BANCA D'ITALIA
EUROSISTEMA

Vigilanza bancaria e finanziaria

Documento per la consultazione

MODIFICHE ALLA CIRCOLARE N. 285 (DISPOSIZIONI DI VIGILANZA PER LE BANCHE) E RECEPIMENTO DEGLI ORIENTAMENTI EBA/GL/2017/10 E EBA/GL/2017/17 E DELLE RACCOMANDAZIONI EBA/REC/2017/03

RECEPIMENTO DEGLI ORIENTAMENTI EBA EBA/GL/2018/07 PER LE BANCHE E GLI ALTRI PRESTATORI DI SERVIZI DI PAGAMENTO

Il documento illustra le modifiche che la Banca d'Italia intende effettuare sulle Disposizioni di vigilanza per le banche per recepire gli Orientamenti EBA/GL/2017/10 e EBA/GL/2017/17 emanati dall'Autorità Bancaria Europea in attuazione della Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno e per dare attuazione alle Raccomandazioni EBA/REC/2017/03 emesse dalla medesima Autorità in materia di esternalizzazione a fornitori di servizi cloud.

Si comunica inoltre l'intenzione di recepire integralmente nelle disposizioni applicabili alle banche e agli altri prestatori di servizi di pagamento – Poste Italiane S.p.A. per l'attività di Bancoposta, istituti di pagamento, istituti di moneta elettronica e intermediari finanziari autorizzati alla prestazione di servizi di pagamento – gli Orientamenti EBA/GL/2018/07 pubblicati, nella sola versione in inglese, lo scorso 4 dicembre.

Osservazioni, commenti e proposte possono essere trasmessi, entro 30 *giorni dalla data di pubblicazione del presente documento, alla Banca d'Italia:*

- *qualora si disponga di posta elettronica certificata (PEC), in formato elettronico all'indirizzo ram@pec.bancaditalia.it; oppure*
- *in forma cartacea all'indirizzo Servizio Regolamentazione e Analisi Macroprudenziale, Divisione Regolamentazione II, via Nazionale 91, 00184 ROMA. In tal caso, una copia in formato elettronico dovrà essere contestualmente inviata al seguente indirizzo e-mail:servizio.ram.regolamentazione2@bancaditalia.it.*

Per agevolare la valutazione dei contributi alla consultazione, si invitano i rispondenti a indicare esplicitamente i punti del documento a cui le osservazioni, i commenti e le proposte si riferiscono.

I commenti ricevuti durante la consultazione saranno pubblicati sul sito internet della Banca d'Italia. I partecipanti alla consultazione possono chiedere che, per esigenze di riservatezza, i propri commenti non siano pubblicati, oppure siano pubblicati in forma anonima. Una generica indicazione di confidenzialità eventualmente presente in calce alle comunicazioni inviate via posta elettronica non sarà considerata una richiesta di non divulgare i commenti. I contributi ricevuti oltre il termine sopra indicato non saranno presi in considerazione.

Dicembre 2018

Le modifiche alla Circolare n. 285/2013 (nel seguito "Circolare 285") poste in consultazione sono volte a dare attuazione nell'ordinamento nazionale di vigilanza ad alcuni atti di secondo livello emanati dall'Autorità Bancaria Europea (*European Banking Authority* – EBA).

Il documento di consultazione è suddiviso in tre parti:

- **Parte I**: recepimento degli Orientamenti dell'EBA in materia di segnalazione dei gravi incidenti del 19 dicembre 2017 (EBA/GL/2017/10) e degli Orientamenti dell'EBA sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento del 12 gennaio 2018 (EBA/GL/2017/17);
- **Parte II**: recepimento delle Raccomandazioni dell'EBA in materia di esternalizzazione a fornitori di servizi *cloud* del 28 marzo 2018 (EBA/REC/2017/03); e
- **Parte III**: recepimento delle "*Guidelines on the conditions to be met to benefit from an exemption from contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)*" dell'EBA (EBA/GL/2018/07).

Le disposizioni europee, che vengono integralmente recepite, offrono limitati spazi di discrezionalità alle autorità nazionali; l'Autorità Bancaria Europea ha già effettuato l'analisi d'impatto e sottoposto a pubblica consultazione sia gli Orientamenti sia le Raccomandazioni ([1]). Per queste ragioni: i) si fa rinvio, per l'analisi di impatto della regolamentazione ("AIR"), alle valutazioni dell'EBA; ii) la consultazione ha un termine di 30 giorni, inferiore a quello ordinario di 60 giorni previsto dall'articolo 4, comma 4, del Regolamento della Banca d'Italia del 24 marzo 2010.

Di seguito si descrivono sinteticamente le principali modifiche e integrazioni apportate alla Circolare 285.

*** * ***

([1]) Con riferimento alle analisi di impatto effettuate dall'EBA si rinvia rispettivamente a: (i) https://www.eba.europa.eu/-/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions; (ii) https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2/-/regulatory-activity/consultation-paper; (iii) https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2/-/regulatory-activity/consultation-paper.

I. ATTUAZIONE DEGLI ORIENTAMENTI EBA/GL/2017/10 E EBA/GL/2017/17

Nell'ambito dell'attuazione della Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno ("PSD2") ([2]), l'EBA ha emanato, tra gli altri, i seguenti atti normativi di secondo livello:

- gli Orientamenti sulle misure di sicurezza per i rischi operativi e per la sicurezza dei servizi di pagamento (EBA/GL/2017/17): questi orientamenti disciplinano i presìdi che i prestatori di servizi di pagamento devono adottare per attenuare i rischi operativi e di sicurezza relativi alla prestazione di servizi di pagamento;
- gli Orientamenti in materia di segnalazione dei gravi incidenti (EBA/GL/2017/10): essi stabiliscono i criteri, le soglie e la metodologia che i prestatori di servizi di pagamento devono utilizzare per determinare se un incidente operativo o di sicurezza va considerato grave ed essere conseguentemente notificato all'Autorità competente dello Stato membro di origine.

Per gli istituti di pagamento e gli istituti di moneta elettronica la Banca d'Italia sta curando il recepimento di questi atti nell'ambito della modifica delle disposizioni applicabili a questi intermediari a seguito della PSD2 ([3]).

Per le banche, la Banca d'Italia intende recepire integralmente questi Orientamenti, con un rinvio contenuto nei Capitoli 4 ("Sistema informativo") e 5 ("Continuità operativa") del Titolo IV, Parte Prima, della Circolare 285. Le nuove disposizioni si applicherebbero anche a Poste Italiane s.p.a. per l'attività di Bancoposta.

Il contenuto delle disposizioni in materia di "Sistema informativo" e "Continuità operativa" già presenti nella Circolare 285 è coerente, in larga parte, con quanto previsto dagli Orientamenti sulle misure di sicurezza per i rischi operativi e per la sicurezza dei servizi di pagamento. Le Disposizioni di vigilanza sono quindi oggetto soltanto di interventi di raccordo tra gli obblighi vigenti e quelli introdotti dagli Orientamenti.

Nel recepire gli Orientamenti sulla segnalazione dei gravi incidenti relativi ai servizi di pagamento, la Banca d'Italia ritiene di confermare l'impostazione attualmente prevista per i gravi incidenti di sicurezza informatica per il complesso delle attività e servizi bancari, in base alla quale le banche effettuano direttamente una comunicazione all'autorità di vigilanza; in questo modo le banche sono incentivate a rafforzare i presìdi adottati e ad accrescere il grado di consapevolezza degli organi aziendali. Non verrebbe quindi esercitata la discrezionalità che consente agli intermediari di delegare ad un terzo l'invio della comunicazione, inclusa la comunicazione in forma "aggregata" ([4]). Per le banche appartenenti a gruppi, le capogruppo continueranno ad effettuare la segnalazione su base consolidata per le componenti del gruppo. La Banca d'Italia pubblicherà sul proprio sito web gli schemi aggiornati per la segnalazione e le relative istruzioni di compilazione

([2]) Per l'elencazione completa degli atti normativi di secondo livello emanati ai sensi della PSD2 si rinvia al sito dell'EBA, http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money.
([3]) Il recepimento degli Orientamenti nelle disposizioni applicabili agli istituti di pagamento e di moneta elettronica è oggetto di un distinto documento di consultazione; cfr. http://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2018/disposizioni-istituti-imel/index.html
([4]) Cfr., Orientamento 3.2 degli Orientamenti EBA in materia di segnalazione dei gravi incidenti (EBA/GL/2017/10).

per agevolare la raccolta e la rappresentazione delle informazioni necessarie ai nuovi adempimenti. Gli schemi e le istruzioni sostituiranno quelli attualmente in vigore: la Banca d'Italia ha infatti optato per l'adozione di una procedura di notifica unica, indipendente dalla tipologia di incidente occorso, che riguardi i servizi di pagamento o altre aree di attività. Le banche produrranno le segnalazioni secondo il nuovo schema al ricorrere del primo incidente successivo all'entrata in vigore delle disposizioni ora poste in consultazione.

II. ATTUAZIONE DELLE RACCOMANDAZIONI EBA/REC/2017/03

Lo schema di disposizioni in consultazione modifica la Circolare 285 per dare attuazione alle Raccomandazioni EBA in materia di esternalizzazione a fornitori di servizi *cloud*, pubblicate il 28 marzo 2018. Queste integrano le linee guida sull'esternalizzazione emanate il 14 dicembre 2006 dal Comitato delle Autorità Europee di Vigilanza Bancaria – CEBS e introducono presìdi specifici per i casi di esternalizzazione dei servizi in *cloud computing*.

Le Raccomandazioni sono attuate mediante rinvio: nello schema di disposizioni verrebbe quindi previsto in via generale l'obbligo per le banche di attenersi a quanto disciplinato dalle Raccomandazioni.

Le vigenti Disposizioni di vigilanza per le banche includono norme di dettaglio per i casi di esternalizzazione del sistema informativo e di risorse ICT critiche, inclusi quelli di utilizzo di servizi di *cloud computing* ([5]). Queste disposizioni sono in larga misura già conformi a quanto previsto dalle Raccomandazioni e, pertanto, sono state oggetto soltanto di interventi di coordinamento mirati.

Le principali modifiche riguardano l'introduzione degli obblighi, per la banca, di:

- istituire e mantenere specifici registri di tutte le attività rilevanti e non rilevanti esternalizzate a fornitori di servizi *cloud*, a livello individuale e di gruppo;
- valutare i rischi connessi al paese in cui sono forniti o conservati i dati (*e.g.* rischi legali o rischi di elusione o mancata applicazione delle norme in materia fallimentare o in materia di protezione dei dati).

III. RECEPIMENTO DEGLI ORIENTAMENTI EBA/GL/2018/07 SULLE CONDIZIONI DA SODDISFARE PER BENEFICIARE DELL'ESENZIONE DALL'OBBLIGO DI PREDISPORRE IL MECCANISMO DI EMERGENZA DI CUI ALL'ARTICOLO 33(6) DEL REGOLAMENTO (EU) 2018/389

In attuazione della PSD2, la Commissione europea ha adottato il Regolamento Delegato (UE) n. 2018/389 che contiene le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli *standard* aperti di comunicazione comuni e sicuri (di seguito il "Regolamento Delegato"); in base al Regolamento Delegato, i prestatori di servizi di pagamento di radicamento di conti di pagamento ("*Account Servicing Payment Service Providers*" o "ASPSPs") devono

([5]) Circolare 285/2013, Parte Prima, Titolo IV, Capitolo 4, Sezione VI.

predisporre, entro il 14 settembre 2019, un'interfaccia di accesso per consentire agli intermediari che prestano servizi di disposizione degli ordini di pagamento e/o di informazione sui conti nonché ai prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta (nel seguito congiuntamente "*third party providers*" o "TPPs") di svolgere la propria attività.

Questo obbligo è volto a garantire un canale sicuro di autenticazione e comunicazione tra l'ASPSPs e i TPPs e può essere alternativamente soddisfatto attraverso:

i. la realizzazione *ex novo* di un'interfaccia dedicata all'accesso dei TPPs (Opzione 1); ovvero
ii. l'adattamento dell'interfaccia utilizzata dall'ASPSP per l'autenticazione e la comunicazione con i propri clienti (Opzione 2).

In caso di adozione dell'interfaccia dedicata (Opzione 1), il Regolamento impone all'ASPSP di assicurare ai TPPs la possibilità di accedere attraverso l'interfaccia per i clienti in caso di indisponibilità o di prestazioni inadeguate dell'interfaccia dedicata (cd. *fall-back option*, cfr. art. 33 del Regolamento); le Autorità nazionali competenti possono esentare gli ASPSPs, previa consultazione con l'EBA, dal predisporre i meccanismi di *fall-back* quando le interfacce dedicate rispettano alcune condizioni di funzionalità (indicate all'art. 33(6) del Regolamento).

Per chiarire le modalità applicative dei criteri fissati nell'art. 33(6) del Regolamento e garantirne un'applicazione uniforme, l'EBA ha elaborato e posto in consultazione le "*Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)*".

La versione finale degli Orientamenti è stata pubblicata sul sito dell'EBA nella sola versione inglese lo scorso 4 dicembre (EBA/GL/2018/07). In attesa che si concluda il processo di traduzione nelle lingue ufficiali degli Stati membri dell'Unione Europea ([6]), si comunica sin d'ora l'intenzione di recepire integralmente questi Orientamenti prevedendone l'applicazione a banche, Poste Italiane S.p.A. per l'attività di Bancoposta, istituti di pagamento, istituti di moneta elettronica e intermediari finanziari autorizzati alla prestazione di servizi di pagamento, così da favorire la creazione di un quadro normativo nazionale unitario ed organico e assicurare il tempestivo allineamento alle disposizioni europee. Considerato che gli ASPSPs dovranno predisporre l'interfaccia dedicata e l'eventuale *fall-back option* entro il 14 settembre 2019, la Banca d'Italia renderà noto, con separata comunicazione agli operatori, i tempi e le modalità per la presentazione dell'eventuale richiesta di esenzione dalla predisposizione della soluzione di *fall-back*.

([6]) Dalla pubblicazione degli Orientamenti nelle lingue ufficiali degli Stati membri decorre infatti il termine di due mesi per le autorità competenti entro cui comunicare all'EBA l'intenzione di conformarsi al contenuto degli Orientamenti.