Comunicazione del 29 ottobre 2021. Attuazione per i prestatori di servizi di pagamento degli Orientamenti aggiornati dell'EBA in materia di segnalazione dei gravi incidenti ai sensi della direttiva PSD2 (EBA/GL/2021/03).

1. Premessa

L'articolo 96, paragrafo 3, della direttiva PSD2 ([1]) conferisce all'EBA il mandato di predisporre, in collaborazione con la Banca centrale europea, Orientamenti (*Guidelines*) concernenti la segnalazione dei gravi incidenti operativi e di sicurezza riguardanti i servizi di pagamento. In data 10 giugno 2021 l'EBA ha emanato gli **Orientamenti aggiornati in materia di segnalazione dei gravi incidenti ai sensi della direttiva PSD2** ([2]) che abrogano e sostituiscono i precedent Orientamenti del 2017 ([3]) e che sono applicabili a partire dal 1° gennaio 2022.

Con la presente comunicazione la Banca d'Italia dà attuazione, con riferimento ai prestatori di servizi di pagamento, agli Orientamenti aggiornati dell'EBA in materia di segnalazione dei gravi incidenti ai sensi della PSD2 ([4]).

Gli Orientamenti si applicano alle banche, alle succursali di banche extracomunitarie, agli istituti di pagamento, agli istituti di moneta elettronica e a Bancoposta.

In continuità con il quadro normativo previgente, i prestatori di servizi di pagamento effettuano direttamente la segnalazione alla Banca d'Italia ([5]) secondo le istruzioni operative dalla stessa definite ([6]). Per le banche, inoltre, gli Orientamenti continuano ad essere 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.

2. Contenuto

Gli Orientamenti stabiliscono i criteri per la classificazione dei gravi incidenti operativi o di sicurezza, nonché il contenuto, il formato e le procedure per la comunicazione di questi incidenti alle autorità nazionali. Rispetto alla precedente versione, gli Orientamenti aggiornano il *framework* per rafforzare e, allo stesso tempo, semplificare il regime di segnalazione dei gravi incidenti alla luce dell'esperienza maturata.

In particolare, gli Orientamenti introducono un nuovo criterio segnaletico relativo alla violazione della sicurezza della rete o dei sistemi informativi, con l'obiettivo di catturare in maniera più adeguata gli incidenti derivanti da un'azione dolosa che abbia compromesso la disponibilità, l'autenticità, l'integrità o la riservatezza della rete o dei sistemi informativi (inclusi i dati) relativi alla prestazione di servizi di pagamento.

Sono inoltre introdotte le seguenti semplificazioni negli obblighi in capo agli intermediari:

- l'ampliamento delle tempistiche per l'invio del report iniziale (che va trasmesso non più entro 4 ore dal momento in cui l'incidente viene rilevato, ma da quando viene classificato come grave) e del report finale (da trasmettere 20 giorni lavorativi dopo la chiusura dell'incidente, anziché dopo 2 settimane). Le banche significative continuano a effettuare la notifica del report iniziale entro 2 ore dal momento della classificazione

[1] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno.

[2] EBA *Revised Guidelines on major incident reporting under PSD2* (EBA/GL/2021/03). Il testo è disponibile sul sito dell'EBA al seguente link: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-majorincidents-reporting-under-psd2.

[3] Orientamenti dell'EBA in materia di segnalazione di gravi incidenti ai sensi della PSD2 (EBA/GL/2017/10), emanati dall'EBA il 27 luglio 2017.

[4] Cfr. Circolare 285, Parte I, Tit. IV, Cap. 4, Sez. IV, par. 6, e Sez. VII; Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, Cap. VI.

[5] Non è pertanto possibile delegare a un terzo l'invio della comunicazione.

[6] Cfr. "Istruzioni per la segnalazione dei gravi incidenti di sicurezza informativa", in corso di aggiornamento, disponibile all'indirizzo: https://www.bancaditalia.it/statistiche/raccolta-dati/segnalazioni/rilevazioni-vigilanza/index.html.

dell'incidente per garantire l'allineamento con quanto già richiesto dalla Banca centrale europea con riferimento agli incidenti *cyber*;

- la limitazione dell'obbligo di inviare report intermedi periodici soltanto nei casi in cui la durata dell'incidente grave si prolunghi oltre i tre giorni lavorativi;
- l'innalzamento delle soglie operative, relative al volume di transazioni interessate, oltre le quali l'incidente deve essere classificato come grave;
- l'allineamento della tassonomia adottata a quelle di altri sistemi di segnalazione degli incidenti sviluppati nell'UE (in particolare, Agenzia dell'Unione europea per la cybersecurity – ENISA; Banca centrale europea).

* * *

Gli Orientamenti sono stati già sottoposti a consultazione pubblica e ad analisi di impatto della regolamentazione a livello europeo ([7]). Stante la natura contenuta delle modifiche e tenuto conto che le scelte operate dalla Banca d'Italia con riguardo all'obbligo per i prestatori di servizi di pagamento di effettuare la segnalazione direttamente, nonché per le banche di integrare gli Orientamenti nel quadro degli incidenti di sicurezza informatica per il complesso delle attività svolte, si pongono in linea di continuità con il regime previgente, non è stata condotta una nuova consultazione pubblica né un'analisi di impatto della regolamentazione, in linea con quanto previsto nel Regolamento della Banca d'Italia sugli atti normativi ([8]).

La presente comunicazione ha natura di atto normativo di carattere generale vincolante per i destinatari ed entra in vigore il giorno della pubblicazione sul sito web della Banca d'Italia.

Le previsioni contenute negli Orientamenti si applicano a partire dal 1° gennaio 2022.

[7] Gli Orientamenti aggiornati sono stati sottoposti dall'EBA a consultazione pubblica da ottobre a dicembre 2020. Per l'analisi di impatto della regolamentazione, cfr. EBA, *Final Report on Revised Guidelines on major-incident reporting under PSD2*, disponibile sul sito dell'EBA al seguente link: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20major%20incident%20reporting%20under%20PSD2%20EBA-GL-202103/1014562/Final%20revised%20Guidelines%20on%20major%20incident%20reporting%20under%20PSD2.pdf

[8] Provvedimento della Banca d'Italia del 9 luglio 2019 "Regolamento recante la disciplina dell'adozione degli atti di natura normativa o di contenuto generale della Banca d'Italia nell'esercizio delle funzioni di vigilanza, ai sensi dell'articolo 23 della legge 28 dicembre 2005, n. 262", art. 8, comma 2, lett. a).