT SA entretient un programme de sécurité ISMS basé sur le risque afin de gérer et de protéger systématiquement les informations commerciales de l'organisation, ainsi que les informations de sa clientèle et de ses partenaires.

b. **Comité directeur sécurité**: TWINT SA entretient un Comité directeur sécurité composé des banques émettrices et de l'acquéreur ou des acquéreurs représentant les actionnaires de TWINT, dans le but de superviser le programme de sécurité de l'entreprise. Ce Comité se réunit tous les mois afin d'examiner le statut opérationnel de l'ISMS (y compris les résultats des audits, les risques, les menaces, les mesures correctives et d'autres questions relatives à la sécurité) et d'apporter continuellement des améliorations en matière de sécurité à l'ensemble de l'entreprise.

c. **Politique de gestion des incidents de sécurité**: TWINT SA applique des politiques et des procédures pour (1) enquêter sur et répondre aux incidents de sécurité, y compris des procédures pour évaluer la menace des vulnérabilités ou d'incidents de sécurité, en appliquant des classements et des catégories d'incidents prédéfinis et (2) mettre en place des mesures correctives et d'atténuation en cas d'événement, y compris des procédures de recueil de documents et de preuves, ainsi que des mesures correctives prédéfinies.

d. **Maintenance de la politique**: Toutes les politiques relatives à la sécurité et à la confidentialité sont documentées, revues et mises à jour régulièrement et approuvées par la Direction afin de garantir leur conformité aux meilleures pratiques, aux exigences légales et de régulation, ainsi qu'aux standards du secteur.

e. **Communication et engagement**: Les politiques et les procédures de sécurité et de confidentialité sont publiées et communiquées efficacement à l'ensemble du personnel et aux sous-traitants concernés. Les questions de sécurité sont abordées aux plus hauts niveaux de l'entreprise. La Direction discute régulièrement des questions de sécurité et met en œuvre des initiatives en matière de sécurité concernant l'ensemble de l'entreprise.

Personnel en charge de la sécurité

a. **Vérification des antécédents**: Le personnel ayant accès aux données personnelles (des clientes et clients) ou à l'équipement dans lequel ces données sont stockées fait l'objet d'une vérification des antécédents (conformément à la législation et à la réglementation locales).

b. **Obligations de confidentialité**: Le personnel ayant accès aux données personnelles (des clientes et clients) est soumis à une obligation contractuelle contraignante avec TWINT SA d'assurer la confidentialité des données personnelles (des clientes et clients).

c. **Formation de sensibilisation à la sécurité**: Le personnel reçoit une formation dès l'embauche ainsi que des formations ultérieures régulières concernant les meilleures pratiques en matière de sécurité et les principes de confidentialité.

d. **Code de conduite**: TWINT SA entretient une politique de code de conduite professionnelle et un programme de conformité afin d'assurer un comportement éthique et la conformité avec les lois et les réglementations applicables.

Sécurité assurée par des tiers

a. **Vérification**: TWINT applique des politiques et des procédures afin de s'assurer que tout nouveau fournisseur, toute nouvelle application SaaS, tout nouveau logiciel informatique et toute nouvelle solution de service fasse l'objet d'une diligence raisonnable, dans le but de confirmer leur capacité à satisfaire aux exigences de l'entreprise en matière de sécurité et de conformité et à répondre aux objectifs de l'entreprise.

b. **Obligations contractuelles**: TWINT SA veille à ce que les accords contractuels avec les fournisseurs incluent des dispositions en matière de confidentialité et de respect de la sphère privée appropriées pour protéger les intérêts de TWINT SA et pour assurer que TWINT puisse remplir les obligations de sécurité et de confidentialité envers ses clientes et clients, ses partenaires, ses employées et employés, les régulateurs et les autres parties prenantes.

c. **Surveillance**: TWINT SA réexamine périodiquement les fournisseurs tiers existants afin de s'assurer que le fournisseur respecte les dispositions contractuelles, y compris les exigences en matière de sécurité et de disponibilité.

Sécurité physique

a. **Sécurité des installations de l'entreprise**: TWNIT SA applique un programme de sécurité des installations qui gère les entrées des bâtiments, la vidéosurveillance et la sécurité générale de ses locaux, y compris un périmètre de sécurité.

b. **Sécurité du centre de données de l'entreprise**: Les systèmes installés dans les locaux de TWINT SA sont protégés de sorte à prévenir efficacement tout accès logique et physique illicite.

c. **Sécurité du centre de données**: TWINT SA tire parti de centres de données Infrastructure as a Service (IaaS) pour l'hébergement de services d'infrastructure. TWINT SA examine régulièrement les mesures de sécurité et de conformité du fournisseur de centre de données. Le fournisseur applique les meilleures pratiques du secteur et respecte un certain nombre de standards.

Sécurité des solutions

c. **Cycle de vie des systèmes et des logiciels (SDLC)**: TWINT applique une politique de cycle de vie des systèmes et des logiciels qui définit le processus par lequel le personnel crée des produits et de services sûrs, ainsi que les activités que le personnel est tenu d'effectuer lors des différents stades du développement (exigences, design, implémentation, vérification, documentation et livraison).

d. **Sécurité du développement**: Les équipes de gestion, de développement, d'essai et de déploiement des produits appliquent des politiques et des procédures de développement conformes aux standards de l'industrie.

e. **Examen de la vulnérabilité**: TWINT SA effectue régulièrement des examens de sécurité, des analyses de la vulnérabilité et des tests d'intrusion. Tout problème lié aux produits est évalué en termes d'impact de risque et de probabilité, ainsi qu'en termes de conséquences potentielles en cas de survenance. Les vulnérabilités sont corrigées sur la base du risque évalué.

Sécurité opérationnelle

a. **Contrôles de l'accès**: TWINT SA applique des politiques, des procédures et des contrôles logiques pour l'établissement d'autorisations d'accès pour les employées et employés et des tierces parties afin de limiter l'accès à du personnel autorisé et de prévenir tout accès non autorisé.

b. **Droit d'accès minimal**: TWINT SA veille à ce que le personnel n'ait accès qu'à des systèmes et des données nécessaires à l'exercice de leur fonction. Seul le personnel autorisé a un accès physique à l'infrastructure et aux équipements; l'accès aux ressources de production est limité au personnel ayant besoin d'un tel accès. Les droits d'accès sont réexaminés et validés régulièrement afin de garantir que l'accès soit approprié.

c. **Logiciels malveillants**: TWINT SA applique des mesures standard de l'industrie afin de détecter et de combattre les logiciels malveillants, les virus, les rançongiciels, les logiciels espions ou tout autre programme intentionnellement malveillant qui pourrait être utilisé pour obtenir un accès non autorisé aux informations ou aux systèmes.

d. **Cryptage**: TWINT SA utilise les méthodes de cryptage puissantes correspondant aux standards du secteur afin de protéger les données en cours de transmission et au repos de manière appropriée au caractère sensible des données et aux risques liés à la perte. Tous les ordinateurs portables et tout autre support amovible, y compris les sauvegardes, sont cryptés.

e. **Continuité des opérations et reprises après un sinistre (BCDR)**: TWINT SA applique des plans formels BCDR qui sont régulièrement revus et mis à jour afin d'assurer la résilience des systèmes et des services TWINT en cas de défaillance, y compris les catastrophes naturelles ou les pannes de système

f. **Sauvegardes des données**: TWINT SA sauvegarde les données et les systèmes en utilisant des sites de conservation alternatifs, ce qui permet une restauration en cas de défaillance du système primaire. Toutes les sauvegardes sont puissamment cryptées lors de leur transmission et au repos.

g. **Gestion des changements**: TWINT SA applique des politiques et des procédures de gestion des changements afin de planifier, tester, agender, communiquer et exécuter des changements à l'infrastructure, aux systèmes, aux réseaux et aux applications de TWINT.

h. **Sécurité des réseaux**: TWINT SA implémente des technologies et des contrôles correspondant au standards de l'industrie afin de protéger la sécurité des réseaux, y compris des pare-feu, une segmentation des réseaux et la sécurité sans fil. Les réseaux sont conçus et configurés de manière à restreindre les connections entre les réseaux fiables et non fiables. La conception et les contrôles des réseaux sont revus au moins une fois par an.

i. **Ségrégation des données**: TWINT SA veille à ce que les données de production et de non-production soient strictement ségréguées.

TWINT Acquiring SA
Stauffacherstrasse 41
CH-8004 Zurich