RAIFFEISEN

Informativa particolare sulla protezione dei dati di Raiffeisen per le carte e per l'app Raiffeisen TWINT («mezzo di pagamento»)

1 Considerazioni generali

La presente Informativa particolare sulla protezione dei dati di Raiffeisen per le carte **e per l'app Raiffeisen TWINT** (nel prosieguo «**Informativa sulla protezione dei dati carte**») fornisce ulteriori informazioni rispetto alla Dichiarazione generale sulla protezione dei dati del Gruppo Raiffeisen (nel prosieguo «**Dichiarazione generale sulla protezione dei dati**», consultabile su raiffeisen.ch/informazioni-legali o su richiesta) in merito al trattamento dei dati personali (nel prosieguo «**dati personali**») in relazione alle carte emesse dalla Banca Raiffeisen (nel prosieguo «**Banca**») come, in particolare, le carte di credito e Prepaid Raiffeisen e le carte di credito Business di Raiffeisen (nel prosieguo collettivamente «**carte di credito**»), le carte di debito Raiffeisen (nel prosieguo «**carte di debito**») nonché, ove applicabile, anche le carte di conto Raiffeisen (nel prosieguo «**carte di conto**») e l'app Raiffeisen TWINT (nel prosieguo «app TWINT»). Laddove, nel prosieguo, si faccia riferimento alle «**carte**», con ciò sono da intendersi tutte le carte – ossia le carte di credito, di debito, Prepaid e di conto nonché le carte di credito Business – singolarmente e anche collettivamente. Laddove, invece, si faccia riferimento ai «mezzi di pagamento», con ciò sono da intendersi oltre alle carte, anche l'app TWINT. Gli aspetti rappresentati nella presente Informativa sulla protezione dei dati carte possono assumere un'importanza diversa e di diversa entità per le carte di credito, le carte di debito o le carte di conto, nonché l'app TWINT, in particolare a fronte delle diverse possibilità di utilizzo, della portata dei servizi forniti, dei processi, delle infrastrutture e dei fornitori dei servizi. Le seguenti considerazioni si applicano anche alle aziende che prevedono di usufruire di carte di credito Business.

La presente Informativa sulla protezione dei dati carte non limita in alcun modo la Dichiarazione generale sulla protezione dei dati. Parimenti, la Dichiarazione generale sulla protezione dei dati non limita in alcun modo la presente Informativa sulla protezione dei dati carte. Entrambe le informative sulla protezione dei dati forniscono vicendevolmente informazioni integrative e si applicano in via integrativa alle «Condizioni per l'utilizzo delle carte di credito Raiffeisen», alle «Condizioni per l'utilizzo delle carte di credito Business di Raiffeisen», alle «Condizioni per l'utilizzo delle carte di debito Raiffeisen», alle «Condizioni per l'utilizzo delle carte di conto Raiffeisen», nonché alle «Condizioni per l'utilizzo dell'app Raiffeisen TWINT» e alle «Condizioni generali di affari» nella versione vigente (consultabili su raiffeisen.ch/i/downloadcenter, raiffeisen.ch/informazioni-legali o disponibili su richiesta presso la Banca). Anche alle carte si applicano altresì i regolamenti di base della Banca (consultabili su raiffeisen.ch/informazioni-legali o disponibili su richiesta presso la Banca).

2 Raccolta dei dati; categorie di dati

In particolare, la Banca elabora dati personali che le vengono comunicati dal titolare della carta rispettivamente dall'utente dell'app TWINT (di seguito singolarmente «titolare del mezzo di pagamento» e congiuntamente «titolari del mezzo di pagamento») (tra cui nell'ambito della visita o dell'utilizzo di offerte online e offline come, in particolare, siti web e app), che vengano resi noti nell'ambito della relazione d'affari, che siano pubblicamente accessibili (ad es. dati del registro fondiario, dati del registro di commercio, dati del registro delle esecuzioni, dati di geolocalizzazione, dati raccolti da Internet, dai social media e dalla stampa), che siano disponibili presso le autorità, che possano essere ottenuti da terzi (ad es. agenzie di informazione sul credito, dati sulla solvibilità o di rating, gestori di indirizzi) o che derivino dal trattamento di tali dati.

Con riferimento ai dati oggetto di trattamento (che la Banca ottiene autonomamente o da terzi) si tratta, in particolare, di informazioni sulla persona (ad es. dati di contatto, indirizzi, dati personali, indirizzi e-mail, numeri di telefono, età, sesso, luogo di domicilio, dati di legittimazione e di accesso), di dati contrattuali (ad es. dati di credito e di prodotto), di dati finanziari (ad es. dati di scoring, di rating e di solvibilità, dati patrimoniali e di prodotto), di dati relativi alle transazioni (ad es. pagamenti con carta, punti di accettazione, beneficiari/mandanti di pagamenti P2P, importi dei pagamenti, tipologia di impieghi della carta, altri dati relativi ai pagamenti), di dati relativi a prestazioni a valore aggiunto di TWINT (ad esempio campagne, carte clienti, funzioni di partner), di dati di interazione (ad es. utilizzo di app, visite ai siti web e ai canali di social media della Banca o del Gruppo Raiffeisen) nonché di dati riguardanti le esigenze della clientela (ad es. canali di contatto preferiti, interesse a prodotti e servizi), di dati raccolti dai siti Internet di aziende e dei profili creati da tutti questi dati relativi agli interessi per prodotti e servizi e ad altri aspetti concernenti il titolare del mezzo di pagamento.

Altre categorie di dati personali sono: dati in relazione a procedimenti o indagini di autorità, tribunali, associazioni e organismi (come, ad es., un organismo di autodisciplina) e ad altre istanze, dati estratti dai registri pubblici, dati ottenuti da agenzie di informazione sul credito, da gestori di indirizzi, dati sulla solvibilità o di rating ottenuti da terzi, dati ottenuti da banche, da assicurazioni, da partner commerciali del

Gruppo Raiffeisen, da partner di distribuzione e da altri partner contrattuali del Gruppo Raiffeisen (ad es. in relazione a prodotti e a servizi di o per titolari del mezzo di pagamento, concernenti, in particolare, acquisti avviati o avvenuti, pagamenti, reclami ecc.), dati riguardanti la professione e altre attività del titolare del mezzo di pagamento. (ad es. hobby, attività associative ecc.), dati trasmessi da persone vicine al titolare del mezzo di pagamento, come il datore di lavoro, i familiari, i consulenti, gli avvocati ecc. (in particolare, per la gestione dei contratti), procure, riferimenti e dati ottenuti a seguito di contatti del titolare del mezzo di pagamento con terzi (ad es. verbali, note agli atti ecc.), dati relativi al rispetto delle prescrizioni normative come, ad esempio, la lotta contro il riciclaggio di denaro, le restrizioni alle esportazioni, dati ottenuti dalla stampa e dai media nel loro complesso, da Internet, dati sociodemografici, dati di geolocalizzazione, dati concernenti gli interessi del titolare del mezzo di pagamento (ad es. per il marketing), dati ottenuti a seguito dell'utilizzo di siti web e di app (ad es. indirizzo IP, indirizzo MAC di prodotti elettronici come dispositivi mobili, computer ecc., informazioni inerenti a tali dispositivi e alle relative impostazioni, cookie, data, ora e durata di una visita, contenuti consultati, funzioni utilizzate, ordinazioni effettuate o tentate, siti web di riferimento e informazioni sulla posizione).

Sono inoltre oggetto di trattamento da parte della Banca i dati menzionati nella Dichiarazione generale sulla protezione dei dati e i dati citati di seguito al punto 3.

La Banca elabora altresì i dati personali di persone associate a una relazione cliente (ad es. aventi diritto economico, partner, beneficiari/mandanti di pagamenti P2P), che essa ha ricevuto o ha ottenuto dal titolare del mezzo di pagamento o da terzi. Ove i dati siano stati ottenuti dal titolare del mezzo di pagamento, questi deve assicurarsi che tali persone siano a conoscenza della presente Informativa sulla protezione dei dati carte; il titolare del mezzo di pagamento comunica i loro dati personali alla Banca solo se autorizzato e se i dati corrispondenti sono corretti.

3 Finalità di trattamento e basi giuridiche

La Banca elabora dati personali in linea con le disposizioni applicabili in materia di protezione dei dati e con le finalità riportate di seguito e nella Dichiarazione generale sulla protezione dei dati a proprio nome o a nome di terzi, in particolare nell'interesse della Banca, del Gruppo Raiffeisen o, qualora sia necessaria una causa di giustificazione, conformemente alle cause di giustificazione anch'esse riportate di seguito:

- Per la verifica, la stipula, l'adempimento e l'attuazione dei contratti: la Banca elabora dati personali in particolare per la verifica delle richieste di carta, per l'esecuzione delle stipulazioni dei contratti e nell'ambito dell'adempimento dei contratti. Rientrano in tale sfera anche l'esecuzione di un'analisi del rischio di credito e del comportamento (ivi compresi l'analisi del rischio di truffa e lo scoring), la gestione e lo sviluppo delle relazioni cliente (ivi compresi il servizio clientela, il supporto e lo svolgimento di eventi per i clienti) e la comunicazione con i clienti.
- Per l'erogazione dei servizi correlati alle carte, in particolare l'esecuzione delle transazioni e l'amministrazione delle carte. Rientra in tale sfera anche la divulgazione dei dati relativi alle transazioni ai terzi coinvolti nell'esecuzione della transazione (cfr. anche il punto 6.3).
- Per l'erogazione di servizi correlati all'app TWINT, ossia in particolare la gestione dei pagamenti (ivi inclusa la funzione «Pagare dopo») e le prestazioni a valore aggiunto (ad esempio campagne, carte clienti, funzioni di partner). Rientra in tale sfera anche la divulgazione dei dati 'ai fornitori terzi e partner coinvolti nell'erogazione di prestazioni, vale a dire al gestore del sistema di pagamento TWINT SA e al fornitore della funzione «Pagare dopo».
- Per la salvaguardia degli interessi della Banca o di un terzo: la Banca elabora i dati personali anche per la salvaguardia dei propri interessi legittimi o degli interessi legittimi di un terzo. Gli interessi della Banca sono molteplici e comprendono, in particolare, i seguenti:
  - continuo miglioramento e sviluppo dei prodotti, delle prestazioni, dei servizi e delle app offerti;
  - comprensione del comportamento dei clienti, delle richieste e delle esigenze, svolgimento di studi di mercato nonché creazione di profili cliente corrispondenti (ad es. sulla base dell'utilizzo dei mezzi di pagamento per determinate categorie di punti di accettazione o sulla base della frequenza di utilizzo dei mezzi di pagamento per acquisti via Internet);
  - svolgimento di attività pubblicitarie e di marketing, ivi inclusa la creazione di profili di marketing, ad es. tramite l'invio di una newsletter (ivi inclusa l'analisi della presa di conoscenza) e/o di materiale promozionale, gestione della pubblicità online e di «campagne TWINT»;
  - gestione di un'assistenza ai clienti efficiente ed efficace, mantenimento dei contatti e di altra comunicazione con i titolari del mezzo di pagamento al di fuori della gestione dei contratti;
  - garanzia dell'attività e dell'infrastruttura (in particolare infrastruttura IT e in generale offerte online, distributori automatici ecc.);
  - salvaguardia della sicurezza dei dati, in particolare per la protezione da perdita, distruzione e accesso non autorizzato ai dati personali, ai segreti del titolare del mezzo di pagamento e alle parti di sostanza della Banca;
  - amministrazione, gestione, contabilità e archiviazione;
  - rispetto dei requisiti legali e regolamentari applicabili alla Banca nonché delle disposizioni interne della Banca;
  - nell'ambito della gestione dei rischi e per la prevenzione e l'individuazione di transazioni fraudolente, ulteriori reati e altro comportamento illecito;
  - protezione di persone e valori (ad es. videosorveglianza, registrazioni);
  - difesa dalle azioni legali avviate nei confronti della Banca;
  - garanzia dei diritti della Banca nonché realizzazione di garanzie del titolare del mezzo di pagamento o di terzi;
  - incasso di crediti vantati dalla Banca nei confronti del titolare del mezzo di pagamento;
  - gestione dei reclami del titolare del mezzo di pagamento nei confronti della Banca in pubblico o nei confronti delle centrali sul territorio nazionale o all'estero;
  - preparazione ed esecuzione della vendita o dell'acquisizione di settori di attività, aziende o rami di aziende

e altre transazioni aziendali e il trasferimento dei dati personali a ciò connessi;
  - rivendicazione e realizzazione di diritti e pretese, difesa da pretese legali, controversie o reclami nonché lotta contro la condotta fraudolenta, avvio di accertamenti e procedimenti, in caso di richieste delle autorità, prevenzione di danni e perdite nonché risposta a richieste delle autorità.
- Per il rispetto di obblighi legali: la Banca effettua trattamenti dei dati nell'ambito dei propri obblighi di legge (ai sensi del diritto nazionale ed estero), in particolare per la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo, per la verifica della capacità creditizia del titolare della carta, per la conservazione di determinati dati, per la risposta a richieste delle autorità.
- Sulla base del consenso del titolare del mezzo di pagamento, laddove sia necessario un consenso: la Banca elabora i dati personali anche sulla base del consenso del titolare del mezzo di pagamento, che viene presentato al titolare del mezzo di pagamento ad es. in occasione della visita di un sito web, all'atto della richiesta e all'atto della stipula di un rapporto contrattuale o nell'ambito dell'utilizzo del rispettivo servizio, di servizi o di un'app. I relativi consensi sono disponibili, in particolare, nelle condizioni applicabili delle carte o nelle condizioni dell'app TWINT. Al riguardo, il trattamento dei dati avviene per le finalità indicate nel consenso.

4 Singoli trattamenti concreti di dati personali fondati sulle basi giuridiche riportate al punto 3

4.1 Elaborazione della richiesta di carta

Con la richiesta di carta, il titolare della carta trasmette dati personali alla Banca.

Per la verifica della richiesta di carta (inclusa la verifica della solvibilità risp. della capacità creditizia) la Banca elabora, in particolare, i dati di contatto, la lingua, il sesso, la data di nascita, i dati di solvibilità nonché i dati con riferimento a una verifica ai fini della lotta contro il riciclaggio di denaro (ad es. informazioni relative alla professione e all'avente diritto economico).

I dati personali del richiedente ovvero del titolare della carta possono essere elaborati e associati anche insieme ai dati che la Banca ha ricevuto o ha raccolto autonomamente da altre fonti.

In particolare, la Banca riceve o ottiene dati dalle autorità, da banche dati/agenzie di informazioni (World Check, Teledata/CRIF, Creditreform, Zefix, tel.search.ch ecc.), da servizi di informazione sul credito come ad es. la Centrale per informazioni di credito (nel prosieguo «ZEK») e la centrale d'informazione per il credito al consumo (nel prosieguo «IKO»), da datori di lavoro, da registri come ad es. local.ch, da registri di commercio, dai media nonché in generale da Internet.

4.2 Utilizzo della carta o dell'app TWINT

In caso di impiego della carta o dell'app TWINT, la Banca elabora, in particolare, i seguenti dati:
- dati che vengono comunicati alla Banca nel corso della durata del rapporto contrattuale o che la Banca raccoglie autonomamente (ad es. modifiche di nome e cognome, modifiche dell'avente diritto economico, estratti patrimoniali, dati di altre persone nel caso di un evento assicurato ecc.);
- dati relativi alle transazioni (dati concernenti i dettagli dei servizi e dei prelevamenti di contanti). Al riguardo si tratta, in particolare, delle seguenti informazioni:
  - punto di accettazione;
  - beneficiari/mandanti di pagamenti P2P (in particolare i relativi numeri di cellulare);
  - importo della transazione;
  - luogo della transazione;
  - data della transazione;
  - dati supplementari, come ad es. il tipo di impiego della carta (ad es. online, in assenza di contatti), il numero dei tentativi errati di immissione del NIP o la valuta selezionata.
- Per determinate transazioni, ad esempio per l'acquisto di biglietti aerei, per noleggi di automobili e per la prenotazione di pernottamenti (in hotel) nonché per pagamenti tra privati, tali informazioni sono più dettagliate (ad es. dati relativi all'oggetto dell'acquisto, al venditore, all'acquirente ovvero dati della persona che ha impiegato la carta o l'app TWINT, come ad es. i suoi dati personali, il suo indirizzo e-mail, il numero di telefono ecc.). Pertanto, in casi specifici la Banca è a conoscenza ad es. di ciò che il titolare del mezzo di pagamento ha acquistato con il mezzo stesso;
- nell'ambito della gestione dei rischi e della prevenzione delle attività fraudolente la Banca elabora, in particolare, dati di base e relativi alle transazioni affinché sia possibile valutare e coprire costantemente i rischi di credito della Banca (ad es. per la fissazione di un limite di credito adeguato);
- per il rispetto di leggi, di direttive e di raccomandazioni delle autorità e di regolamentazioni interne, ad es. per la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo e per l'adempimento di obblighi di controllo e di comunicazione di diritto tributario; inoltre, per finalità di archiviazione, la Banca elabora, in particolare, dati di base, finanziari e relativi alle transazioni del titolare del mezzo di pagamento;
- nell'ambito di un riaddebito (chargeback), la Banca riceve regolarmente dal punto di accettazione interessato, tramite l'acquirer, informazioni dettagliate in merito alla transazione, inclusi dati personali (ad es. indirizzo e-mail e numero di telefono del titolare del mezzo di pagamento, dati relativi all'oggetto dell'acquisto ecc.);
- qualora la Banca usufruisca di servizi aggiuntivi di organizzazioni di carte, essa ha la possibilità di ottenere dati relativi ai giustificativi e dati supplementari dal punto di accettazione («Consumer Clarity Features»);
- dai dati relativi alle transazioni la Banca trae eventualmente ampie conclusioni sulla condotta del titolare del mezzo di pagamento (ad es. luogo di domicilio e di lavoro, stato di salute, situazione finanziaria, comportamento nel tempo libero, comportamento sociale e altre informazioni);
- dati associati all'utilizzo della carta per pagamenti online come ad esempio l'accesso a Internet (indirizzo IP), i dispositivi utilizzati, l'impostazione della lingua del browser,

l'impronta digitale (device fingerprint) o l'effettuazione di un'autenticazione aggiuntiva da parte del titolare del mezzo di pagamento;
- dati correlati alle prestazioni a valore aggiunto TWINT (ad es. campagne, carte clienti, funzioni di partner) o alla funzione «Pagare dopo»;
- dati provenienti da altre fonti (ad es. dalla ZEK e dall'IKO, da autorità, da agenzie di informazioni, dal datore di lavoro, da banche dati pubblicamente accessibili o da registri come local.ch o dal registro di commercio) nell'ambito della finalità corrispondente;
- nell'ambito delle prescrizioni normative sulla correttezza dei dati nonché per garantire la comunicazione inerente alla relazione d'affari con titolari del mezzo di pagamento, la Banca può rendere noti i dati di base e relativi all'indirizzo dei titolari del mezzo di pagamento alla Posta o ad altri responsabili del trattamento (fornitori di servizi) ai fini dell'armonizzazione dell'indirizzo.

4.3 Pagamento in assenza di contatti con carte fisiche

La Banca consente al titolare della carta di pagare in assenza di contatti con le carte (eccetto che con le carte di conto). Ciò avviene tramite un chip integrato nella carta o in un dispositivo mobile, il quale è dotato di un'antenna. Tale antenna utilizza la tecnologia Near Field Communication (NFC) per condividere informazioni tra il terminale di pagamento e la carta o un dispositivo mobile.

Sul chip nonché sulla banda magnetica della carta non vengono memorizzati dati relativi alle transazioni (come ad es. dati relativi al punto di accettazione nonché la data o l'importo di una transazione) o dati personali del titolare della carta (come ad es. cognome, nome o indirizzo). Sia sul chip che sulla banda magnetica della carta sono memorizzati il numero della carta (Primary Account Number), la data di scadenza nonché i dati di verifica della carta, i quali sono necessari per l'esecuzione della transazione e l'impiego della carta.

I titolari di carta i quali, nonostante i vantaggi del pagamento in assenza di contatti, desiderino rinunciare a tale funzionalità, possono disattivarla autonomamente con l'ausilio dei servizi online o chiedere una disattivazione alla Banca. Il titolare della carta prende atto e comprende che la disattivazione del pagamento in assenza di contatti non comprende alcuna riduzione dei dati memorizzati sul chip o sulla banda magnetica. In caso di utilizzo della carta è impedita tecnicamente soltanto la funzione del pagamento in assenza di contatti.

4.4 Memorizzazione delle carte per il Mobile Payment

In caso di memorizzazione delle carte (eccetto delle carte di conto) per le soluzioni di Mobile Payment, la Banca raccoglie, in particolare, i seguenti dati:
- informazioni sull'utilizzo di Mobile Payment, come ad es. l'attivazione o la disattivazione delle carte e l'utilizzo delle carte per il Mobile Payment;
- informazioni sull'importo della transazione;
- informazioni sull'utilizzo della carta, data della transazione, tipo di verifica.

In caso di utilizzo di una soluzione di Mobile Payment di un fornitore terzo, anche il fornitore terzo può raccogliere ed elaborare i dati personali del titolare della carta. A seconda dell'offerta, tra questi rientrano ad es. il nome e il cognome, il numero della carta e anche i dati relativi alle transazioni. Il fornitore terzo riceve questi ultimi regolarmente dalla Banca.

In caso di memorizzazione della carta, i dati relativi al cliente e ai dispositivi vengono condivisi con le organizzazioni internazionali di carte per l'amministrazione della carta, ai fini della verifica dell'identificazione, ai fini della lotta contro gli abusi e le attività fraudolente, ai fini del rispetto delle disposizioni legali e ai fini dell'esecuzione e della visualizzazione delle transazioni. Per motivi di sicurezza, la trasmissione del numero della carta (Primary Account Number) viene tokenizzata.

La Banca elabora i dati del titolare della carta in relazione alla memorizzazione delle carte per le soluzioni di Mobile Payment per le seguenti finalità:
- per la decisione in merito all'autorizzazione della carta per Mobile Payment;
- per l'attivazione, la disattivazione e l'aggiornamento delle carte per Mobile Payment;
- per impedire l'uso illecito delle carte aggiunte;
- per la comunicazione con un eventuale fornitore terzo di una soluzione di Mobile Payment.

La Banca e il fornitore terzo della soluzione di Mobile Payment sono responsabili reciprocamente indipendenti e autonomi in relazione all'elaborazione dei dati. Il fornitore terzo elabora i dati sul territorio nazionale e all'estero per le proprie finalità in conformità alle proprie condizioni d'uso e alle proprie informative sulla protezione dei dati. La Banca non ha alcuna influenza sull'utilizzo e sulla protezione dei dati da parte del fornitore terzo. Tutte le contestazioni al riguardo dovranno essere indirizzate direttamente al fornitore terzo.

4.5 Protocollo di sicurezza aggiuntivo («3-D Secure») per i pagamenti online

In caso di utilizzo di 3-D Secure la Banca raccoglie, in particolare, i seguenti dati:
- informazioni sul punto di accettazione, sulla transazione e sulla relativa esecuzione nonché sulla conferma della transazione con 3-D Secure;
- informazioni in relazione ai dispositivi mobili che sono stati utilizzati per la transazione e la conferma;
- informazioni in relazione all'accesso a Internet o alla rete di telefonia mobile, come ad es. indirizzo IP, nome dell'access provider, impostazioni del browser, impronta digitale (device fingerprint) ecc.

4.6 Sorveglianza delle transazioni

In caso di impiego del mezzo di pagamento, i dati relativi alle transazioni vengono trasmessi alla Banca dai punti di accettazione, ossia ad esempio dal negozio presso il quale viene impiegato il mezzo di pagamento o da un distributore automatico. In seguito le transazioni vengono verificate, approvate dalla Banca e addebitate al titolare del mezzo di pagamento.

In caso di prelevamento di contanti presso distributori automatici nazionali con una carta di debito, la trasmissione avviene tramite Direct Debit (richiesta di autorizzazione e addebito diretto del conto bancario corrispondente del titolare della carta).

In fase di approvazione delle transazioni viene verificato se sussistono indizi di una transazione illecita. Al fine di limitare il rischio finanziario derivante da transazioni fraudolente, la Banca adotta, a propria discrezione, diverse misure per la prevenzione delle attività fraudolente ovvero in caso di sospetto di attività fraudolenta.

Qualora per il mezzo di pagamento venga utilizzato 3-D Secure in un Online Shop, la Banca raccoglie e verifica i dati necessari per tale processo.

I dati del titolare del mezzo di pagamento vengono inoltre elaborati in fase di trattamento nell'ambito del processo di contestazione delle transazioni e di rimborso (chargeback), ad es. per il chiarimento di transazioni sconosciute o in caso di addebiti non autorizzati. Allo stesso modo vengono raccolti ed elaborati dati ai fini della gestione di eventi assicurati, allo scopo di chiarire i diritti in collaborazione con il partner assicurativo.

4.7 Pagamenti con l'app TWINT

La Banca consente all'utente di pagare con l'app TWINT («pagamenti P2M») e di inviare o ricevere denaro da altri utenti TWINT («pagamenti P2P»). L'app TWINT supporta l'esecuzione di pagamenti P2M ai punti di accettazioni aderenti al sistema TWINT.

I pagamenti P2P con altri utenti TWINT avvengono in base al numero di cellulare indicato nell'ordine di pagamento. Il numero di cellulare del beneficiario del pagamento può essere registrato direttamente nell'app TWINT o selezionato accedendo alla rubrica personale del dispositivo mobile dell'utente. Per l'esecuzione di pagamenti P2P il numero di cellulare dell'utente viene memorizzato anche nel sistema TWINT che viene gestito da TWINT SA.

Presso la Banca e presso TWINT SA vengono registrati l'importo totale dell'acquisto, la data dell'acquisto e la sede del punto di accettazione presso cui viene effettuato il pagamento. La Banca e TWINT SA non ricevono alcuna informazione sul contenuto del carrello, a meno che la trasmissione di questi dati sia espressamente prevista.

Senza l'esplicito consenso dell'utente, la Banca e TWINT SA non trasmettono dati personali ai punti di accettazione e/o ai terzi coinvolti, a meno che la trasmissione dei dati sia espressamente prevista.

4.8 Prestazioni a valore aggiunto con l'app TWINT

Con l'app TWINT l'utente può utilizzare prestazioni a valore aggiunto come, in particolare, le campagne, le carte clienti, le funzioni di partner nonché la funzione «Pagare dopo». La Banca e TWINT SA raccolgono i dati per lo svolgimento personalizzato delle campagne di fornitori terzi e analizzano i dati, il che consente loro di indirizzare all'utente campagne di fornitori terzi mirate in base ai suoi interessi personali. L'utilizzo dei dati è retto esclusivamente dal rapporto contrattuale (ivi incluse le disposizioni sulla protezione dei dati) tra l'utente e il rispettivo fornitore terzo. Per le offerte correlate alle funzioni di partner nonché alla funzione «Pagare dopo» valgono le disposizioni e le informative sulla protezione dei dati di questi partner.

La Banca e TWINT SA non trasmettono i dati personali degli utenti ai punti di accettazione e/o ai terzi coinvolti, a meno che l'utente non acconsenta espressamente a tale trasmissione nell'app TWINT. Senza tale consenso, i punti di accettazione coinvolti avranno solamente accesso ai dati anonimizzati.

Al momento della riscossione delle campagne nel sistema del punto di accettazione, TWINT SA trasmette il numero di identificazione della campagna al punto di accettazione. Il punto di accettazione calcola l'eventuale sconto o il vantaggio monetario per l'utente. In questo modo, il punto di accettazione riceve le stesse informazioni di quando l'utente esibisce fisicamente il numero di identificazione della campagna.

Al momento della riscossione delle campagne nel sistema TWINT, lo sconto o il vantaggio monetario viene calcolato nel sistema TWINT e trasmesso al punto di accettazione, affinché quest'ultimo possa rielaborarlo nel proprio sistema (ad es. deduzione di uno sconto).

Con la registrazione o l'attivazione di una carta cliente nell'app TWINT questa viene inserita automaticamente nel processo di pagamento con l'app TWINT, purché ciò sia tecnicamente possibile tramite il rispettivo emittente della carta cliente.

Se una carta cliente viene registrata nell'app TWINT, il pagamento viene effettuato con l'app TWINT e l'utente ottiene un eventuale vantaggio (punti, sconto, ecc.) utilizzando la carta cliente, l'emittente della carta cliente o un terzo legittimamente coinvolto' riceve gli stessi dati come se l'utente esibisse fisicamente la carta cliente al punto di accettazione.

TWINT SA trasmette il numero di identificazione della carta cliente al punto di accettazione o a terzi a lei collegati e indipendentemente dalla carta cliente utilizzata anche dati di base relativi al pagamento, come l'indicazione oraria, l'importo e gli eventuali sconti o punti concessi con l'utilizzo della carta. L'impiego della carta cliente e l'utilizzo dei dati sono retti esclusivamente dal rapporto contrattuale (ivi incluse le disposizioni sulla protezione dei dati) tra l'utente e l'emittente della carta clienti rispettivamente tra l'utente e il punto di accettazione, nonché con questi terzi collegati. Lo stesso vale per analogia per le funzioni di partner.

4.9 Programma bonus surprize di Viseca

Qualora il titolare di carte di credito per privati partecipi al programma bonus surprize (si vedano le «Condizioni per l'utilizzo delle carte di credito Raiffeisen»), la Banca inoltra i dati di base, di contatto, relativi alle transazioni e relativi

all'indirizzo necessari a tale scopo ai fini dell'esecuzione del calcolo dei premi e dei punti nonché della gestione del processo di ordinazione a Viseca Payment Services SA (nel prosieguo «Viseca»); ai fini dell'utilizzo del programma bonus surprize, trovano applicazione le relative condizioni di partecipazione e le relative informative sulla protezione dei dati. La Banca e Viseca sono responsabili reciprocamente indipendenti e autonomi in relazione all'elaborazione dei dati. Viseca elabora i dati sul territorio nazionale e all'estero per le proprie finalità in conformità alle condizioni di partecipazione e informative sulla protezione dei dati. La Banca non ha alcuna influenza sull'utilizzo e sulla protezione dei dati da parte di Viseca. Tutte le richieste e le contestazioni a ciò correlate devono essere indirizzate direttamente a Viseca.

4.10 Utilizzo dei servizi online di Viseca
Per quanto concerne la protezione dei dati con riferimento all'utilizzo dei servizi online di Viseca in relazione alle carte di credito, le informazioni sono disponibili nelle condizioni d'uso e nelle informative sulla protezione dei dati di Viseca.

4.11 Trattamento dei dati per finalità legate ai rischi (creazione di profili)
La Banca elabora dati per finalità legate ai rischi, al fine di individuare e di sorvegliare i rischi correlati all'emissione e all'utilizzo delle carte (ad es. rischi di credito e di mercato).

4.12 Trattamento dei dati e creazione di profili per finalità di marketing
Dai dati personali, ivi inclusi i dati relativi alle transazioni che vengono elaborati, la Banca, anche in combinazione con dati pubblicamente accessibili o ottenuti dai partner, può creare profili cliente, di utente, di consumo e di preferenze, in particolare per finalità di marketing, che consentono alla Banca di sviluppare e offrire prodotti e servizi interessanti per il titolare del mezzo di pagamento. La Banca può inviare ai titolari del mezzo di pagamento tali informazioni sui propri prodotti e servizi o sui prodotti e sui servizi dei propri partner tramite i canali di comunicazione disponibili (ad es. posta, e-mail, notifiche push, app) o gestire la pubblicità online di conseguenza.

Tali profili permettono anche lo sviluppo, la gestione, l'adeguamento e la personalizzazione di prodotti, servizi e offerte. I profili sono altresì utilizzati dalla Banca per la gestione dei rischi, la gestione dei contratti, per la lotta contro gli usi illeciti e per l'adempimento di obblighi legali.

Ciascun titolare del mezzo di pagamento ha la possibilità di opporsi all'invio di pubblicità con effetto futuro tramite comunicazione scritta corrispondente a mezzo lettera o una comunicazione tramite i servizi online della Banca alla Banca. Ne sono esclusi le comunicazioni non pubblicitarie e i testi relativi alla fatturazione generati automaticamente.

Con l'opposizione ovvero la revoca, i dati personali del titolare del mezzo di pagamento non vengono più utilizzati per la finalità corrispondente. Di norma, i dati per le campagne pubblicitarie o le informazioni generali vengono preparati con alcune settimane di anticipo. Pertanto è possibile che per un certo periodo di tempo al titolare del mezzo di pagamento sia inviata ancora pubblicità anche dopo l'esercizio del suo diritto di opposizione o di revoca.

4.13 Invio di informazioni e di pubblicità
La Banca può comunicare ai titolari del mezzo di pagamento informazioni (inclusa pubblicità) tramite spedizione postale o per via elettronica (tramite e-mail, tramite notifica push, tramite SMS, tramite i servizi online o i servizi online della Banca (siti web o app)), tramite l'app TWINT o tramite altra modalità idonea e comunicare con titolari del mezzo di pagamento. La comunicazione elettronica avviene tramite le reti di comunicazione pubbliche. I dati trasmessi in tal modo sono fondamentalmente visibili per i terzi, possono andare perduti durante il trasferimento oppure essere intercettati o alterati da terzi non autorizzati. Per questo motivo non è possibile escludere che, nonostante tutte le misure di sicurezza adottate, terzi possano ottenere l'accesso alla comunicazione della Banca con il titolare del mezzo di pagamento.

Una presa di contatto tramite e-mail avviene solo se la Banca ha ricevuto l'indirizzo e-mail in occasione di una presa di contatto da parte del titolare del mezzo di pagamento, ad esempio a seguito dell'indicazione nella richiesta di carta, all'atto dell'immissione in un modulo di richiesta, in fase di registrazione per un servizio o la newsletter o in caso di partecipazione a concorsi.

4.14 Trattamento dei dati ampliato correlato all'app TWINT
Oltre ai dati relativi alle transazioni, la Banca e TWINT SA analizzano quali offerte e prestazioni a valore aggiunto l'utente visualizza, attiva e riscuote nell'app TWINT.

Agli utenti che consentono all'app TWINT di accedere alla funzionalità di localizzazione del loro dispositivo mobile, viene trasmessa anche la posizione quando l'app TWINT viene utilizzata attivamente. Questo serve a poter mostrare agli utenti le offerte nei luoghi in cui si trovano più spesso. La località non viene trasmessa se l'app TWINT si trova in background. Non avviene alcun cosiddetto tracciamento in background (background tracking). L'utente può attivare e disattivare l'accesso alla localizzazione da parte dell'app TWINT nelle impostazioni del sistema operativo del dispositivo mobile. I dati sulla localizzazione vengono memorizzati solo in modo impreciso (raggio di 16 km) ed eliminati al più tardi dopo sei mesi.

4.15 Raccolta e utilizzo dei dati per il miglioramento continuo e lo sviluppo dei prodotti, delle prestazioni, dei servizi e delle app offerti
La Banca raccoglie e utilizza i dati per la messa a disposizione, lo sviluppo e il miglioramento dei prodotti, delle prestazioni, dei servizi e delle app.

Questo comprende in particolare anche l'app TWINT; in questo caso si tratta, da un lato, di dati ai quali l'app TWINT ha accesso in base alle impostazioni dell'utente sul dispositivo

mobile (ad es. ricezione di segnali BLE, geolocalizzazione, ecc.), dall'altro, di dati e informazioni tecniche che rientrano nell'ambito dell'utilizzo dell'app TWINT. La Banca condivide questi dati in forma anonima anche con TWINT SA, la quale li utilizza per lo stesso scopo.

4.16 Utilizzo di Google Firebase per l'app TWINT

Nell'app TWINT, la Banca e TWINT SA utilizzano il Google Firebase Software Development Kit (SDK) di Google Inc. («Google») o soluzioni equivalenti per analizzare il comportamento degli utenti nell'app allo scopo di ottimizzare continuamente l'app TWINT e di adattarla alle esigenze degli utenti.

L'utente ha la possibilità di disattivare in qualsiasi momento la raccolta e la trasmissione dei dati di utilizzo a Google nelle impostazioni dell'app TWINT.

Le informazioni raccolte attraverso l'SDK sull'utilizzo dell'app TWINT, in particolare:

- l'analytics-ID (valore casuale, tramite il quale TWINT SA può identificare l'utente);
- il client ID (valore casuale che identifica il dispositivo utilizzato e permette a Google di riassumere gli eventi inviati in una sessione di dispositivi), che non consente di risalire al dispositivo dell'utente;
- i dati chiave del dispositivo (marca, tipo, schermo, memoria);
- le informazioni sulla piattaforma (ad es., versione iOS e versione Android);
- la versione dell'app TWINT installata;
- eventualmente, il tipo e la versione del browser Internet utilizzato;
- l'indirizzo IP del computer in uso (abbreviato in modo che non sia più possibile assegnarlo a un utente specifico)
- vengono trasmesse a server di Google negli Stati Uniti e lì memorizzate. Questi dati vengono analizzati da Google per generare dei report sull'utilizzo dell'app TWINT e per fornire ulteriori servizi connessi all'utilizzo dell'app TWINT.

L'utente è consapevole che Google può trasmettere queste informazioni, ove necessario, a terzi nella misura in cui ciò sia consentito dalla legge o nella misura in cui terzi trattino questi dati su mandato di Google. In nessun caso Google associa l'indirizzo IP dell'utente con altri dati di Google. Gli indirizzi IP dell'utente vengono anonimizzati (abbreviati di tre cifre), in modo che non sia possibile associarli all'utente.

5 Profilazione e decisioni individuali automatizzate

Nell'ambito delle finalità di trattamento elencate, la Banca può trattare e analizzare i dati personali in modo parzialmente o totalmente automatizzato, ovvero informatizzato. In questo modo, la Banca, partendo dai dati raccolti, può creare dei profili con gli interessi e altri aspetti della personalità del titolare del mezzo di pagamento. La Banca utilizza questi profili in particolare per gli scopi seguenti:

- verifica e gestione del contratto (ad es. correlata alla valutazione dei rischi presenti o alla verifica della solvibilità, agli adeguamenti dei limiti nel corso del rapporto contrattuale e al blocco automatico di determinate transazioni in presenza di anomalie);
- sorveglianza delle transazioni e identificazione dei rischi in particolare correlati alla gestione dei rischi rispettivamente alla lotta al riciclaggio di denaro, agli abusi o alle truffe e alla sicurezza informatica;
- personalizzazione di pubblicità per prodotti e servizi della Banca e quelli di terzi;
- analisi di mercato, sviluppo e miglioramento di prodotti (affinché la Banca possa continuare a sviluppare e a migliorare i prodotti e i servizi, come pure i siti web e le app in base alle esigenze di clienti e utenti).

In genere la Banca non prende decisioni individuali basate esclusivamente su un trattamento automatizzato dei dati personali e che producano effetti giuridici per il titolare del mezzo di pagamento o lo limitino in modo considerevole. In caso contrario, la Banca informerà il titolare del mezzo di pagamento in base alle norme di legge e gli concederà i rispettivi diritti.

6 Conservazione dei dati e misure per garantire la sicurezza dei dati

La Banca memorizza i dati personali nella misura in cui ciò è necessario per l'adempimento dei termini di conservazione legali o regolamentari o per la finalità per la quale sono stati trattati i dati. Nel farlo, la Banca terrà conto delle finalità del trattamento e, in particolare, della necessità di perseguire i propri interessi (ad es., per l'esercizio e la difesa di diritti e per garantire la sicurezza informatica). Se questi scopi sono raggiunti o non si applicano più e non vi è più un obbligo di conservazione dei dati, la Banca cancella o anonimizza i dati personali.

La Banca rispettivamente il Gruppo Raiffeisen utilizza un sistema gestionale per la sicurezza delle informazioni (ISMS). Questo comprende un sistema di istruzioni e di controllo con misure tecniche e organizzative per la protezione dei dati personali. Oltre al livello generale di protezione, nei regolamenti e nei processi interni del Gruppo Raiffeisen sono definite misure esplicite e basate sul rischio per la protezione dei dati personali. I rischi informatici sono controllati attraverso misure tecniche e organizzative. I controlli di sicurezza per i servizi informatici interni ed esterni sono allineati agli standard di mercato. Il Gruppo Raiffeisen adatta la protezione dei dati personali alla situazione di minaccia di volta in volta presente, in un processo di miglioramento continuo.'''

7 Inoltro dei dati

7.1 Inoltro all'interno del Gruppo Raiffeisen

Il Gruppo Raiffeisen comprende le Banche Raiffeisen in Svizzera (singola Banca Raiffeisen), Raiffeisen Svizzera società cooperativa (nel prosieguo «Raiffeisen Svizzera») e le società del Gruppo di Raiffeisen Svizzera nonché delle Banche Raiffeisen.

Per la fornitura della prestazione in relazione ai mezzi di pagamento, la Banca si avvale di altre società del Gruppo del Gruppo Raiffeisen, in particolare di Raiffeisen Svizzera, e inoltra altresì i dati a tali società del Gruppo.

All'interno della Banca e anche del Gruppo Raiffeisen, ricevono l'accesso ai dati solo le centrali e le persone che necessitano dell'accesso per l'adempimento ai contratti o per la salvaguardia degli interessi legittimi o per l'adempimento degli obblighi contrattuali e legali.

7.2 Trattamento dei dati da parte di fornitori di servizi specializzati

La Banca può esternalizzare per intero o in parte settori e funzioni ivi inclusi i dati dei titolari del mezzo di pagamento a fornitori di servizi (in particolari ai cd. responsabili del trattamento dei dati) nonché ai relativi sub-responsabili sul territorio nazionale e all'estero e divulgarli nell'ambito della fornitura delle prestazioni. A loro volta, essi possono rendere noti i dati a sub-responsabili. Tali fornitori di servizi nonché i relativi sub-responsabili sono assoggettati agli obblighi legali e contrattuali di protezione dei dati e di discrezione nonché, in qualità di responsabili della Banca, al segreto bancario.

Le categorie di destinatari dei dati dei titolari del mezzo di pagamento di seguito indicate possono essere ubicate anche al di fuori dell'UE ovvero dello Spazio economico europeo (Stati terzi). Tali Stati terzi potrebbero non disporre di leggi in grado di tutelare i dati dei titolari del mezzo di pagamento al pari di quanto avviene in Svizzera o nell'UE ovvero nel SEE. In tal caso, la Banca assicura la protezione dei dati tramite contratti aventi ad oggetto la trasmissione dei dati. Al riguardo si tratta, in particolare, di servizi nei seguenti settori:

- Service Payment Provider;
- Customer Care Center per richieste telefoniche dei titolari del mezzo di pagamento e dei terzi autorizzati;
- centrale di blocco delle carte, 7 giorni su 7, 24 ore su 24;
- lotta contro le attività fraudolente;
- gestione dei danni;
- contestazioni di transazioni di pagamento;
- elaborazione della richiesta;
- personalizzazione delle carte, generazione di NIP ecc.;
- servizi IT, ad es. manutenzione e gestione dei sistemi delle carte, servizi nei settori memorizzazione dei dati (hosting), manutenzione e gestione dell'app TWINT, invio di newsletter tramite e-mail, analisi dei dati ecc.;
- servizi nel settore dell'esecuzione, della spedizione e della logistica, ad es. per la fatturazione, l'invio delle carte ordinate nonché servizi di stampa;
- gestione in relazione all'opzione di pagamento rateale delle carte di credito;
- informazioni economiche e incasso, ad es. in caso di mancato pagamento dei crediti dovuti.

In particolare, la Banca collabora con Viseca ad es. nell'ambito dell'attività delle carte di credito. Viseca opera su incarico della Banca, ma anche per proprio conto, nei confronti dei titolari di carta. Il titolare della carta avrà anche un contatto diretto con i collaboratori di Viseca, ad esempio nel Customer Care Center e nella centrale di blocco delle carte, nella lotta contro le attività fraudolente nonché nella gestione dei danni. Inoltre, il titolare della carta, ad es. qualora utilizzi i servizi online e partecipi al programma bonus, concluderà un rapporto contrattuale diretto con Viseca, nel qual caso trova conseguentemente applicazione l'informativa sulla protezione dei dati di Viseca.

Nell'ambito dell'attività delle carte di debito, la Banca collabora, in particolare, con una società appartenente a SIX Group SA (nel prosieguo «SIX») in qualità di fornitore di servizi. SIX eroga servizi alla Banca comparabili a quelli di Viseca nell'ambito dell'attività delle carte di credito.

7.3 Inoltro a organizzazioni internazionali di carte (Mastercard e Visa)

In caso di impiego della carta da parte del titolare della carta, i dati relativi alle transazioni vengono trasmessi dai punti di accettazione, ivi inclusi i distributori automatici, alla Banca. Tale trasmissione avviene fondamentalmente tramite le reti globali delle organizzazioni internazionali di carte Mastercard e Visa.

A seguito dell'impiego della carta in Svizzera e all'estero, le organizzazioni internazionali di carte nonché i terzi incaricati dalle organizzazioni di carte a cui viene affidata l'elaborazione delle transazioni vengono a conoscenza dei dati relativi alle transazioni (ad es. numero della carta, importo/data della transazione, punto di accettazione). In determinati casi (ad es. acquisto di un biglietto aereo, fatture di hotel, noleggio di automobili ecc.), apprendono ulteriori dati come ad es. il nome e il cognome del titolare della carta.

I dati trasmessi alle organizzazioni internazionali di carte o tali dati consultati possono essere elaborati dalle organizzazioni internazionali di carte per le loro proprie finalità e in conformità alle loro proprie informative sulla protezione dei dati (cfr. visa.com emastercard.com) sul territorio nazionale e all'estero, ossia anche in Paesi senza un'adeguata protezione dei dati.

Le organizzazioni internazionali di carte vincolano l'emittente di carte a offrire i relativi servizi di aggiornamento (Visa Account Updater ovvero Mastercard Automatic Billing Updater). Tali servizi di aggiornamento hanno l'obiettivo di aggiornare automaticamente presso i punti di accettazione e i fornitori di servizi aderenti (ad es. fornitori terzi di soluzioni di Mobile Payment) le informazioni relative alla carta memorizzate dal titolare della carta per l'esecuzione dei pagamenti (ad es. per servizi online, abbonamenti o ticket app), in particolare il numero della carta e la data di scadenza, se queste subiscono variazioni. In tal modo viene garantito che, nonostante modifiche ai dati relativi alla carta, i punti di accettazione e i fornitori di servizi (ad es. fornitori terzi di soluzioni di Mobile Payment) che supportano tali servizi di aggiornamento possano continuare a effettuare una gestione senza difficoltà dei pagamenti con carta con il titolare della carta.

Per tali servizi di aggiornamento, la Banca trasmette il numero della carta e la data di scadenza della carta alle organizzazioni internazionali di carte summenzionate. Per l'ulteriore trattamento dei dati trasmessi alle organizzazioni internazionali di carte si rimanda alle relative disposizioni in materia di trattamento dei dati.

Ciascun titolare di carta ha la possibilità di impedire l'inoltro nell'ambito dei servizi di aggiornamento, a seguito di (a) disdetta del rapporto contrattuale avente ad oggetto la carta prima della ricezione di una carta sostitutiva, (b) cancellazione dei dati relativi alla carta memorizzati presso i punti

di accettazione o i fornitori di servizi (ad es. fornitori terzi di soluzioni di Mobile Payment) o disdetta del rapporto contrattuale con i punti di accettazione, oppure (c) dichiarazione di opposizione alla partecipazione ai servizi di aggiornamento da inviarsi alla Banca.

Per i pagamenti con l'app TWINT, con una carta di credito come fonte di addebito, si applicano anche queste disposizioni.

7.4 Inoltro dei dati dall'app TWINT al gestore del sistema di pagamenti TWINT SA come pure a fornitori terzi e partner di prestazioni a valore aggiunto di TWINT

Il funzionamento del sistema TWINT avviene tramite TWINT SA.

TWINT SA tratta i dati ricevuti dalla Banca in relazione all'elaborazione dei pagamenti e all'erogazione di prestazioni a valore aggiunto. Al riguardo TWINT SA è soggetta alle stesse leggi e regolamenti della Banca. TWINT SA può a sua volta trasmettere i dati a subappaltatori incaricati del trattamento, ma rimane responsabile dei dati. I dati comprendono anche, in particolare, i numeri di cellulare svizzeri dell'utente, nonché altri dati necessari per l'erogazione dei servizi a valore aggiunto.

Esclusi dalle disposizioni di questo punto sono i dati che devono essere conservati per un periodo più lungo dalla Banca o da TWINT SA al fine di adempiere agli obblighi legali.

7.5 Inoltro dei dati al fornitore della funzione «Pagare dopo» con l'app TWINT

Utilizzando l'app TWINT per i pagamenti, l'utente può utilizzare la funzione «Pagare dopo».

La Banca trasmette al fornitore i dati necessari per la valutazione della solvibilità e per l'elaborazione della funzione «Pagare dopo», ossia, in particolare anche il cognome, il nome, la data di nascita, l'indirizzo, il numero di cellulare e l'indirizzo e-mail dell'utente, nonché i dati di pagamento.

Il fornitore della funzione «Pagare dopo» tratta i dati ricevuti dalla Banca in relazione alla messa a disposizione della funzione supplementare «Pagare dopo». La funzione «Pagare dopo» e l'utilizzo dei dati sono retti esclusivamente dal relativo rapporto contrattuale tra l'utente e il fornitore.

7.6 Inoltro dei dati ad altri terzi

Ove sussista un obbligo di divulgazione o un interesse legittimo della Banca, è inoltre possibile una trasmissione dei dati del titolare del mezzo di pagamento, in particolare ai seguenti terzi sul territorio nazionale e all'estero:

- organismi e autorità di vigilanza, penali e di altro tipo;
- altre parti in possibili o effettivi procedimenti legali o controversie;
- titolari del mezzo di pagamento e aventi diritto di firma risp. procuratori, in particolare in relazione a conti congiunti o a clienti aziendali.

7.7 Informazioni relative alla solvibilità

Nell'ambito della verifica della capacità creditizia risp. della solvibilità, la Banca rende note informazioni rilevanti per la solvibilità in particolare alla ZEK ovvero all'IKO. In particolare in caso di blocco della carta, mora dei pagamenti qualificata o utilizzo illecito del mezzo di pagamento e fattispecie simili, la Banca è autorizzata a farne rapporto alla ZEK nonché, nei casi stabiliti dalla legge, in particolare alle autorità penali.

7.8 Inoltro dei dati dell'app TWINT tramite Internet

L'app TWINT viene offerta tramite Internet e, quindi, tramite una rete aperta e accessibile a tutti. Nonostante l'utilizzo delle più moderne tecnologie di sicurezza, non è possibile garantire una sicurezza assoluta né da parte della Banca né da parte dell'utente. La trasmissione di dati via Internet varca regolarmente i confini transfrontalieri e potrebbe non essere controllabile dalla Banca, anche se il mittente e il beneficiario si trovano in Svizzera. I singoli pacchetti di dati vengono trasmessi in forma criptata, ma è possibile per terzi risalire al mittente e al destinatario, nonché a una relazione bancaria esistente.

7.9 Inoltro dei dati al fornitore del sistema operativo/ all'app store per l'app TWINT

Scaricando, installando e utilizzando l'app TWINT, terzi (ad es., fornitori di sistemi operativi o app store) possono risalire a un rapporto di clientela esistente, precedente o futuro tra l'utente e la Banca. I dati acquisiti possono essere raccolti, trasferiti, trattati e resi accessibili conformemente alle condizioni di questi terzi. Le condizioni di contratto di questi terzi devono essere distinte dal resto delle condizioni della Banca o di TWINT SA.

8 Divulgazione dei dati all'estero

I destinatari dei dati personali menzionati nella presente Informativa sulla protezione dei dati carte possono essere ubicati in Svizzera, ma anche all'estero. I dati personali possono, quindi, essere trattati in tutto il mondo. Se il beneficiario si trova in un Paese privo di un'adeguata protezione dei dati, la Banca obbligherà il beneficiario a rispettare un'adeguata protezione dei dati stipulando clausole contrattuali tipo riconosciute o basandosi su 'una disposizione di deroga legale (ad es., il consenso del titolare del mezzo di pagamento, la stipula o l'esecuzione di un contratto, il perseguimento di interessi pubblici prevalenti, 'l'esercizio di diritti in via giudiziaria o se si tratta di dati resi generalmente accessibili dal titolare del mezzo di pagamento il cui trattamento non è stato contestato dal titolare del mezzo di pagamento). I dati trasmessi via Internet spesso transitano anche attraverso Paesi terzi. I dati possono quindi finire all'estero anche se il mittente e il beneficiario dei dati si trovano nello stesso Paese.

9 Diritti del titolare del mezzo di pagamento in relazione al trattamento dei dati

Le informazioni contenute nella presente Informativa sulla protezione dei dati carte hanno lo scopo di consentire ai titolari del mezzo di pagamento di esercitare i propri diritti ai sensi della legge applicabile sulla protezione dei dati. Di conseguenza, al titolare del mezzo di pagamento spettano in particolare i seguenti diritti:

- diritto a determinate informazioni sul nostro trattamento dei dati personali;
- diritto alla rettifica dei dati personali se sono inesatti o incompleti;
- diritto di cancellare alcuni dati personali se la finalità del trattamento non è più data;
- diritto di opporsi a un determinato trattamento e diritto di revoca di un consenso separato, in ogni caso con efficacia ex nunc;
- quando la Banca informa il titolare del mezzo di pagamento di una decisione individuale automatizzata, il titolare del mezzo di pagamento ha l'opportunità di esprimere il proprio parere e di chiedere che la decisione sia rivista da una persona fisica.

Se il trattamento dei dati personali si basa eccezionalmente su un consenso separato, il titolare del mezzo di pagamento ha il diritto di revocare tale consenso in qualsiasi momento con efficacia ex nunc. A seguito della revoca, i dati personali non saranno più trattati per lo scopo corrispondente, a meno che interessi pubblici o privati prevalenti o la legge non ne consentano l'ulteriore trattamento. Lo stesso vale se il titolare del mezzo di pagamento si oppone al trattamento dei dati. In questo caso, la Banca non sarà in grado di fornire i suoi servizi. L'attuazione della revoca o dell'opposizione può richiedere alcuni giorni lavorativi. I dati per le campagne pubblicitarie o le informazioni generali vengono solitamente preparati con diverse settimane di anticipo. È, quindi, possibile che il titolare del mezzo di pagamento continui a ricevere pubblicità per un certo periodo di tempo dopo aver esercitato la revoca o l'opposizione.

Il titolare del mezzo di pagamento può esercitare questi diritti inviando una lettera firmata all'ufficio designato dalla Banca, allegando una copia del proprio documento d'identità o passaporto. La revoca o l'opposizione può essere esercitata anche attraverso i servizi online della Banca (tramite l'applicazione sulla privacy) (ad es., per quanto riguarda la creazione di profili e la presa di contatto a fini pubblicitari, nonché la presa di contatto a fini di ricerca di mercato). Questi diritti sono soggetti a requisiti e restrizioni legali (ad es., la Banca non può cancellare i dati se è soggetta a un obbligo di conservazione a tale riguardo. La Banca informerà il titolare del mezzo di pagamento di eventuali restrizioni. Il titolare del mezzo di pagamento vanta questi diritti anche nei confronti di altri terzi (ad es., fornitori di servizi di pagamento via cellulare, fornitori terzi di campagne TWINT e carte clienti, Viseca come fornitore del programma bonus surprize e dei servizi online) che trattano i dati sotto la propria responsabilità. Il titolare del mezzo di pagamento può contattare direttamente questi terzi per esercitare i propri diritti in relazione al loro trattamento.

10 Modifiche

La Banca si riserva il diritto di modificare in qualsiasi momento la presente Informativa sulla protezione dei dati senza informare attivamente il titolare del mezzo pagamento di una modifica. 'La versione pubblicata all'indirizzo raiffeisen.ch/rch/it/chi-siamo/gruppo-raiffeisen/disclaimer-website-i.html è quella attualmente valida. Tutti gli altri documenti citati possono essere consultati in qualsiasi momento sul sito web della Banca all'indirizzo raiffeisen.ch/rch/it/chi-siamo/gruppo-raiffeisen/disclaimer-website-i.html o raiffeisen.ch/rch/it/clientela-privata/conti-e-pagamenti/downloads.html.

11 Responsabilità e punto di riferimento

Generalmente, la Banca con cui il titolare del mezzo di pagamento si interfaccia è responsabile del trattamento dei dati personali.

Punto di riferimento per qualsiasi richiesta in merito alla protezione dei dati è il responsabile della protezione dei dati del Gruppo Raiffeisen, indipendentemente dalla Banca o dalla società del Gruppo Raiffeisen responsabile del trattamento dei suoi dati nel singolo caso:

Raiffeisen Svizzera società cooperativa
Responsabile della protezione dei dati
Raiffeisenplatz 4
9000 San Gallo
Svizzera

datenschutz@raiffeisen.ch
raiffeisen.ch