Informativa Integrativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679 ("GDPR"), relativa all'utilizzo della APP

Questa Informativa integra l'Informativa Privacy Clienti disponibile sul sito www.bancobpm.it (sezione privacy), alla quale si rinvia per i contenuti che non sono qui espressamente previsti, ed ha lo scopo di illustrare le attività di trattamento dei dati personali effettuate dal Titolare del trattamento (Banco BPM S.p.A., in seguito la "Banca") nell'ambito dell'utilizzo della Applicazione di mobile banking (in seguito "APP").

Informazioni sul trattamento dei dati

L'avvio dell'APP comporta la rilevazione automatica e la raccolta di alcuni Suoi dati personali da parte della Banca, in particolare:

- **dati relativi al dispositivo**: informazioni relative al sistema operativo utilizzato, modello del dispositivo, lingua, indirizzo IP, identificatori univoci[1] e di stato. Vengono inoltre rilevate le applicazioni installate sul dispositivo per verificare la presenza di app malevole;
- **dati relativi alla connessione di rete**: informazioni sul numero e/o sull'operatore telefonico o sull'Internet Service Provider utilizzati per collegarsi ai servizi erogati dalla Banca tramite connessione fisica o WiFi;
- **dati relativi alla posizione**: informazioni sulla posizione dalla quale viene effettuato l'accesso o le operazioni;

Finalità del trattamento

I dati personali raccolti attraverso l'APP sono trattati per le seguenti finalità:

i) **impedire utilizzi fraudolenti** e **monitorare il corretto funzionamento dell'APP**. I dati possono essere raccolti e inviati al dominio *bancobpm.it* utilizzando delle librerie software integrate nell'APP (le c.d. "SDK"), allo scopo di prevenire utilizzi fraudolenti ed anomalie nel funzionamento dell'applicazione (dovute, ad es., ad arresti irregolari o all'errata visualizzazione dei contenuti). In particolare, i dati vengono analizzati per individuare applicazioni installate sul dispositivo in grado di mettere a rischio la sicurezza del sistema, per valutare la sicurezza della connessione e l'affidabilità del device utilizzato e per rilevare eventuali accessi o operazioni effettuate all'interno di un'area geografica diversa da quella abituale. La Banca può altresì assegnare un profilo che consente di attribuire un giudizio sintetico utile a valutare se l'operatività effettuata attraverso l'APP sia riconducibile o meno al cliente,

[1] Si tratta di informazioni che permettono di identificare l'interessato in modo univoco. Sul dispositivo, sono considerati identificatori univoci gli identificativi pubblicitari messi a disposizione dai produttori dei dispositivi mobile, come l'IDFA di Apple e l'AAIG di Android. Per assicurare la sicurezza delle autenticazioni e delle transazioni vengono utilizzati l'UUID (Universally unique identifier), l'IMEI (International Mobile station Equipment Identity), il MAC Address, l'ICCID (Integrated Circuit Card ID), l'IMSI (International mobile subscriber identity), il BSSID (Basic Service Set Identifier) e l'SSID (Service Set Identifier).

in modo da intervenire tempestivamente qualora venga rilevato il rischio concreto di subire una frode. L'elaborazione del profilo viene effettuata utilizzando un modello predittivo basato su algoritmi di tipo statistico e, nell'ambito dell'attività di profilazione, è escluso il trattamento di categorie particolari di dati personali dell'art. 9 del GDPR. Si precisa che nell'ambito delle attività di trattamento effettuate per prevenire e impedire utilizzi fraudolenti la Banca può trattare dati relativi alle transazioni quali, ad es., il numero di conto corrente, le informazioni sull' ordinante e sul beneficiario, l'importo della disposizione.

ii) **consentire la corretta gestione del rapporto**, ivi incluse tutte le attività e i Servizi correlati. Durante l'utilizzo dell'APP, la Banca può trattare ulteriori categorie di dati personali necessari per garantire la corretta erogazione dei Servizi da Lei espressamente richiesti: ad es., su esplicita autorizzazione, l'APP può attivare la fotocamera per acquisire le immagini del documento di identità da aggiornare o per inquadrare codici (es. QR Code) e testi e ricavare le informazioni necessarie per completare l'operazione di pagamento, oppure rilevare la Sua posizione per mostrare l'elenco delle filiali più vicine. In caso di utilizzo dell'impronta digitale o del riconoscimento facciale per effettuare l'autenticazione e l'accesso al servizio, la Banca non raccoglie i dati relativi alle impronte digitali o alle caratteristiche facciali registrate dal dispositivo mobile ma soltanto un codice numerico univoco che conferma che l'impronta digitale o le caratteristiche del volto corrispondono alla stessa persona abilitata ad utilizzare il dispositivo.

Base giuridica

I Suoi dati saranno trattati da Banco BPM in conformità alla vigente normativa in materia di privacy e protezione dati, secondo principi di correttezza, liceità, trasparenza. La base giuridica del trattamento dei dati è: i) l'art. 6, 1° comma, lett. f) del GDPR, ovvero il Legittimo Interesse della Banca a prevenire frodi[2], nel rispetto degli obblighi normativi a cui è soggetta[3], e ad evitare disguidi nell'erogazione del Servizio; ii) l'art. 6, 1° comma, lett. b) GDPR, ovvero l'esecuzione del Servizio.

[2] Si richiama il paragrafo 3.2 delle "Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati".

[3] Si fa riferimento, a titolo esemplificativo, alle previsioni contenute nell'art. 2 par. 2 del "Regolamento Delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri", in cui si prescrive ai prestatori di servizi di pagamento di adottare meccanismi di monitoraggio delle operazioni che tengano conto di fattori di rischio quali : a) gli elenchi degli elementi di autenticazione compromessi o rubati; b) l'importo di ciascuna operazione di pagamento; c) gli scenari di frode noti nella prestazione dei servizi di pagamento; d) i segnali della presenza di malware in una qualsiasi delle sessioni della procedura di autenticazione; e) se il dispositivo o il software di accesso sono forniti dal prestatore di servizi di pagamento, un registro dell'utilizzo del dispositivo o del software di accesso forniti all'utente del servizio di pagamento e l'utilizzo anomalo degli stessi.

Periodo di conservazione

I dati verranno trattati solo da personale autorizzato e formato, al fine di garantire la necessaria riservatezza delle informazioni fornite e saranno conservati per il tempo strettamente necessario, nel rispetto dei termini prescrizionali o nei diversi tempi eventualmente stabiliti dalla normativa legale e regolamentare di riferimento. In relazione alle finalità indicate al punto i) (impedire utilizzi fraudolenti e monitorare il corretto funzionamento dell'APP), i dati verranno conservati per un periodo massimo di un anno.

Trasferimento e accesso ai Suoi dati

Il conseguimento delle finalità potrà avvenire anche per mezzo di trasmissione e comunicazione di dati a terzi autorizzati al trattamento, in quanto incaricati di svolgere o fornire specifici servizi strettamente funzionali a quelli della Banca, quali altre società del Gruppo o società in outsourcing.

I Suoi dati personali saranno prevalentemente trattati all'interno del territorio dell'Unione Europea. La Banca si riserva di trasferire i Suoi dati personali verso Paesi extra UE per soddisfare eventuali esigenze di natura tecnica ed organizzativa. In ogni caso, il trattamento dei Suoi dati avverrà nel rispetto delle adeguate garanzie previste dalla vigente normativa come le decisioni di adeguatezza della Commissione Europea, clausole contrattuali tipo approvate dalla Commissione Europea o altri strumenti legali.

Diritti

Le ricordiamo che per far valere i Suoi diritti di cui agli artt. da 15 a 22 del GDPR potrà rivolgersi all'indirizzo protezionedati@bancobpm.it ovvero alla sede legale della Banca in Piazza F. Meda n. 4, 20121 Milano all'attenzione del Responsabile Protezione Dati. Qualora intendesse esercitare il diritto di opposizione di cui all'art. 21 del GDPR, la Banca si asterrà dal trattare ulteriormente i Suoi dati personali a meno che non vi siano motivi legittimi per procedere al trattamento, prevalenti sui Suoi interessi, diritti e sulle Sue libertà fondamentali.

L'informativa completa è disponibile sul sito istituzionale, sezione privacy.