Comunicazione della Banca d'Italia in materia di accesso ai conti di pagamento (previsto dalla Direttiva PSD2): istruzioni per l'esenzione dall'obbligo di realizzare la procedura di contingency ("fall-back solution").

Il Regolamento delegato 2018/389 della Commissione Europea del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 (PSD2) per quanto riguarda le norme tecniche per l'autenticazione forte del cliente e gli standard aperti di comunicazione (nel seguito RTS), prevede che tutti i prestatori di servizi di pagamento che detengono conti accessibili online (Account Servicing Payment Service Providers o ASPSP) predispongano, entro il 14 settembre 2019, un'interfaccia di accesso per consentire a terze parti (Third Party Providers o TPP)[1] di svolgere la propria attività.

Tale obbligo è volto a garantire un canale sicuro di autenticazione e comunicazione tra l'ASPSP e il TPP e può essere alternativamente soddisfatto attraverso:

a) la realizzazione ex novo di un'interfaccia online dedicata all'accesso dei TPP;

b) l'adattamento di interfacce già disponibili ai clienti per accedere direttamente ai propri conti di pagamento online.

In caso di adozione dell'interfaccia dedicata (opzione sub a), gli RTS impongono all'ASPSP di assicurare ai TPP l'accesso ai conti anche attraverso un meccanismo alternativo (cd. soluzione di fall-back, cfr. art. 33, par.4), da utilizzare in caso di indisponibilità o di prestazioni inadeguate dell'interfaccia dedicata. Ai sensi dell'art. 33, par. 6 degli RTS, la Banca d'Italia può esentare gli ASPSP dall'obbligo di realizzare questa interfaccia di fall-back se sono soddisfatte le condizioni previste dal medesimo articolo[2].

La Banca d'Italia intende adottare un termine per la conclusione del procedimento amministrativo su istanza di parte per l'esenzione dalla soluzione di fall-back inferiore a quello ordinariamente previsto dal Regolamento della Banca d'Italia del 25 giugno 2008 e successive modifiche (indicativamente 45 giorni)[3].

Gli RTS prevedono che gli ASPSP rendano disponibili le interfacce dedicate, a fini di test, al più tardi entro il 14 marzo 2019, e siano in grado di dimostrare che le interfacce siano state "ampiamente utilizzate", in ambiente di produzione, per almeno 3 mesi prima di poter avanzare l'istanza di esenzione dalla soluzione di fall-back.

Per poter rispettare tali tempistiche stringenti, prevedendo anche sufficiente margine di tempo per permettere alla Banca d'Italia l'esame delle istanze, è necessario che i test di funzionalità delle interfacce siano avviati con tempestività, preferibilmente entro i primi giorni del mese di febbraio, e che le interfacce siano messe in esercizio entro il primo giugno.

---

[1] I TPP sono gli intermediari che prestano servizi di disposizione degli ordini di pagamento (Payment Initiation Services Providers o PISP), gli intermediari che offrono servizi di informazione sui conti (Account Information System Providers o AISP), i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta (Card-Based Payment Instrument Issuers o CBPII).

[2] Le condizioni per l'esenzione specificate all'articolo 33, par. 6 dell'RTS sono dettagliate negli orientamenti dell'ABE, "Guidelines on the exemption from the contingency mechanism under the RTS on SCA and CSC", pubblicate il 4 dicembre 2018. Il recepimento degli Orientamenti nelle disposizioni di vigilanza applicabili alle banche, agli istituti di pagamento e di moneta elettronica sarà oggetto di un apposito documento di consultazione.

[3] L'unità organizzativa responsabile è il Servizio Rapporti istituzionali di vigilanza.

Al fine di agevolare l'esame della documentazione, è stata predisposta la modulistica allegata, che consente di armonizzare e rappresentare in forma sintetica le informazioni richieste e che andrà inviata in più fasi (cfr. infra Domande di esenzione dalla soluzione di fall-back).

Secondo quanto previsto dalla Circ. n. 285 "Disposizioni di vigilanza per le banche" del 17 dicembre 2013 e dalle "Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica" in materia di esternalizzazione di funzioni operative importanti, gli intermediari che intendono ricorrere a soluzioni di soggetti terzi per l'accesso ai conti sono tenuti ad inviare alla Banca d'Italia una comunicazione preventiva. A questo fine, per gli intermediari che aderiscono a una piattaforma multi-operatore offerta dal mercato e sorvegliata ai sensi dell'Art. 146 del TUB, la comunicazione è effettuata con la trasmissione delle informazioni di cui al Modulo 1 - Parte 1, purché la piattaforma abbia comunicato agli aderenti di aver fornito alla funzione di Sorveglianza sul sistema dei pagamenti della Banca d'Italia ex Art. 146 del TUB le informazioni necessarie a valutarne la conformità al quadro normativo. Questi intermediari attestano il rispetto delle condizioni previste dalle disposizioni di vigilanza applicabili e, ove previsto, presentano l'analisi dei rischi entro il 14 marzo 2019, in contemporanea con l'invio del primo modulo di documentazione previsto per la richiesta di esenzione.

Infine, con la presente comunicazione si forniscono alcuni chiarimenti sull'applicazione dell'articolo 17 dell'RTS "Processi e protocolli di pagamento sicuri per le imprese", con riferimento alle esenzioni dal requisito di autenticazione forte del cliente per gli intermediari che prestino servizi di pagamento avvalendosi di processi o protocolli dedicati ai pagamenti "corporate" (cfr. infra Esenzioni dall'autenticazione forte del cliente per i pagamenti corporate).

Domande di esenzione dalla soluzione di fall-back

Le domande di esenzione dalla realizzazione della soluzione di fall-back andranno inviate secondo le seguenti modalità e tempistiche:

1) Parte 1 - INFORMAZIONI SULL'INTERFACCIA DEDICATA (cfr. "Modulo 1 - Parte 1"): vanno forniti i dettagli, previsti dagli orientamenti dell'ABE, relativi alle soluzioni adottate. Il modulo compilato va inoltrato non appena le informazioni in esso richieste sono disponibili e comunque non oltre la data del 14 marzo 2019. Ai fini della comunicazione preventiva per l'esternalizzazione di funzioni operative importanti, gli intermediari che aderiscono a una piattaforma multi-operatore offerta dal mercato e sorvegliata ai sensi dell'Art. 146 del TUB attestano il rispetto delle condizioni previste dalle disposizioni di vigilanza in materia di esternalizzazione di funzioni operative importanti. Le banche presentano l'analisi dei rischi prevista dalla Circ. n. 285 "Disposizioni di vigilanza per le banche" del 17 dicembre 2013, sempre entro il termine del 14 marzo, secondo le consuete modalità;

2) Parte 2 – INFORMAZIONI SUI TEST E SUGLI STRESS TEST (cfr. "Modulo 2 - Parte 2"): vanno fornite evidenze circa il risultato degli stress test e dei test di funzionalità previsti dall'articolo 30(5) dell'RTS; va inoltre confermato l'avvio in esercizio, al più tardi entro il primo giugno, delle interfacce dedicate. Il modulo va inviato entro la data del 14 giugno 2019;

3) Parte 3 - UTILIZZO DELLE INTERFACCE DEDICATE (cfr. "Modulo 3 - Parte 3"): vanno inviate le evidenze conclusive circa il requisito, previsto dagli orientamenti ABE (par.7), di ampio utilizzo delle interfacce dedicate. Tale documentazione va inoltrata non appena disponibile e comunque non oltre il primo agosto 2019. Tale ultimo invio di documentazione costituisce l'atto formale di presentazione dell'istanza di esenzione. Se le evidenze sul requisito di utilizzo presentate in tale fase si riferiscono a un periodo inferiore ai tre mesi previsti dall'RTS, l'intermediario fornirà un aggiornamento di tale documentazione, al più tardi durante i primi giorni di settembre, solo nel caso in cui siano emersi problemi, o elementi di rilevante novità, nell'utilizzo dell'interfaccia non già evidenziati.

Le istanze, sottoscritte dal legale rappresentante, vanno presentate dalle capogruppo di gruppi bancari (per conto proprio e di tutti i prestatori di servizi di pagamento appartenenti al gruppo aventi sede in Italia), dalle banche individuali non appartenenti a gruppi, dalle succursali di banche extracomunitarie, dagli Istituti di Pagamento e dagli IMEL non appartenenti a gruppi bancari. Gli intermediari italiani inclusi nella vigilanza consolidata di una banca o società di partecipazione finanziaria (mista) madre nell'UE nonché le capogruppo di gruppi bancari che abbiano filiazioni in altri Stati membri dell'UE specificano nella prima parte dell'istanza se analoga richiesta è stata o sarà presentata per la stessa interfaccia dedicata ad altre autorità, indicandone il nome.

Le istanze andranno inviate via PEC alla casella RIV@pec.bancaditalia.it e recheranno nell'oggetto il codice abi dell'intermediario, la dizione "esenzione dalla soluzione di fallback" e la parte della modulistica in esse contenuta (parte 1,2,3). La Banca d'Italia prenderà in considerazione, oltre alle informazioni prodotte, le informazioni rese disponibili dalle piattaforme multi-operatore e ogni altro dato a propria disposizione; essa si riserva inoltre di richiedere qualsiasi chiarimento o informazione necessari alla finalizzazione dell'istanza.

Esenzioni dall'autenticazione forte del cliente per i pagamenti corporate

In base all'articolo 17 dell'RTS, ai prestatori di servizi di pagamento è consentito non applicare l'autenticazione forte del cliente (Strong Customer Authentication o SCA) nei confronti di clientela corporate, se utilizzano processi o protocolli di pagamento dedicati - resi disponibili unicamente a clienti diversi dai consumatori - nel caso in cui le autorità abbiano accertato che tali processi o protocolli garantiscano i livelli di sicurezza previsti dalla direttiva PSD2.

Al riguardo, sulla base di un approccio condiviso a livello europeo, si fa presente che per poter usufruire di tale esenzione è necessario che gli operatori rispettino tre criteri di carattere generale: i) sia assicurato il monitoraggio delle transazioni; ii) i canali di comunicazione sicura siano conformi ai requisiti previsti in materia di crittografia, riservatezza e integrità delle credenziali di sicurezza personalizzate dei clienti; iii) siano applicati meccanismi di autenticazione sicura.

Le soluzioni adottate dovranno essere accuratamente descritte nell'ambito di un documento di valutazione del rischio operativo e di sicurezza, che dovrà essere inviato annualmente alla Banca d'Italia, secondo quanto previsto dagli Orientamenti ABE[4].

Eventuali richieste di chiarimento in merito a tutto quanto precede potranno essere inviate alla casella mail PSD2_Procedimentodiesenzione@bancaditalia.it.

[4] Cfr. "Orientamenti dell'ABE sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento" (EBA/GL2017/17). Per il recepimento degli Orientamenti nelle Disposizioni di vigilanza per gli istituti di pagamento e di moneta elettronica, cfr. http://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2018/disposizioni-istituti-imel/index.html. Il recepimento per le banche sarà oggetto di un apposito documento di consultazione.