ABI Associazione Bancaria Italiana

Position Paper sulla consultazione della Banca d'Italia per le 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

E

Recepimento degli Orientamenti EBA/GL/2018/07 per le banche e per gli altri Prestatori di servizi di pagamento

8 Febbraio 2019

POSITION PAPER
2/2019

Introduzione

L'Associazione Bancaria Italiana (ABI) apprezza l'opportunità di formulare osservazioni e commenti sul documento contenente le modifiche alla Circolare n. 285 (disposizioni di vigilanza per le banche) che illustra le modifiche che la Banca d'Italia intende effettuare sulle Disposizioni di vigilanza per le banche per recepire gli atti di secondo livello emanati dall'Autorità Bancaria Europea (*European Banking Authority* - EBA), 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 (PSD2), e in particolare:

1. gli Orientamenti in materia di segnalazione dei gravi incidenti (**EBA/GL/2017/10**),
2. gli Orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento (**EBA/GL/2017/17**),
3. le Raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud (**EBA/REC/2017/03**),
4. gli Orientamenti sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza a norma dell'articolo 33, paragrafo 6, del Regolamento (UE) 2018/389 (norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri) (**EBA/GL/2018/07**).

L'ABI è consapevole che le disposizioni europee, in quanto integralmente recepite e già precedentemente sottoposte in pubblica consultazione dall'EBA, offrono limitati spazi di discrezionalità alle Autorità nazionali e tuttavia, pur non ravvedendosi elementi di elevato impatto, si coglie occasione per segnalare alcune osservazioni al riguardo.

L'ABI ha preparato il presente documento raccogliendo i commenti dei suoi Associati e avendo cura di indicare come richiesto un esplicito riferimento ai punti del documento cui le osservazioni si riferiscono. Il presente documento è stato quindi strutturato in tre parti coerentemente con la suddivisione del documento posto in consultazione dalla Banca d'Italia (di seguito Documento).

Parte I: recepimento degli Orientamenti EBA/GL/2017/10 e EBA/GL/2017/17

1. Titolo IV - Capitolo 4 – Sezione I – Paragrafo 3 - Definizioni

Con riferimento alle **definizioni** riportate al paragrafo 3 della sezione I del documento, si richiama quanto segue:

- Si ritiene che le **definizioni** presenti nel Titolo IV - Capitolo 4 – Sezione I – Paragrafo 3 del Documento e, in particolare quelle relative a **«*autenticazione*», «*autorizzazione*» e «*credenziali*»,** debbano essere rese **conformi a quelle di cui all'Articolo 4** della Direttiva 2015/2366/UE (**PSD2**) e all'art. 1 del D. Lgs. 11/2010, come modificato dall'art. 2, comma 1 del D. Lgs. 218/2017 di recepimento della PSD2 e agli Orientamenti EBA in materia di segnalazione dei gravi incidenti.

In particolare, si ritiene che tale allineamento debba essere realizzato nel rispetto di quanto indicato nelle Disposizioni transitorie di cui al *Titolo IV – Capitolo 4 – Sezione VII – Paragrafo 2* del Documento, laddove si riporta che: «*Le banche che prestano servizi di pagamento mediante uso del canale internet applicano le disposizioni degli Orientamenti finali in materia di sicurezza dei pagamenti via internet*» *secondo il regime transitorio delineato dall'ABE nella «Opinion on the transition from PSD1 to PSD2» del 19 dicembre 2017 e fino 14 settembre 2019, data di applicazione del Regolamento delegato della Commissione del 27 novembre 2017 n. 2018/389 riguardante le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri previsti dall'articolo 98, paragrafo 4, della direttiva 2015/2366/UE (PSD2)*».

Infatti, l'Opinione dell'EBA "*On the transition from PSD1 to PSD2*", richiamata nel Documento, specifica che, per garantire la continua applicabilità di requisiti di sicurezza stringenti, vale quanto segue:

- parte degli Orientamenti EBA sulla sicurezza dei pagamenti via internet del 19 Dicembre 2014 continuerà ad applicarsi oltre la data di entrata in vigore della PSD2 (13 gennaio 2018) e fino al 14 settembre 2019 (cd. transitional period II), data di entrata in vigore degli RTS in materia di Autenticazione forte del cliente e standard aperti di comunicazione comuni e sicuri.
- le parti degli Orientamenti del 2014 che sono state superate con la PSD2 (e quindi le relative definizioni), cesseranno di essere applicate a partire dal 13 gennaio 2018.

Pertanto, per chiarezza degli operatori si ritiene indispensabile l'allineamento con le definizioni di cui all'articolo 4 della PSD2 (e relativa normativa nazionale di recepimento).

- Si è consapevoli che l'EBA, nella versione finale degli Orientamenti ha accolto solo parzialmente l'osservazione pervenuta dal mercato (e avanzata anche da questa Associazione nella risposta alla consultazione sulla bozza di Orientamenti), relativa alla opportunità di limitare la segnalazione a incidenti che hanno ripercussioni gravi nel concreto e non in potenza e ha conseguentemente adattato la definizione di incidente grave. Tale definizione è ripresa nel Documento. Tuttavia, in relazione all'integrazione apportata alla definizione di «**grave incidente di sicurezza informatica**» e relativa alla dicitura «*[**..è probabile che derivi** …]*» si ribadisce che l'introduzione di una sorta di misurazione in termini probabilistici potrebbe portare ad un incremento del numero di accadimenti da segnalare (con conseguente maggiore onerosità sia per i prestatori di servizi di pagamento sia per l'Autorità nazionale competente) indipendentemente dal reale manifestarsi degli impatti ipotizzati e che, in congiunzione con le stringenti tempistiche di segnalazione e le maggiori informazioni da fornire nei tre report richiesti, potrebbero anche rilevarsi inattendibili a seguito di analisi più approfondite.Pertanto, anche in considerazione dei fini statistici della raccolta da parte dell'Autorità nazionale, si richiede di meglio circoscrivere nella definizione di «grave incidente di sicurezza informatica» la dicitura «***o è probabile che derivi***», così da chiarire che la segnalazione dovrà avvenire soltanto per gli incidenti con un reale impatto rilevato. L'obiettivo della scrivente è che il processo di segnalazione degli incidenti sia basato su criteri certi e univoci e non su valutazioni soggettive di

ipotetici impatti che metterebbero il vigilato nella condizione di non avere mai la certezza della necessità o meno di segnalare.

2. *Titolo IV - Capitolo 4 – Sezione IV – Paragrafo 3 – La sicurezza delle informazioni e delle risorse ICT*

Con riferimento a quanto riportato nel paragrafo 3 della sezione II del documento, si richiama quanto segue:

- Il secondo sottoparagrafo stabilisce che «*[…] i diritti di accesso sono accordati, di norma, secondo l'approccio dell'**accesso basato sulle funzioni** (c.d. role-based access control), previa formale autorizzazione. L'autorizzazione è rilasciata a personale adeguatamente addestrato e soggetto a monitoraggio […]*»

  A tal proposito, si ritiene opportuno segnalare che, nell'accezione più comune, con l'espressione «*role-based*» si fa riferimento ad una tecnica specifica di access control, probabilmente differente da quella che, si presume, si vuole indicare nel testo in consultazione.
  Al fine di evitare fraintendimenti tra gli operatori, a nostro avviso, potrebbe essere più efficace esplicitare il concetto in italiano, eliminando dunque il termine inglese «*role-based access control*», e chiarendo che le policy interne di assegnazione dei privilegi devono essere organizzate in modo tale da permettere una profilazione degli utenti coerente con quelle che sono le figure, i ruoli e le responsabilità ricoperti in azienda.

- Il nono sottoparagrafo stabilisce che «*[…] le procedure per **lo svolgimento delle operazioni** critiche, garantendo il rispetto dei principi del minimo privilegio e della segregazione dei compiti (ad es., specifiche procedure di abilitazione e di autenticazione, controlli di tipo four eyes (3), o di verifica giornaliera ex post). L'accesso a componenti critiche del sistema informativo da parte di utenti privilegiati o amministratori di sistema è effettuato attraverso procedure di autenticazione rafforzate, come l'autenticazione a più fattori ("autenticazione forte") (4)*»

  Si segnala che, la disposizione sopracitata potrebbe configurarsi come un'interpretazione più restrittiva rispetto al requisito già espresso all'interno degli orientamenti EBA sulle misure di sicurezza (orientamento 4.10), che annovera, a titolo esemplificativo, una serie di meccanismi di controllo sull'accesso privilegiato ai sistemi e l'autenticazione forte è uno di questi. Il testo in consultazione, dunque, introdurrebbe l'obbligo per gli intermediari di adottare l'autenticazione forte come specifica misura di sicurezza. A tal proposito, appare opportuno segnalare che quanto citato potrebbe avere un impatto rilevante sulle organizzazioni che potrebbero non godere di sistemi informativi adeguati per adempiere a tale disposizione.

- Il tredicesimo sottoparagrafo stabilisce che «*Le registrazioni sono conservate in archivi non modificabili o le cui modifiche sono puntualmente registrate per un periodo commisurato al livello di criticità delle funzioni aziendali, dei processi di*

supporto e delle risorse informatiche, documentato negli inventari aziendali (6).»

Rispetto al testo attualmente in vigore nel Documento si rileva l'eliminazione di qualunque riferimento temporale in merito alla quantificazione del periodo minimo di conservazione delle cd. «tracce elettroniche», relative alle caratteristiche salienti delle transazioni. A tale riguardo si ritiene che, la determinazione di un periodo di *retention* «*commisurato al livello di criticità delle funzioni aziendali, dei processi di supporto e delle risorse informatiche, documentato negli inventari aziendali*», lascia un ampio margine di discrezionalità ad ogni operatore nel determinare tale periodo. Si segnala inoltre che, negli anni scorsi, gli operatori hanno sostenuto investimenti e sforzi organizzativi per rispettare il requisito minimo temporale di 24 mesi precedentemente introdotto. Quanto descritto, se da un lato potrebbe essere considerato come elemento di semplificazione per alcuni operatori, dall'altro può causare una variazione delle direttive organizzative finora adottate. Sarebbe, dunque, importante anche comprendere le motivazioni per le quali si vorrebbe eliminare tale riferimento. A tal proposito, pur concordando con la possibilità di commisurare in maniera differente per ogni realtà il periodo di *retention* necessario, si propone comunque di quantificare un periodo minimo di conservazione delle tracce elettroniche, seppur di entità minore rispetto a quanto attualmente previsto.

3. *Titolo IV – Capitolo 4 – Sezione VI – Paragrafo 3 – Indicazioni Particolari*

Con riferimento alle Indicazioni Particolari riportate al paragrafo 3 della sezione VI del documento, si richiama quanto segue:

- *«L'intermediario pone particolare cautela nella valutazione di iniziative di esternalizzazione a fornitori di servizi in cloud computing (servizi cloud), ossia un modello che consente l'accesso in rete diffuso, conveniente, flessibile e su richiesta, a un gruppo condiviso di risorse informatiche configurabili (ad esempio reti, server, memorie, applicazioni e servizi), che possono essere fornite e messe a disposizione rapidamente con un minimo di attività gestionale o di interazione con il fornitore del servizio.»*

  Si segnala che, la definizione di cloud computing (o servizi cloud) riportata nel testo potrebbe essere fuorviante per alcuni operatori, in quanto, si discosta da altre definizioni internazionalmente più diffuse. Al solo fine di evitare differenti interpretazioni di quanto espresso e per una maggiore chiarezza, si suggerisce di valutare l'opportunità di riformulare tale concetto utilizzando le definizioni che determinano tali servizi, adottate da organizzazioni internazionalmente riconosciute (es. ENISA, Cloud Alliance, ecc.) e da standard internazionali, già considerati come riferimento da diversi operatori. Inoltre, si pone l'attenzione sul fatto che le caratteristiche dei modelli di cloud citati sono solo di tipo qualitative e quindi permettono un livello ampio di discrezionalità da parte degli operatori. A tal proposito, si propone di definire meglio anche le caratteristiche dei modelli di cloud che si intendono esplicitare.

4. *Titolo IV - Capitolo 4 – Sezione VII - Paragrafo 1 - Sicurezza dei servizi di pagamento*

In linea di massima si concorda con i Principi organizzativi relativi a specifiche attività o profili di rischio. Tuttavia, si ritiene **opportuno definire in maniera più dettagliata cosa si intende per** «**criticità delle risorse ICT»,** laddove si dice che: «*[… le banche: (a) integrano la classificazione delle risorse ICT* ***in termini di criticità*** *con quella delle funzioni delle attività e dei processi di supporto per la prestazione servizi di pagamento…]*», richiamandosi anche a quanto espresso nei punti da 3.1 a 3.3 degli Orientamenti EBA sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento.

5. *Titolo IV - Capitolo 5 – Sezione II - Paragrafo 3.5 – Le verifiche*

Con riferimento alle verifiche da effettuare sui piani per la continuità operativa, il Documento introduce per intero il primo comma, laddove si riporta: «*Gli intermediari sottopongono a verifica annuale i piani per la continuità operativa delle funzioni, dei servizi, dei sistemi, delle transazioni e delle interdipendenze riferite ai processi critici*», in recepimento dell'Orientamento 6.6 degli Orientamenti EBA sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento.

Nello specifico, si chiede conferma che quanto introdotto possa essere ricompreso nel concetto di verifiche complessive già presente in precedenza al terzo comma del medesimo paragrafo, in base al quale: «*Con frequenza almeno annuale sono svolte verifiche complessive, basate su scenari il più possibile realistici, del ripristino della operatività dei processi critici in condizioni di crisi, riscontrando la capacità dell'organizzazione di attuare nei tempi previsti le misure definite nel piano di continuità operativa*».

Inoltre, nel confronto tra il documento di «*Draft Guidelines on ICT and security risk management*» pubblicato da EBA il 13 dicembre 2018 e il Documento, emerge un disallineamento sulla definizione di Recovery Time Objective (RTO).

a) Quest'ultima bozza di Orientamenti dell'EBA definisce l'RTO come: «*the maximum time within which a system or process must be restored after an incident. »*
b) il Documento definisce il tempo di ripristino come: «*il periodo che intercorre fra il momento in cui l'operatore dichiara lo stato di crisi e l'istante in cui il processo è ripristinato a un livello di servizio predefinito. Esso è costituito dai tempi di: analisi degli eventi e decisione delle azioni da intraprendere, prima di effettuare gli interventi; ripartenza del processo, attraverso l'attuazione degli interventi tecnici e organizzativi e la successiva verifica sulla possibilità di rendere nuovamente disponibili i servizi senza danni e in condizioni di sicurezza.»*

Poiché gli operatori hanno implementato un processo di continuità operativa coerente con la definizione presente nella Circolare 285e riproposta in questo Documento sarebbe opportuno chiarire come si intenderà allineare le due definizioni in previsione del futuro recepimento dei citati ulteriori Orientamenti EBA.

6. Titolo IV – Capitoli 4 e 5

Con riferimento generale alla segnalazione dei gravi incidenti, si evidenzia la necessità di un allineamento del Documento, oltre agli Orientamenti **EBA/GL/2017/10**, anche rispetto al nuovo **framework** emesso il 7 settembre 2018 dall'**Eurosistema** su «*Major incident reporting framework for payment schemes and retail payment systems*» - che prevede l'obbligo di segnalazione di incidenti gravi a carico dei soggetti sotto la supervisione dell'Eurosistema in qualità di «operatori che partecipano ai sistemi di pagamento al dettaglio», «partecipanti/gestori di schemi di pagamento». Infatti, a quest'ultimo documento si è adeguato quanto previsto nel documento dell'European Payment Council (**EPC 190-18**) già in vigore da gennaio 2019, che fissa le regole per i partecipanti agli schemi SEPA relativi alla valutazione degli incidenti e relative segnalazioni, ivi inclusi aspetti procedurali e altri aspetti pratici.

Nell'ottica della massima armonizzazione a livello nazionale e comunitario, **sarebbe** da un lato **auspicabile conciliare i vari documenti** (Framework BCE/Eurosistema, Orientamenti EBA e Circolare 285), principalmente **in termini di contenuti** (tipologia e frequenza delle segnalazioni, criteri per la valutazione della gravità dell'incidente, etc.), **modalità di trasmissione della reportistica** (processo di segnalazione e autorità competenti) e **tempi di adeguamento** e, dall'altro, assicurare omogeneità di applicazione da parte delle autorità competenti, ivi inclusa la BCE/Eurosistema, per quanto riguarda l'applicazione agli schemi SEPA. Ciò gioverebbe sia alle autorità competenti sia a ciascun intermediario segnalante, che vedrebbe da un lato ridurre i propri oneri gestionali e dall'altro garantire la maggior prontezza di intervento richiesta. Infatti, stante il quadro normativo di riferimento, il medesimo intermediario è chiamato ad effettuare più segnalazioni, seguendo indicazioni che, ancorché sostanzialmente allineate, presentano tuttora delle differenze, in parte anche richiamate dall'EPC, che aggiungono maggiore complessità al verificarsi di situazioni che sono di per sé già critiche.

A ciò va aggiunto che, nell'interesse comune di evitare confusione ed inefficienze che potrebbero derivare dall'avere quadri di segnalazione divergenti, si ritiene opportuno prevedere un congruo periodo di tempo per consentire agli intermediari di adeguarsi alle nuove disposizioni del Documento (si segnala, ad esempio, che il testo in consultazione prevede l'invio entro il 30 aprile alla Banca d'Italia/BCE di una relazione sull'*assessment* dei rischi operativi e di sicurezza relativi ai sistemi di pagamento - cfr. Parte Prima, Titolo IV, Capitolo 4, Sezione VII).

Parte II: recepimento delle Raccomandazioni EBA/REC/2017/03

In linea generale si concorda con le Raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud (EBA/REC/2017/03) del 28 Marzo 2018.

Tuttavia, sarebbe opportuno considerare il fatto che tali Raccomandazioni sono state ulteriormente riviste nell'ambito della consultazione pubblica, aperta il 22 giugno 2018, sugli Orientamenti EBA in materia di "*outsourcing arrangements*" (consultazione EBA/CP/2018/11), a valle della quale si è in attesa della pubblicazione della versione definitiva degli Orientamenti.

Pertanto, considerato che gli Orientamenti EBA posti in consultazione non solo abrogheranno le Raccomandazioni, ma prevederanno disposizioni che si sovrappongono ad esse, con anche l'apporto di possibili modifiche, si chiede di non

procedere al recepimento delle norme contenute nel documento EBA/REC/2017/03 e di attendere invece l'imminente pubblicazione degli Orientamenti EBA/CP/2018/11, al fine di evitare agli intermediari di avviare l'adeguamento a disposizioni che a distanza di pochi mesi potrebbero essere superate o modificate.

Parte III: recepimento degli Orientamenti EBA/GL/2018/07

Si concorda con quanto indicato all'interno del Documento.