Circolare n. 285 del 17 dicembre 2013 «Disposizioni di Vigilanza per le banche» - 28° aggiornamento – Recepimento degli Orientamenti EBA/GL/2017/10, EBA/GL/2017/17, EBA/GL/2018/07 e delle Raccomandazioni EBA/REC/2017/03

1. Premessa

Con il presente aggiornamento si modificano i Capitoli "Il sistema informativo" (Parte Prima, Titolo IV, Cap.4) e "Continuità operativa" (Parte Prima, Titolo IV, Cap. 5) della Circolare n. 285 del 17 dicembre 2013 "Disposizioni di vigilanza per le banche".

Le modifiche recepiscono nella normativa nazionale i seguenti atti di secondo livello emanati dall'Autorità Bancaria Europea (European Banking Authority – EBA):

1. gli Orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza dei pagamenti (EBA/GL/2017/17) e gli Orientamenti in materia di segnalazione dei gravi incidenti (EBA/GL/2017/10) e gli Orientamenti sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza a norma dell'articolo 33, par. 6, del Regolamento (UE) 2018/389 (EBA/GL/2018/07), attuativi della Direttiva 2015/2366 del Parlamento europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno (PSD2); e
2. le Raccomandazioni in materia di esternalizzazione a fornitori di servizi *cloud* (EBA/REC/2017/03).

Le modifiche alle Disposizioni di vigilanza per le banche sono state sottoposte a consultazione pubblica. Sul sito internet della Banca d'Italia sono pubblicati il resoconto della consultazione e le osservazioni pervenute per le quali non è stata chiesta la riservatezza.

Non è stata effettuata l'analisi di impatto tenuto conto che gli atti di secondo livello recepiti nelle Disposizioni di vigilanza per le banche offrono limitati spazi di discrezionalità e che l'analisi di impatto è stata già effettuata dall'EBA.

Sono altresì disciplinati i procedimenti amministrativi introdotti a seguito dell'adozione del Regolamento delegato 2018/389 della Commissione europea, 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.

2. Contenuto

Gli **Orientamenti dell'EBA in materia di misure di sicurezza per i rischi operativi e di sicurezza dei pagamenti** definiscono i presìdi che, nel rispetto del principio di proporzionalità, gli intermediari che prestano servizi di pagamento adottano per attenuare e gestire i rischi operativi e di sicurezza derivanti dalla prestazione di questi servizi. Le disposizioni in materia di sistema informativo, gestione del rischio informativo e le regole in materia di sicurezza e continuità dell'attività sono oggetto di interventi di raccordo per assicurare il coordinamento con la nuova normativa e mantenere l'unitarietà della valutazione e gestione dei rischi aziendali.

Gli **Orientamenti in materia di segnalazione dei gravi incidenti** definiscono i criteri e la metodologia per la classificazione dei gravi incidenti di sicurezza relativi ai pagamenti. I nuovi criteri sono integrati nel generale quadro della disciplina in materia di rilevazione e notifica alla Banca d'Italia degli incidenti di sicurezza informatica per il complesso delle attività svolte dalla banca. Le banche effettuano direttamente la segnalazione; non è esercitata la discrezionalità che consente agli intermediari di delegare a un terzo l'invio della comunicazione, inclusa la comunicazione in forma "aggregata".

Gli **Orientamenti sulle condizioni per beneficiare dell'esenzione del meccanismo di emergenza** ("interfaccia di *fall-back*") **dell'articolo 33, par. 6, del Regolamento (UE) 2018/389** specificano i criteri al ricorrere dei quali i prestatori di servizi di pagamento che detengono conti accessibili online possono essere esonerati dall'obbligo di predisporre l'interfaccia di emergenza prevista dall'art. 33, par. 4, del Regolamento (UE) 2018/389 della Commissione europea, 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 (1).

Le **Raccomandazioni EBA in materia di esternalizzazione a fornitori di servizi *cloud*** integrano il quadro generale in materia di esternalizzazione e introducono presìdi specifici per i casi di esternalizzazione dei servizi in *cloud computing*.

3. Disciplina dei procedimenti amministrativi ai sensi degli articoli 2 e 4 della legge 7 agosto 1990, n. 241, e successive modificazioni

Ai sensi dell'art. 33, par. 6, del Regolamento 2018/389, la Banca d'Italia può esentare i prestatori di servizi di pagamento che detengono conti accessibili *online* dall'obbligo di realizzare l'interfaccia di *fall-back* prevista dall'art. 33, par. 4, del Regolamento. Con il presente aggiornamento sono pertanto introdotti i seguenti procedimenti amministrativi (2):

- esenzione dall'obbligo di predisporre l'interfaccia di *fall-back* prevista dall'art. 33, par. 4 del Regolamento delegato 2018/389 della Commissione Europea del 27 novembre 2017, ai sensi dell'art. 33, par. 6 del Regolamento delegato 2018/389 (termine: 45 giorni);
- revoca dell'esenzione dall'obbligo di predisporre l'interfaccia di *fall-back* prevista dall'art. 33, par. 4 del Regolamento delegato 2018/389 della Commissione Europea del 27 novembre 2017, ai sensi dell'art. 33, par. 7 del Regolamento delegato 2018/389 (termine: 45 giorni).

L'Unita organizzativa responsabile dei procedimenti citati è il Servizio Rapporti Istituzionali di Vigilanza della Banca d'Italia.

4. Entrata in vigore

Le modifiche contenute nel presente aggiornamento entrano in vigore il giorno successivo a quello della pubblicazione sul sito internet della Banca d'Italia.

[1] Il Regolamento 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) di svolgere la propria attività.

[2] Le istanze, sottoscritte dal legale rappresentante, sono 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. Le banche italiane, incluse 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.