EBA/GL/2021/03

10 giugno 2021

Orientamenti aggiornati

in materia di segnalazione dei gravi incidenti ai sensi della PSD2

1. Conformità e obblighi di comunicazione

Status giuridico degli orientamenti

1. Il presente documento contiene orientamenti emanati in applicazione dell'articolo 16 del regolamento ABE ([1]). Conformemente all'articolo 16, paragrafo 3, del regolamento ABE, le autorità competenti e gli enti finanziari compiono ogni sforzo per conformarsi agli orientamenti.

2. Gli orientamenti definiscono la posizione dell'ABE in merito alle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione in un particolare settore. Le autorità competenti come definite all'articolo 4, paragrafo 2, del regolamento ABE cui si applicano gli orientamenti sono tenute a conformarsi ad essi integrandoli opportunamente nelle rispettive prassi (ad esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti sono diretti principalmente agli enti.

Obblighi di comunicazione

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento ABE, le autorità competenti devono comunicare all'ABE entro il (07.11.2021) se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna comunicazione da parte delle autorità competenti, queste sono ritenute dall'ABE non conformi. Le notifiche dovrebbero essere inviate trasmettendo il modulo disponibile sul sito web dell'ABE con il riferimento «EBA/GL/2021/03» da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti. Ogni eventuale variazione dello status di conformità deve essere altresì comunicata all'ABE.

4. Le notifiche sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3.

([1]) Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12).

2. Oggetto, ambito di applicazione e definizioni

Oggetto

5. I presenti orientamenti sono stati redatti in virtù del mandato conferito all'ABE ai sensi dell'articolo 96, paragrafo 3, della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (PSD2).

6. In particolare, i presenti orientamenti specificano i criteri per la classificazione dei gravi incidenti operativi o di sicurezza riscontrati dai prestatori di servizi di pagamento, nonché il formato e le procedure da seguire per comunicare tali incidenti all'autorità competente dello Stato membro di origine, ai sensi dell'articolo 96, paragrafo 1, della PSD2.

7. Inoltre, i presenti orientamenti indicano il modo in cui tali autorità competenti dovrebbero valutare la rilevanza dell'incidente e i dettagli delle segnalazioni di incidente che, ai sensi dell'articolo 96, paragrafo 2, della PSD2, sono tenute a condividere con altre autorità nazionali.

8. I presenti orientamenti riguardano anche la condivisione con l'ABE e la BCE dei dettagli pertinenti degli incidenti segnalati, al fine di promuovere un approccio comune e coerente.

Ambito di applicazione

9. I presenti orientamenti si applicano alla classificazione e alla segnalazione dei gravi incidenti operativi o di sicurezza, ai sensi dell'articolo 96 della PSD2.

10. I presenti orientamenti si applicano a tutti gli incidenti che rientrano nella definizione di «grave incidente operativo o di sicurezza», che comprende eventi sia esterni sia interni, dolosi o accidentali.

11. I presenti orientamenti si applicano anche se il grave incidente operativo o di sicurezza ha origine al di fuori dell'Unione (ad esempio, quando un incidente ha origine presso la società capogruppo o una succursale costituita al di fuori dell'Unione) e riguarda i servizi di pagamento forniti da un prestatore di servizi di pagamento con sede nell'Unione direttamente (un servizio connesso ai pagamenti è effettuato dalla società interessata costituita al di fuori dell'Unione) o indirettamente (la capacità del prestatore di servizi di pagamento di continuare a svolgere l'attività di pagamento viene compromessa in altro modo a causa dell'incidente).

12. I presenti orientamenti si applicano anche ai gravi incidenti che interessano funzioni esternalizzate dai prestatori di servizi di pagamento a terzi.

Destinatari

13. La prima parte degli orientamenti (sezione 4) è rivolta ai prestatori di servizi di pagamento come definiti all'articolo 4, paragrafo 11, della PSD2 e di cui all'articolo 4, paragrafo 1, del regolamento (UE) n. 1093/2010.

14. La seconda e la terza parte degli orientamenti (sezioni 5 e 6) si rivolgono alle autorità competenti come definite all'articolo 4, paragrafo 2, lettera i), del regolamento (UE) n. 1093/2010.

Definizioni

15. Se non diversamente specificato, i termini utilizzati e definiti nella PSD2 sono utilizzati con lo stesso significato nei presenti orientamenti. In aggiunta, ai fini dei presenti orientamenti, si applicano le seguenti definizioni.

Incidente operativo o di sicurezza	Singolo evento o serie di eventi collegati non pianificati dal prestatore di servizi di pagamento che ha o probabilmente avrà un impatto negativo su integrità, disponibilità, riservatezza, e/o autenticità dei servizi connessi ai pagamenti.
Integrità	Proprietà di salvaguardare l'esattezza e la completezza delle risorse (inclusi i dati).
Disponibilità	Proprietà dei servizi connessi ai pagamenti di essere pienamente accessibili e utilizzabili da parte degli utenti di servizi di pagamento, secondo livelli accettabili predefiniti dal prestatore di servizi di pagamento.
Riservatezza	Proprietà per cui le informazioni non sono rese disponibili o divulgate a persone, entità o procedure non autorizzate.
Autenticità	Proprietà di una fonte di essere quella che dichiara di essere.
Servizi connessi ai pagamenti	Attività commerciali intese ai sensi dell'articolo 4, paragrafo 3, della PSD2 e tutte le attività di supporto tecnico necessarie per la corretta prestazione dei servizi di pagamento.

3. Attuazione

Data di applicazione

16. I presenti orientamenti si applicano a partire dal 1° gennaio 2022.

Abrogazione

17. I seguenti orientamenti sono abrogati con effetto dal 1° gennaio 2022:

Orientamenti in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2) (EBA/GL/2017/10)

4. Orientamenti per i prestatori di servizi di pagamento in materia di segnalazione dei gravi incidenti operativi o di sicurezza all'autorità competente del rispettivo Stato membro di origine

Orientamento 1: classificazione come incidente grave

1.1. I prestatori di servizi di pagamento dovrebbero classificare come gravi gli incidenti operativi o di sicurezza che soddisfano

a. uno o più criteri al «livello di impatto maggiore», o

b. tre o più criteri al «livello di impatto minore»

come indicato all'orientamento 1.4 e seguendo la valutazione indicata nei presenti orientamenti.

1.2. I prestatori di servizi di pagamento dovrebbero basare la propria valutazione di un incidente operativo o di sicurezza sui seguenti criteri e sui rispettivi indicatori sottostanti.

i. Transazioni interessate

I prestatori di servizi di pagamento dovrebbero determinare il valore totale delle transazioni interessate e il numero dei pagamenti compromessi come percentuale del livello normale delle operazioni di pagamento effettuate mediante i servizi di pagamento interessati.

ii. Utenti di servizi di pagamento interessati

I prestatori di servizi di pagamento dovrebbero determinare il numero di utenti di servizi di pagamento interessati, sia in termini assoluti sia in percentuale del numero totale di utenti di servizi di pagamento.

iii. Violazione della sicurezza della rete o dei sistemi informativi

I prestatori di servizi di pagamento dovrebbero determinare se un'azione dolosa ha compromesso la sicurezza della rete o dei sistemi informativi relativi alla prestazione di servizi di pagamento.

iv. Periodo di indisponibilità del servizio

I prestatori di servizi di pagamento dovrebbero determinare il periodo di tempo durante il quale il servizio probabilmente non sarà disponibile all'utente di servizi di pagamento o durante il quale l'ordine di pagamento, inteso ai sensi dell'articolo 4, paragrafo 13, della PSD2, non potrà essere eseguito dal prestatore di servizi di pagamento.

v. Impatto economico

I prestatori di servizi di pagamento dovrebbero determinare in modo olistico i costi monetari associati all'incidente e tenere conto sia della cifra assoluta sia, se applicabile, dell'importanza relativa di tali costi in relazione alla dimensione (ossia al capitale di classe 1) del prestatore di servizi di pagamento.

vi. Alto livello di escalation interna

I prestatori di servizi di pagamento dovrebbero determinare se l'incidente è stato o sarà segnalato ai rispettivi dirigenti esecutivi.

vii. Altri prestatori di servizi di pagamento o infrastrutture connesse potenzialmente coinvolti

I prestatori di servizi di pagamento dovrebbero determinare le implicazioni sistemiche che l'incidente probabilmente avrà, ossia il suo potenziale di estendersi oltre il prestatore di servizi di pagamento inizialmente interessato ad altri prestatori di servizi di pagamento, infrastrutture dei mercati finanziari e/o a schemi di pagamento.

viii. Impatto sulla reputazione

I prestatori di servizi di pagamento dovrebbero determinare in che modo l'incidente possa minare la fiducia degli utenti nei confronti del prestatore di servizi di pagamento stesso e, più in generale, nei confronti dei servizi coinvolti o del mercato nel suo complesso.

1.3. I prestatori di servizi di pagamento dovrebbero calcolare il valore degli indicatori in base alla seguente metodologia.

i. Transazioni interessate

Come regola generale, i prestatori di servizi di pagamento dovrebbero considerare come «transazioni interessate» tutte le transazioni nazionali e transfrontaliere che sono state o probabilmente saranno interessate, direttamente o indirettamente, dall'incidente e, in particolare, quelle transazioni che potrebbero non essere iniziate o elaborate, quelle per le quali il contenuto del messaggio di pagamento è stato alterato e quelle ordinate in modo fraudolento (a prescindere dal fatto che i fondi siano stati recuperati o meno) o la cui corretta esecuzione è impedita o ostacolata in altro modo dall'incidente.

Per gli incidenti operativi che incidono sulla capacità di iniziare e/o elaborare transazioni, i prestatori di servizi di pagamento dovrebbero segnalare solo gli incidenti che hanno una durata superiore a un'ora. La durata dell'incidente dovrebbe essere misurata dal momento in cui l'incidente si verifica al momento in cui le normali attività/operazioni sono state ripristinate al livello di servizio prestato prima dell'incidente.

Inoltre, i prestatori di servizi di pagamento dovrebbero intendere come livello normale di operazioni di pagamento la media annuale giornaliera delle operazioni di pagamento nazionali e transfrontaliere effettuate con gli stessi servizi di pagamento interessati dall'incidente, prendendo l'anno precedente come periodo di riferimento per i calcoli. Nel caso in cui i prestatori di servizi di pagamento non ritengano che tale dato sia rappresentativo (ad esempio, a causa della stagionalità), essi dovrebbero utilizzare un'altra metrica, più

rappresentativa, e comunicare all'autorità competente la motivazione alla base di tale approccio compilando il campo corrispondente del modello (cfr. allegato).

ii. Utenti di servizi di pagamento interessati

I prestatori di servizi di pagamento dovrebbero considerare come «utenti di servizi di pagamento interessati» tutti i clienti (nazionali o esteri, consumatori o imprese) che hanno un contratto con il prestatore di servizi di pagamento interessato che garantisce loro l'accesso al servizio di pagamento interessato e che hanno subito o probabilmente subiranno le conseguenze dell'incidente. I prestatori di servizi di pagamento dovrebbero ricorrere a stime basate sull'attività precedente al fine di determinare il numero di utenti di servizi di pagamento che potrebbero aver utilizzato il servizio di pagamento nel corso dell'incidente.

Nel caso di gruppi, ogni prestatore di servizi di pagamento dovrebbe considerare solo i propri utenti di servizi di pagamento. Nel caso di un prestatore di servizi di pagamento che offre servizi operativi ad altri, tale prestatore di servizi di pagamento dovrebbe considerare solo i propri utenti di servizi di pagamento (se esistenti) e i prestatori di servizi di pagamento che ricevono tali servizi operativi dovrebbero valutare l'incidente in relazione ai propri utenti di servizi di pagamento.

Per gli incidenti operativi che incidono sulla capacità di iniziare e/o elaborare transazioni, i prestatori di servizi di pagamento dovrebbero segnalare solo gli incidenti che interessano gli utenti di servizi di pagamento e che hanno una durata superiore a un'ora. La durata dell'incidente dovrebbe essere misurata dal momento in cui l'incidente si verifica al momento in cui le normali attività/operazioni sono state ripristinate al livello di servizio prestato prima dell'incidente.

Inoltre, i prestatori di servizi di pagamento dovrebbero calcolare il numero totale degli utenti di servizi di pagamento considerando il totale degli utenti di servizi di pagamento nazionali e transfrontalieri contrattualmente vincolati al momento dell'incidente (o, in alternativa, il numero più recente disponibile) e aventi accesso al servizio di pagamento interessato, a prescindere dalla loro dimensione o dal fatto che siano considerati utenti attivi o passivi di servizi di pagamento.

iii. Violazione della sicurezza della rete o dei sistemi informativi

I prestatori di servizi di pagamento dovrebbero determinare se un'azione dolosa ha 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.

iv. Periodo di indisponibilità del servizio

I prestatori di servizi di pagamento dovrebbero considerare il periodo di tempo in cui qualsiasi attività, processo o canale che abbia un collegamento con la prestazione di servizi di pagamento è o sarà probabilmente interrotto, impedendo di conseguenza i) l'avvio e/o l'esecuzione di un servizio di pagamento e/o ii) l'accesso a un conto di pagamento. I prestatori di servizi di pagamento dovrebbero calcolare il periodo di indisponibilità del servizio dal momento del suo inizio e dovrebbero considerare sia gli intervalli di tempo in cui

sono operativi, come richiesto per l'esecuzione dei servizi di pagamento, sia gli orari di chiusura e i periodi di manutenzione, se del caso e se applicabile. Se i prestatori di servizi di pagamento non sono in grado di determinare il momento di inizio del periodo di indisponibilità del servizio, essi dovrebbero eccezionalmente calcolare tale periodo a partire dal momento in cui l'indisponibilità è stata rilevata.

v. *Impatto economico*

I prestatori di servizi di pagamento dovrebbero considerare sia i costi che possono essere collegati direttamente all'incidente sia quelli che sono indirettamente associati ad esso. Tra le altre cose, i prestatori di servizi di pagamento dovrebbero tener conto dei fondi o dei beni espropriati, dei costi di sostituzione dell'hardware o del software, di altri costi di indagine o di riconfigurazione, delle penali dovute alla mancata osservanza di obblighi contrattuali, delle sanzioni, delle passività esterne e dei mancati guadagni. Per quanto riguarda i costi indiretti, i prestatori di servizi di pagamento dovrebbero considerare solo quelli già noti o molto probabili.

vi. *Alto livello di escalation interna*

I prestatori di servizi di pagamento dovrebbero considerare se, in conseguenza dell'impatto dell'incidente sui servizi connessi ai pagamenti, l'organo di gestione quale definito negli orientamenti dell'ABE sulla gestione dei rischi ICT e di sicurezza è stato o sarà probabilmente informato dell'accaduto, in linea con l'orientamento 60, lettera d), di detti orientamenti, in via straordinaria rispetto alla procedura di informazione periodica e in modo continuativo per tutta la durata dell'incidente. Inoltre, i prestatori di servizi di pagamento dovrebbero considerare se, a seguito dell'impatto dell'incidente sui servizi connessi ai pagamenti, è stata o sarà probabilmente attivata la modalità di gestione delle crisi.

vii. *Altri prestatori di servizi di pagamento o infrastrutture connesse potenzialmente coinvolti*

I prestatori di servizi di pagamento dovrebbero valutare l'impatto dell'incidente sui mercati finanziari, intesi come le infrastrutture dei mercati finanziari e/o gli schemi di pagamento che li supportano e altri prestatori di servizi di pagamento. In particolare, i prestatori di servizi di pagamento dovrebbero valutare se l'incidente si è ripetuto o probabilmente si ripeterà presso altri prestatori di servizi di pagamento, se ha influenzato o probabilmente influenzerà il buon funzionamento delle infrastrutture dei mercati finanziari e se ha compromesso o probabilmente comprometterà il regolare funzionamento del sistema finanziario nel suo complesso. I prestatori di servizi di pagamento dovrebbero tener conto di vari elementi, ad esempio se il componente/software interessato è proprietario o genericamente disponibile, se la rete compromessa è interna o esterna e se il prestatore di servizi di pagamento ha smesso o probabilmente smetterà di adempiere i propri obblighi nelle infrastrutture dei mercati finanziari di cui è membro.

viii. *Impatto sulla reputazione*

I prestatori di servizi di pagamento dovrebbero considerare il livello di visibilità che, per quanto di loro conoscenza, l'incidente ha ricevuto o probabilmente riceverà sul mercato. In particolare, i prestatori di servizi di pagamento dovrebbero considerare la probabilità che

l'incidente causi danni alla società quale valido indicatore del suo potenziale di incidere sulla loro reputazione. I prestatori di servizi di pagamento dovrebbero considerare se i) gli utenti di servizi di pagamento e/o altri prestatori di servizi di pagamento si sono lamentati dell'impatto negativo dell'incidente, ii) l'incidente ha influito su un processo visibile collegato a servizi di pagamento e pertanto è probabile che riceva o ha già ricevuto copertura mediatica (non solo tramite i media tradizionali, come i quotidiani, ma anche blog, social network, ecc.), iii) sono stati o saranno probabilmente disattesi obblighi contrattuali, con la conseguente pubblicazione di azioni legali contro il prestatore di servizi di pagamento, iv) non si sono adempiuti obblighi regolamentari, con la conseguente imposizione di misure di vigilanza o sanzioni che sono state o saranno probabilmente rese pubbliche, e v) un tipo analogo di incidente si è verificato in passato.

1.4. I prestatori di servizi di pagamento dovrebbero valutare un incidente determinando, per ogni singolo criterio, se le soglie pertinenti di cui alla tabella 1 sono o saranno probabilmente raggiunte prima che l'incidente sia risolto.

Tabella 1: soglie

Criteri	Livello di impatto minore	Livello di impatto maggiore
Transazioni interessate	> 10 % del livello normale delle transazioni del prestatore di servizi di pagamento (in termini di numero di transazioni) **e** durata dell'incidente > 1 ora* **o** > 500 000 EUR **e** durata dell'incidente > 1 ora*	> 25 % del livello normale delle transazioni del prestatore di servizi di pagamento (in termini di numero di transazioni) **o** > 15 000 000 EUR
Utenti di servizi di pagamento interessati	> 5 000 **e** durata dell'incidente > 1 ora* **o** > 10 % degli utenti di servizi di pagamento del prestatore di servizi di pagamento **e** durata dell'incidente > 1 ora*	> 50 000 **o** > 25 % degli utenti di servizi di pagamento del prestatore di servizi di pagamento
Periodo di indisponibilità del servizio	> 2 ore	Non applicabile
Violazione della sicurezza della rete o dei sistemi informativi	Sì	Non applicabile
Impatto economico	Non applicabile	> Max (0,1 % del capitale di classe 1**, 200 000 EUR)

		o > 5 000 000 EUR
Alto livello di escalation interna	Sì	Sì, ed è probabile che si attivi la modalità di gestione delle crisi (o equivalente)
Altri prestatori di servizi di pagamento o infrastrutture connesse potenzialmente coinvolti	Sì	Non applicabile
Impatto sulla reputazione	Sì	Non applicabile

* La soglia relativa alla durata dell'incidente per un periodo superiore a un'ora si applica solo agli incidenti operativi che incidono sulla capacità del prestatore di servizi di pagamento di iniziare e/o elaborare transazioni.

** Capitale di classe 1 come definito all'articolo 25 del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012.

1.5. Qualora non dispongano di dati effettivi, i prestatori di servizi di pagamento dovrebbero ricorrere a stime per avvalorare il loro giudizio in merito al fatto che una data soglia è o sarà probabilmente raggiunta prima che l'incidente sia risolto (ad esempio, ciò potrebbe accadere durante la fase di analisi iniziale).

1.6. I prestatori di servizi di pagamento dovrebbero effettuare questa valutazione su base continuativa per tutta la durata dell'incidente, in modo da identificare ogni possibile cambiamento di stato, sia verso l'alto (da non grave a grave) sia verso il basso (da grave a non grave). Un'eventuale riclassificazione dell'incidente da grave a non grave dovrebbe essere comunicata all'autorità competente in linea con i requisiti dell'orientamento 2.21 e senza indebito ritardo.

Orientamento 2: procedura di segnalazione

2.1. I prestatori di servizi di pagamento dovrebbero raccogliere tutte le informazioni pertinenti, produrre un rapporto sull'incidente compilando il modello di cui all'allegato e trasmetterlo all'autorità competente dello Stato membro d'origine. I prestatori di servizi di pagamento dovrebbero compilare tutti i campi del modello seguendo le istruzioni fornite nell'allegato.

2.2. I prestatori di servizi di pagamento dovrebbero usare lo stesso modello per la trasmissione del rapporto iniziale, intermedio e finale relativi allo stesso incidente. I prestatori di servizi di pagamento dovrebbero pertanto compilare un unico modello in maniera incrementale e aggiornare, ove applicabile, le informazioni fornite nei rapporti precedenti.

2.3. I prestatori di servizi di pagamento dovrebbero inoltre presentare all'autorità competente dello Stato membro d'origine, se applicabile, una copia delle informazioni che sono state (o che saranno) fornite ai propri utenti, come previsto dall'articolo 96, paragrafo 1, comma 2, della PSD2, non appena disponibili.

2.4. I prestatori di servizi di pagamento dovrebbero, su richiesta dell'autorità competente dello Stato membro d'origine, fornire qualsiasi documento supplementare che integri le informazioni trasmesse con il modello standardizzato. I prestatori di servizi di pagamento dovrebbero rispondere a tutte le richieste dell'autorità competente dello Stato membro di origine di fornire ulteriori informazioni o chiarimenti riguardanti la documentazione già presentata.

2.5. Tutte le informazioni supplementari contenute nei documenti forniti dai prestatori di servizi di pagamento all'autorità competente, su iniziativa del prestatore di servizi di pagamento o su richiesta dell'autorità competente in linea con l'orientamento 2.4, dovrebbero essere indicate dal prestatore di servizi di pagamento nel modello di cui all'orientamento 2.1.

2.6. I prestatori di servizi di pagamento dovrebbero, in ogni momento, preservare la riservatezza e l'integrità delle informazioni scambiate e mantenere un'opportuna autenticazione nei confronti dell'autorità competente del loro Stato membro d'origine.

Rapporto iniziale

2.7. I prestatori di servizi di pagamento dovrebbero trasmettere un rapporto iniziale all'autorità competente dello Stato membro d'origine dopo che un incidente operativo o di sicurezza è stato classificato come grave. Le autorità competenti dovrebbero confermare senza indugio la ricezione del rapporto iniziale e assegnare un codice di riferimento univoco che identifichi l'incidente in modo inequivocabile. I prestatori di servizi di pagamento dovrebbero indicare questo codice di riferimento quando trasmettono un aggiornamento del rapporto iniziale o del rapporto intermedio e finale relativi allo stesso incidente, a meno che il rapporto intermedio e finale non siano presentati insieme al rapporto iniziale.

2.8. I prestatori di servizi di pagamento dovrebbero inviare il rapporto iniziale all'autorità competente entro quattro ore dal momento in cui l'incidente operativo o di sicurezza è stato classificato come grave. Se è noto che i canali di segnalazione dell'autorità competente non sono disponibili o operativi in quel momento, i prestatori di servizi di pagamento dovrebbero inviare il rapporto iniziale non appena i canali lo diventino nuovamente.

2.9. I prestatori di servizi di pagamento dovrebbero classificare l'incidente conformemente agli orientamenti 1.1 e 1.4 in modo tempestivo dopo che l'incidente è stato rilevato, ma non oltre 24 ore dopo la rilevazione dell'incidente, e senza indebito ritardo dopo che le informazioni necessarie per la classificazione dell'incidente diventano disponibili al prestatore di servizi di pagamento. Se è necessario più tempo per classificare l'incidente, i prestatori di servizi di pagamento dovrebbero spiegarne i motivi nel rapporto iniziale trasmesso all'autorità competente.

2.10. I prestatori di servizi di pagamento dovrebbero trasmettere un rapporto iniziale all'autorità competente dello Stato membro d'origine anche laddove un incidente classificato in precedenza come non grave sia riclassificato come grave. In questo caso particolare, i

prestatori di servizi di pagamento dovrebbero inviare il rapporto iniziale all'autorità competente immediatamente dopo la rilevazione del cambiamento di stato o, se è noto che i canali di segnalazione dell'autorità competente non sono disponibili o operativi in quel momento, non appena essi lo diventino nuovamente.

2.11. I prestatori di servizi di pagamento dovrebbero fornire nei loro rapporti iniziali le informazioni basilari (sezione A del modello), indicando alcune caratteristiche fondamentali dell'incidente e le sue conseguenze previste sulla base delle informazioni disponibili subito dopo che è stato classificato come grave. I prestatori di servizi di pagamento dovrebbero ricorrere a stime quando non sono disponibili i dati effettivi.

Rapporto intermedio

2.12. I prestatori di servizi di pagamento dovrebbero trasmettere il rapporto intermedio quando le regolari operazioni sono state ripristinate e l'attività è tornata alla normalità, informando l'autorità competente di questa circostanza. I prestatori di servizi di pagamento dovrebbero considerare ristabilita la normalità quando le attività/operazioni sono state ripristinate allo stesso livello di servizio/alle stesse condizioni definiti dal prestatore di servizi di pagamento o disposti esternamente da un accordo sul livello dei servizi (tempi di elaborazione, capacità, requisiti di sicurezza, ecc.) e le misure di emergenza non sono più in vigore. Il rapporto intermedio dovrebbe contenere una descrizione più dettagliata dell'incidente e delle sue conseguenze (sezione B del modello).

2.13. Se le normali attività non sono state ancora ripristinate, i prestatori di servizi di pagamento dovrebbero trasmettere un rapporto intermedio all'autorità competente entro tre giorni lavorativi dalla trasmissione del rapporto iniziale.

2.14. I prestatori di servizi di pagamento dovrebbero aggiornare le informazioni già inserite nelle sezioni A e B del modello quando vengano a conoscenza di cambiamenti significativi rispetto al rapporto precedente (ad esempio, se la gravità dell'incidente aumenta o diminuisce, se sono state identificate nuove cause o intraprese azioni per risolvere il problema). Ciò comprende il caso in cui l'incidente non è stato risolto entro tre giorni lavorativi, il che richiederebbe ai prestatori di servizi di pagamento di trasmettere un ulteriore rapporto intermedio. In ogni caso, i prestatori di servizi di pagamento dovrebbero trasmettere un rapporto intermedio supplementare se l'autorità competente dello Stato membro d'origine ne fa richiesta.

2.15. Come nel caso dei rapporti iniziali, qualora non siano disponibili dati effettivi, i prestatori di servizi di pagamento dovrebbero ricorrere a stime.

2.16. Se l'attività dovesse ritornare alla normalità prima che siano trascorse quattro ore dalla classificazione dell'incidente come grave, i prestatori di servizi di pagamento dovrebbero adoperarsi per trasmettere simultaneamente sia il rapporto iniziale sia il rapporto intermedio (compilando le sezioni A e B del modello) entro la scadenza delle quattro ore.

Rapporto finale

2.17. I prestatori di servizi di pagamento dovrebbero trasmettere un rapporto finale una volta effettuata l'analisi delle cause all'origine dell'incidente (indipendentemente dal fatto che siano state già attuate misure di mitigazione o che sia stata individuata definitivamente la causa all'origine dell'incidente) e quando sono disponibili dati effettivi da sostituire alle eventuali stime effettuate.

2.18. I prestatori di servizi di pagamento dovrebbero trasmettere il rapporto finale all'autorità competente entro un termine massimo di 20 giorni lavorativi dal momento in cui si considera che le attività siano tornate alla normalità. I prestatori di servizi di pagamento che necessitano di una proroga di tale termine (ad esempio, qualora non siano ancora disponibili dati effettivi sull'impatto o le cause all'origine dell'incidente non siano state ancora individuate) dovrebbero contattare l'autorità competente prima della scadenza del suddetto termine e fornire una giustificazione adeguata del ritardo e una nuova data stimata per il rapporto finale.

2.19. Laddove i prestatori di servizi di pagamento siano in grado di fornire tutte le informazioni richieste dal rapporto finale (sezione C del modello) entro quattro ore dal momento in cui l'incidente è stato classificato come grave, essi dovrebbero adoperarsi per fornire congiuntamente le informazioni relative al rapporto iniziale, intermedio e finale.

2.20. I prestatori di servizi di pagamento dovrebbero includere nel loro rapporto finale informazioni complete, ovvero i) dati effettivi relativi all'impatto anziché stime (nonché eventuali altri aggiornamenti necessari nelle sezioni A e B del modello) e ii) la sezione C del modello, che comprende la causa all'origine dell'incidente, se già nota, e una sintesi delle misure che sono state adottate o che si prevede di adottare per eliminare il problema ed evitare che si ripeta in futuro.

2.21. I prestatori di servizi di pagamento dovrebbero inviare inoltre un rapporto finale quando, in esito all'analisi dell'incidente svolta nel continuo, ritengano che un incidente già segnalato non soddisfi più i criteri per essere considerato grave e non si prevede che li soddisferà prima che l'incidente sia risolto. In tale eventualità, i prestatori di servizi di pagamento dovrebbero inviare il rapporto finale non appena questa circostanza viene rilevata e, in ogni caso, entro la scadenza per la trasmissione del rapporto successivo. In questa particolare situazione, invece di compilare la sezione C del modello, i prestatori di servizi di pagamento dovrebbero selezionare la casella «incidente riclassificato come non grave» e fornire una spiegazione dei motivi che giustificano questa riclassificazione.

Orientamento 3: segnalazione delegata e consolidata

3.1. Laddove consentito dall'autorità competente, i prestatori di servizi di pagamento che intendono delegare gli obblighi di segnalazione ai sensi della PSD2 a un terzo dovrebbero

informare l'autorità competente dello Stato membro d'origine e assicurare che siano soddisfatte le condizioni specificate di seguito.

a. Il contratto formale o, ove applicabile, le disposizioni esistenti interne a un gruppo che disciplinano la segnalazione delegata tra il prestatore di servizi di pagamento e il terzo definiscono inequivocabilmente l'assegnazione delle responsabilità di tutte le parti. In particolare, il suddetto contratto stabilisce chiaramente che, a prescindere dall'eventuale delega degli obblighi di segnalazione, il prestatore di servizi di pagamento interessato rimane pienamente responsabile dell'adempimento degli obblighi di cui all'articolo 96 della PSD2 e del contenuto delle informazioni fornite alle autorità competenti dello Stato membro d'origine.

b. La delega è conforme ai requisiti per l'esternalizzazione di importanti funzioni operative di cui:

   i. all'articolo 19, paragrafo 6, della PSD2 in relazione agli istituti di pagamento e agli istituti di moneta elettronica, applicabile mutatis mutandis in conformità dell'articolo 3 della direttiva 2009/110/CE; o

   ii. agli orientamenti dell'ABE in materia di esternalizzazione (EBA/GL/2019/02) in relazione a tutti i prestatori di servizi di pagamento.

c. La comunicazione all'autorità competente dello Stato membro di origine è effettuata in anticipo e, in ogni caso, ove applicabile, rispettando le scadenze e le procedure stabilite dall'autorità competente.

d. La riservatezza dei dati sensibili e la qualità, la coerenza, l'integrità e l'affidabilità delle informazioni da fornire all'autorità competente sono opportunamente garantite.

3.2. I prestatori di servizi di pagamento che intendono consentire a un terzo designato di adempiere gli obblighi di segnalazione in modo consolidato (ossia trasmettendo un unico rapporto che fa riferimento a diversi prestatori di servizi di pagamento interessati dallo stesso grave incidente operativo o di sicurezza) dovrebbero informarne l'autorità competente dello Stato membro d'origine, includere le informazioni di contatto di cui alla sezione «PSP interessati» del modello e assicurare che siano soddisfatte le condizioni specificate di seguito:

a. includere questa disposizione nel contratto che disciplina la segnalazione delegata;

b. rendere la segnalazione consolidata possibile unicamente laddove l'incidente sia stato causato da una problematica relativa ai servizi forniti dal terzo;

c. limitare la segnalazione consolidata a prestatori di servizi di pagamento stabiliti nello stesso Stato membro;

d. fornire un elenco di tutti i prestatori di servizi di pagamento interessati dall'incidente;

e. assicurare che il terzo valuti la rilevanza dell'incidente per ciascun prestatore di servizi di pagamento interessato e includa nel rapporto consolidato solo i prestatori di servizi di pagamento per i quali l'incidente è classificato come grave. Inoltre, assicurare che, in caso di dubbio, un prestatore di servizi di pagamento sia incluso nel rapporto consolidato fintanto che non sussista evidenza del fatto che non dovrebbe esservi incluso;

f. assicurare che, laddove in alcuni campi del modello non sia possibile inserire una risposta comune (ad esempio, sezione B2, B4 o C3), il terzo i) li compili singolarmente per ciascun prestatore di servizi di pagamento interessato, precisando inoltre l'identità di ogni prestatore di servizi di pagamento a cui le informazioni si riferiscono; oppure ii) utilizzi i valori cumulativi osservati o stimati per i prestatori di servizi di pagamento;

g. assicurare che il terzo tenga il prestatore di servizi di pagamento costantemente informato comunicando tutte le informazioni pertinenti in merito all'incidente e tutte le interazioni che il terzo avesse con l'autorità competente nonché il loro contenuto, ma solo nei limiti consentiti per evitare qualsiasi violazione della riservatezza delle informazioni relative ad altri prestatori di servizi di pagamento.

3.3. I prestatori di servizi di pagamento non dovrebbero delegare i propri obblighi di segnalazione prima di avere informato l'autorità competente dello Stato membro d'origine o dopo aver ricevuto notifica che l'accordo di esternalizzazione non soddisfa i requisiti di cui all'orientamento 3.1, lettera b).

3.4. I prestatori di servizi di pagamento che intendono ritirare la delega dei propri obblighi di segnalazione dovrebbero comunicare tale decisione all'autorità competente dello Stato membro d'origine, conformemente alle scadenze e alle procedure stabilite da quest'ultima. I prestatori di servizi di pagamento dovrebbero altresì informare l'autorità competente dello Stato membro di origine in merito a qualsiasi sviluppo importante che interessi il terzo designato e influenzi la sua capacità di adempiere gli obblighi di segnalazione.

3.5. I prestatori di servizi di pagamento dovrebbero adempiere materialmente i propri obblighi di segnalazione senza alcun ricorso ad assistenza esterna laddove il terzo designato non sia in grado di informare l'autorità competente dello Stato membro d'origine in merito a un grave incidente operativo o di sicurezza ai sensi dell'articolo 96 della PSD2 e dei presenti orientamenti. I prestatori di servizi di pagamento dovrebbero inoltre assicurare che un incidente non sia segnalato due volte (una volta dal prestatore di servizi di pagamento stesso e una seconda volta dal terzo).

3.6. I prestatori di servizi di pagamento dovrebbero assicurare che, nella situazione in cui un incidente è causato da un'interruzione dei servizi forniti da un prestatore di servizi tecnici (o un'infrastruttura) che interessa più prestatori di servizi di pagamento, la segnalazione delegata si riferisca ai dati individuali del prestatore di servizi di pagamento (tranne nel caso di segnalazione consolidata).

Orientamento 4: politica operativa e di sicurezza

4.1. I prestatori di servizi di pagamento dovrebbero assicurare che la propria politica generale di gestione delle operazioni e della sicurezza definisca chiaramente tutte le responsabilità relative alla segnalazione di incidenti di cui alla PSD2 e le procedure attuate per soddisfare i requisiti definiti nei presenti orientamenti.

5. Orientamenti rivolti alle autorità competenti in merito ai criteri per valutare la rilevanza dell'incidente e i dettagli dei rapporti sugli incidenti da condividere con altre autorità nazionali

Orientamento 5: valutazione della rilevanza dell'incidente

5.1. Le autorità competenti dello Stato membro di origine dovrebbero valutare la rilevanza di un grave incidente operativo o di sicurezza per altre autorità nazionali, sulla base del proprio parere di esperte della materia e utilizzando i seguenti criteri come indicatori primari dell'importanza di detto incidente:

a. le cause dell'incidente rientrano nell'ambito di competenza regolamentare dell'altra autorità nazionale (ossia il suo campo di competenza);
b. le conseguenze dell'incidente hanno un impatto sugli obiettivi di un'altra autorità nazionale (ad esempio, la tutela della stabilità finanziaria);
c. l'incidente interessa o potrebbe interessare utenti di servizi di pagamento su larga scala;
d. l'incidente ha ricevuto, o è probabile che riceva, un'ampia copertura mediatica.

5.2. Le autorità competenti dello Stato membro d'origine dovrebbero effettuare questa valutazione in modo continuativo per tutta la durata dell'incidente, per individuare eventuali cambiamenti che potrebbero rendere rilevante un incidente non considerato tale in precedenza.

Orientamento 6: informazioni da condividere

6.1. Fatti salvi eventuali altri requisiti legali per la condivisione delle informazioni relative agli incidenti con altre autorità nazionali, le autorità competenti dovrebbero fornire informazioni sui gravi incidenti operativi o di sicurezza alle autorità nazionali rilevanti identificate ai sensi dell'orientamento 5.1 quanto meno al momento della ricezione del rapporto iniziale (o, in alternativa, del rapporto che ha indotto la condivisione delle informazioni) e quando ricevono la notifica di ritorno alla normalità delle operazioni (ossia il rapporto intermedio).

6.2. Le autorità competenti dovrebbero trasmettere alle autorità nazionali rilevanti le informazioni necessarie per delineare un quadro chiaro di quanto accaduto e delle potenziali conseguenze. A tal fine, esse dovrebbero fornire almeno le informazioni trasmesse dal

prestatore di servizi di pagamento nei seguenti campi del modello (nel rapporto iniziale o intermedio):

- data e ora della classificazione dell'incidente come grave;
- data e ora di rilevazione dell'incidente;
- data e ora di inizio dell'incidente;
- data e ora in cui l'incidente è stato risolto o in cui si prevede di risolverlo;
- breve descrizione dell'incidente (comprese le parti non sensibili della descrizione dettagliata);
- breve descrizione delle misure adottate o previste per il ripristino dopo l'incidente;
- descrizione di come l'incidente potrebbe interessare altri prestatori di servizi di pagamento e/o infrastrutture;
- descrizione (se del caso) della copertura mediatica;
- causa dell'incidente.

6.3. Le autorità competenti dovrebbero procedere a un'adeguata anonimizzazione, secondo necessità, ed escludere tutte le informazioni che potrebbero essere soggette a restrizioni di riservatezza o di proprietà intellettuale prima di condividere informazioni relative agli incidenti con le autorità nazionali rilevanti. Tuttavia, le autorità competenti dovrebbero fornire alle autorità nazionali rilevanti il nome e l'indirizzo del prestatore di servizi di pagamento segnalante laddove dette autorità nazionali possano garantire che le informazioni saranno trattate in modo riservato.

6.4. Le autorità competenti dovrebbero, in ogni momento, preservare la riservatezza e l'integrità delle informazioni conservate e scambiate e mantenere un'opportuna autenticazione nei confronti delle autorità nazionali rilevanti. In particolare, le autorità competenti dovrebbero trattare tutte le informazioni ricevute in virtù dei presenti orientamenti in conformità degli obblighi di segreto d'ufficio stabiliti nella PSD2, fatte salve la legislazione dell'Unione e le norme nazionali applicabili.

6. Orientamenti rivolti alle autorità competenti sui criteri per valutare i dettagli rilevanti dei rapporti sugli incidenti da condividere con l'ABE e la BCE e sul formato e le procedure per la loro comunicazione

Orientamento 7: informazioni da condividere

7.1. Le autorità competenti dovrebbero sempre fornire all'ABE e alla BCE tutti i rapporti ricevuti da (o per conto di) prestatori di servizi di pagamento interessati da un grave incidente operativo o di sicurezza utilizzando un file standardizzato disponibile sul sito web dell'ABE.

Orientamento 8: comunicazione

8.1. Le autorità competenti dovrebbero, in ogni momento, preservare la riservatezza e l'integrità delle informazioni conservate e scambiate e mantenere un'opportuna autenticazione nei confronti dell'ABE e della BCE. In particolare, le autorità competenti dovrebbero trattare tutte le informazioni ricevute in virtù dei presenti orientamenti in conformità degli obblighi di segreto d'ufficio stabiliti nella PSD2, fatte salve la legislazione dell'Unione e le norme nazionali applicabili.

8.2. Per evitare ritardi nella trasmissione di informazioni sugli incidenti all'ABE e alla BCE e contribuire a ridurre al minimo i rischi di problematiche operative, le autorità competenti dovrebbero avvalersi di mezzi appropriati di comunicazione.

Allegato – Modello di segnalazione per i prestatori di servizi di pagamento

Rapporto iniziale

Rapporto iniziale	entro quattro ore dalla classificazione dell'incidente come grave	Annulla le selezioni
Data del rapporto *(GG/MM/AAAA)*		Ora *(HH:MM)*
Codice di riferimento dell'incidente		

A – Rapporto iniziale				
A 1 – INFORMAZIONI GENERALI				
Tipo di rapporto				
Tipo di rapporto				
Prestatore di servizi di pagamento (PSP) interessato				
Nome PSP				
Numero di identificazione nazionale del PSP				
Capogruppo, se applicabile				
Paese/paesi interessato/i dall'incidente	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ LI ☐ GR ☐ HR ☐ HU ☐ IE ☐ IS ☐ IT ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK			
Referente principale da contattare		E-mail		Telefono
Referente secondario da contattare		E-mail		Telefono
Entità segnalante (compilare questa sezione se l'entità segnalante non è il PSP interessato in caso di segnalazione delegata)				
Nome dell'entità segnalante				
Numero di identificazione nazionale				
Referente principale da contattare		E-mail		Telefono
Referente secondario da contattare		E-mail		Telefono
A 2 – RILEVAZIONE E CLASSIFICAZIONE DELL'INCIDENTE				
Data e ora di rilevazione dell'incidente *(GG/MM/AAAA HH:MM)*				
Data e ora di classificazione dell'incidente *(GG/MM/AAAA HH:MM)*				
Incidente rilevato da		Se «Altro», specificare:		
Tipo di incidente				
Criteri che fanno scattare la segnalazione di un grave incidente	☐ Transazioni interessate ☐ Utenti di servizi di pagamento interessati ☐ Periodo di indisponibilità ☐ Violazione della sicurezza della rete o dei ☐ Impatto economico ☐ Alto livello di escalation interna ☐ Altri PSP o infrastrutture rilevanti potenzialmente ☐ Impatto sulla interessati			
Breve descrizione generale dell'incidente				
Impatto in altri Stati membri dell'UE, se applicabile				
Segnalazione ad altre autorità		Se «Sì», specificare:		
Motivi del ritardo nella presentazione del rapporto iniziale				

Rapporto intermedio

Segnalazione di un grave incidente			
Rapporto intermedio	entro tre giorni lavorativi dalla trasmissione del rapporto iniziale		Annullale
Data del rapporto *(GG/MM/AAAA)*		Ora *(HH:MM)*	
Codice di riferimento dell'incidente			

B – Rapporto intermedio			
B 1 – INFORMAZIONI GENERALI			
Descrizione più dettagliata dell'incidente:			
Qual è il problema specifico?			
Come è iniziato l'incidente?			
Come si è evoluto?			
Quali sono le conseguenze (in particolare per gli utenti di servizi di pagamento)?			
L'incidente è stato comunicato agli utenti di servizi di pagamento?		Se «Sì», specificare:	
L'incidente è collegato a uno o più incidenti precedenti?		Se «Sì», specificare:	
L'incidente ha interessato o coinvolto altri prestatori di servizi o terzi?		Se «Sì», specificare:	
La modalità di gestione delle crisi (interna e/o esterna) è stata attivata?		Se «Sì», specificare:	
Data e ora di inizio dell'incidente (se già identificato) *(GG/MM/AAAA HH:MM)*			
Data e ora in cui l'incidente è stato risolto o in cui si prevede di risolverlo *(GG/MM/AAAA HH:MM)*			
Aree funzionali interessate	☐ Autenticazione/autorizzazione ☐ Regolamento diretto ☐ Comunicazione ☐ Regolamento indiretto ☐ Compensazione ☐ Altro	Se «Altro», specificare:	
Modifiche apportate ai rapporti precedenti			
B 2 – CLASSIFICAZIONE DELL'INCIDENTE / INFORMAZIONI SULL'INCIDENTE			
Transazioni interessate [2]	Livello di impatto Numero di transazioni interessate In % del livello normale delle transazioni Valore delle transazioni interessate in EUR Durata dell'incidente (applicabile solo agli incidenti operativi) Osservazioni:		
Utenti di servizi di pagamento interessati [3]	Livello di impatto Numero di utenti di servizi di pagamento interessati In % degli utenti di servizi di pagamento		
Violazione della sicurezza della rete o dei sistemi informativi	Descrivere come la rete o i sistemi informativi sono stati interessati dall'incidente		
Periodo di indisponibilità del servizio	Periodo totale di indisponibilità del servizio:	Giorni: Ore: Minuti:	
Impatto economico	Livello di impatto Costi diretti in EUR Costi indiretti in EUR		
Alto livello di escalation interna	Descrivere il livello di escalation interna dell'incidente, indicando se è stata o sarà probabilmente attivata la modalità di gestione delle crisi (o equivalente) e, in tal caso, fornire una descrizione		
Altri PSP o infrastrutture rilevanti potenzialmente interessati	Descrivere come questo incidente potrebbe interessare altri PSP e/o infrastrutture		
Impatto sulla reputazione	Descrivere come l'incidente potrebbe influire sulla reputazione del PSP (ad esempio, copertura mediatica, pubblicazione di azioni legali o violazioni della legge ecc.)		
B 3 – DESCRIZIONE DELL'INCIDENTE			
Tipo di incidente			
Causa dell'incidente	☐ In fase di analisi ☐ Azione dolosa ☐ Malfunzionamento del ☐ Malfunzionamento del sistema ☐ Errori umani ☐ Eventi esterni ☐ Altro	Se «Altro», specificare:	
L'incidente vi ha interessati direttamente o indirettamente attraverso un prestatore di servizi?		Se «Indirettamente», fornire il nome del prestatore di servizi:	
B 4 – IMPATTO DELL'INCIDENTE			
Impatto generale	☐ Integrità ☐ Riservatezza ☐ Disponibilità ☐ Autenticità		
Canali commerciali interessati	☐ Succursali ☐ Telephone banking ☐ Punto vendita ☐ E-banking ☐ Mobile banking ☐ Altro ☐ Commercio elettronico ☐ Sportelli automatici per il		
	Se «Altro», specificare:		
Servizi di pagamento interessati	☐ Deposito di contanti su un conto di pagamento ☐ Bonifici ☐ Rimessa di denaro ☐ Prelievo di contanti da un conto di pagamento ☐ Addebiti diretti ☐ Servizi di ☐ Operazioni necessarie per gestire un conto di pagamento ☐ Pagamenti con carta ☐ Servizi di informazione sui conti ☐ Acquiring di strumenti di pagamento ☐ Emissione di strumenti di pagamento		
B 5 – MITIGAZIONE DELL'INCIDENTE			
Quali azioni/misure sono state adottate finora o sono previste per il ripristino a seguito dell'incidente?			
Sono stati attivati il piano di continuità operativa e/o il piano di ripristino in caso di disastro (DRP)?			
In caso affermativo, quando? *(GG/MM/AAAA HH:MM)*			
In caso affermativo, fornire una descrizione			

Rapporto finale

Segnalazione di un grave incidente

Selezionare il tipo di rapporto: | entro 20 giorni lavorativi dalla trasmissione del rapporto intermedio

Descrivere: (applicabile agli incidenti riclassificati come non gravi)

Annulla le selezioni del menu a discesa

Data del rapporto *(GG/MM/AAAA)* | Ora *(HH:MM)*

Codice di riferimento dell'incidente

C – Rapporto finale

Se non è stato inviato un rapporto intermedio, compilare anche la sezione B

C 1 – INFORMAZIONI GENERALI

Aggiornamento delle informazioni del rapporto iniziale e del/i rapporto/i intermedio/i	
Modifiche apportate ai rapporti precedenti	
Altre informazioni rilevanti	
Le misure di controllo originali sono state ripristinate?	
Se «No», specificare quali misure di controllo non sono state ripristinate e il periodo di tempo supplementare richiesto per il loro ripristino	

C 2 – ANALISI DELLE CAUSE ALL'ORIGINE DELL'INCIDENTE E FOLLOW-UP

Quale è stata la causa all'origine dell'incidente (se già nota)?

☐ Azione dolosa | ☐ Malfunzionamento | ☐ Malfunzionamento | ☐ Errore umano | ☐ Evento esterno | ☐ Altro

Specificare:

Azione dolosa	Malfunzionamento	Malfunzionamento	Errore umano	Evento esterno
Codice dannoso	Monitoraggio e controllo carenti	Malfunzionament	Non intenzionale	Inadempienza di un fornitore/prestatore di servizi tecnici
Raccolta di informazioni	Problemi di comunicazione	Malfunzionament	Inazione	Forza maggiore
Intrusioni	Operazioni improprie	Malfunzionament	Risorse insufficienti	Altro
Attacco distributed/denial of service (D/DoS)	Gestione inadeguata del cambiamento	Malfunzionamento di applicativi/software	Altro	
Azioni interne deliberate	Inadeguatezza della documentazione e delle	Danno fisico		
Danno fisico esterno deliberato	Problemi di ripristino	Altro		
Sicurezza del contenuto delle informazioni	Altro			
Azioni fraudolente				
Altro				

Se «Altro», specificare:

Altre informazioni rilevanti sulla causa all'origine dell'incidente	
Principali azioni/misure correttive adottate o pianificate per impedire che l'incidente si verifichi nuovamente in futuro, se già note	

C 3 – INFORMAZIONI AGGIUNTIVE

L'incidente è stato condiviso con altri PSP a scopo informativo?	Se «Sì», fornire dettagli:
È stata intrapresa un'azione legale nei confronti del PSP?	Se «Sì», fornire dettagli:
Valutazione dell'efficacia delle azioni intraprese	Fornire dettagli:

ISTRUZIONI PER LA COMPILAZIONE DEL MODELLO

I prestatori di servizi di pagamento (PSP) dovrebbero compilare la sezione appropriata del modello, a seconda della fase di segnalazione in cui si trovano: sezione A per il rapporto iniziale, sezione B per i rapporti intermedi e sezione C per il rapporto finale. I PSP dovrebbero usare lo stesso modello per la trasmissione del rapporto iniziale, intermedio e finale relativi allo stesso incidente. Se non diversamente specificato, tutti i campi sono obbligatori.

Titolo

Rapporto iniziale: primo rapporto che il PSP trasmette all'autorità competente dello Stato membro d'origine.

Rapporto intermedio: rapporto contenente una descrizione più dettagliata dell'incidente e delle sue conseguenze. È un aggiornamento del rapporto iniziale (e, ove applicabile, di un precedente rapporto intermedio) relativo allo stesso incidente.

Rapporto finale: ultimo rapporto che il PSP invia in merito all'incidente, poiché i) è già stata eseguita un'analisi delle cause all'origine dell'incidente e le stime possono essere sostituite con dati effettivi o ii) l'incidente non è più considerato grave e deve essere riclassificato.

Incidente riclassificato come non grave: l'incidente non soddisfa più i criteri per essere classificato come grave e non si prevede che li soddisfi prima che il problema venga risolto. I PSP dovrebbero spiegare i motivi di questa riclassificazione.

Data e ora del rapporto: data e ora esatte della trasmissione del rapporto all'autorità competente.

Codice di riferimento dell'incidente (applicabile ai rapporti intermedio e finale, nonché agli aggiornamenti del rapporto iniziale): il codice di riferimento rilasciato dall'autorità competente al momento del rapporto iniziale per identificare l'incidente in modo inequivocabile. Ogni autorità competente dovrebbe includere come prefisso il codice ISO a 2 cifre ([2]) del rispettivo Stato membro.

A - Rapporto iniziale

A 1 - Informazioni generali

Tipo di rapporto

Individuale: il rapporto si riferisce a un solo PSP.

Consolidato: il rapporto si riferisce a diversi PSP all'interno dello stesso Stato membro che sono interessati dallo stesso grave incidente operativo o di sicurezza e che si avvalgono dell'opzione di segnalazione consolidata. I campi sotto il titolo «PSP interessato» dovrebbero essere lasciati vuoti (ad eccezione del campo «Paese/paesi interessato/i dall'incidente») e dovrebbe essere fornito un elenco dei PSP inclusi nel rapporto compilando la tabella corrispondente (Rapporto consolidato – Elenco dei PSP).

PSP interessato: si riferisce al PSP coinvolto nell'incidente.

Nome PSP: nome completo del PSP soggetto alla procedura di segnalazione, come appare nell'apposito registro nazionale ufficiale dei PSP.

Numero di identificazione nazionale del PSP: il numero di identificazione nazionale univoco utilizzato dall'autorità competente dello Stato membro d'origine nel suo registro nazionale per identificare il PSP in modo inequivocabile.

Capogruppo: nel caso di gruppi di entità, come definiti all'articolo 4, paragrafo 40, della PSD2, indicare il nome dell'entità capogruppo.

Paese/paesi interessato/i dall'incidente: paese o paesi in cui si è verificato l'incidente (ad esempio, sono interessate diverse succursali di un PSP situate in vari Stati), indipendentemente

([2]) Cfr. i codici paese ISO 3166 alpha-2 consultabili all'indirizzo https://www.iso.org/iso-3166-country-codes.html

dalla gravità dell'incidente nell'altro o negli altri paesi. Può essere o meno lo stesso Stato membro di origine.

Referente principale da contattare: nome e cognome della persona responsabile della segnalazione dell'incidente oppure, nel caso in cui un prestatore di servizi terzo effettui la segnalazione per conto del PSP interessato, nome e cognome del responsabile della gestione degli incidenti o della funzione di gestione dei rischi o di una funzione con compiti simili del PSP interessato.

E-mail: indirizzo e-mail a cui inviare eventuali richieste di ulteriori chiarimenti, se necessario. Può essere un indirizzo e-mail personale o aziendale.

Telefono: numero di telefono tramite il quale richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

Referente secondario da contattare: nome e cognome di una seconda persona che potrebbe essere contattata dall'autorità competente per chiedere informazioni su un incidente quando il referente principale non è disponibile. Nel caso in cui un prestatore di servizi terzo effettui la segnalazione per conto del PSP interessato, nome e cognome di una seconda persona responsabile della gestione degli incidenti o della funzione di gestione dei rischi o di una funzione con compiti simili del PSP interessato.

E-mail: indirizzo e-mail del referente secondario a cui inviare eventuali richieste di ulteriori chiarimenti, se necessario. Può essere un indirizzo e-mail personale o aziendale.

Telefono: numero di telefono del referente secondario tramite il quale richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

Entità segnalante: questa sezione dovrebbe essere compilata nel caso in cui un terzo adempia gli obblighi di segnalazione per conto del PSP interessato, se applicabile.

Nome dell'entità segnalante: nome completo dell'entità che segnala l'incidente, come indicato nell'apposito registro nazionale ufficiale delle imprese.

Numero di identificazione nazionale: numero di identificazione nazionale univoco utilizzato nel paese in cui il terzo ha sede per identificare in modo inequivocabile l'entità che effettua la segnalazione dell'incidente. Se il terzo che effettua la segnalazione è un PSP, il numero di identificazione nazionale dovrebbe essere il numero di identificazione nazionale univoco del PSP utilizzato dall'autorità competente dello Stato membro d'origine nel suo registro nazionale.

Referente principale da contattare: nome e cognome della persona responsabile della segnalazione dell'incidente.

E-mail: indirizzo e-mail a cui inviare eventuali richieste di ulteriori chiarimenti, se necessario. Può essere un indirizzo e-mail personale o aziendale.

Telefono: numero di telefono tramite il quale richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

Referente secondario da contattare: nome e cognome di una seconda persona dell'entità che effettua la segnalazione dell'incidente che potrebbe essere contattata dall'autorità competente quando il referente principale non è disponibile.

E-mail: indirizzo e-mail del referente secondario a cui inviare eventuali richieste di ulteriori chiarimenti, se necessario. Può essere un indirizzo e-mail personale o aziendale.

Telefono: numero di telefono del referente secondario tramite il quale richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

A 2 - Rilevazione e classificazione dell'incidente

Data e ora di rilevazione dell'incidente: data e ora in cui l'incidente è stato rilevato per la prima volta.

Data e ora di classificazione dell'incidente: data e ora in cui l'incidente operativo o di sicurezza è stato classificato come grave.

Incidente rilevato da: indicare se l'incidente è stato rilevato da un utente di servizi di pagamento, dall'interno del PSP (ad esempio, la funzione di audit interno) o da un soggetto esterno (ad esempio, un

prestatore di servizi). Se nessuno dei casi precedenti è applicabile, fornire una spiegazione nel campo corrispondente.

Tipo di incidente: indicare se, per quanto noto e qualora le informazioni siano disponibili, si tratta di un incidente operativo o di sicurezza.

> **Operativo:** incidente derivante da processi, persone e sistemi inadeguati o malfunzionanti o eventi di forza maggiore che influenzano l'integrità, la disponibilità, la riservatezza e/o l'autenticità dei servizi connessi ai pagamenti.
>
> **Di sicurezza**: accesso, uso, divulgazione, interruzione, modifica o distruzione non autorizzata delle risorse del PSP che influenza l'integrità, la disponibilità, la riservatezza e/o l'autenticità dei servizi connessi ai pagamenti. Ciò può avvenire, tra l'altro, quando il PSP subisce una violazione della sicurezza della rete o dei sistemi informativi.

Criteri che fanno scattare la segnalazione di un grave incidente: indicare quali dei criteri hanno fatto scattare la segnalazione di un grave incidente. Sono ammesse scelte multiple tra i seguenti criteri: transazioni interessate, utenti di servizi di pagamento interessati, periodo di indisponibilità del servizio, violazione della sicurezza della rete o dei sistemi informativi, impatto economico, alto livello di escalation interna, altri PSP o infrastrutture rilevanti potenzialmente interessati e/o impatto sulla reputazione.

Breve descrizione generale dell'incidente: spiegare brevemente le problematiche più rilevanti dell'incidente, includendo le possibili cause, gli impatti immediati, ecc.

Impatto in altri Stati membri dell'UE, se applicabile: spiegare brevemente l'impatto che l'incidente ha avuto in un altro Stato membro dell'UE (ad esempio, sugli utenti di servizi di pagamento, sui PSP e/o sulle infrastrutture di pagamento). Se fattibile entro i termini di segnalazione applicabili, fornire una traduzione in inglese.

Segnalazione ad altre autorità: indicare se l'incidente è stato o sarà segnalato ad altre autorità nell'ambito di altri sistemi di segnalazione degli incidenti, se noto al momento della segnalazione. In caso affermativo, specificare le rispettive autorità.

Motivi del ritardo nella presentazione del rapporto iniziale: spiegare i motivi per cui la classificazione dell'incidente ha richiesto più di 24 ore.

B Rapporto intermedio

B 1 – Informazioni generali

Descrizione più dettagliata dell'incidente: descrivere le caratteristiche principali dell'incidente, fornendo quanto meno informazioni sul problema specifico e sul relativo contesto, una descrizione di come l'incidente ha avuto inizio e di come si è evoluto, e una panoramica delle conseguenze, in particolare per gli utenti di servizi di pagamento, ecc. Fornire inoltre informazioni sulla comunicazione intercorsa con gli utenti di servizi di pagamento, se applicabile.

È collegato a uno o più incidenti precedenti? Indicare se l'incidente è collegato a incidenti precedenti, laddove questa informazione sia disponibile. Se l'incidente è collegato a incidenti precedenti, si prega di specificare quali.

L'incidente ha interessato o coinvolto altri prestatori di servizi o terzi? Indicare se l'incidente ha interessato o coinvolto altri prestatori di servizi o terzi, laddove questa informazione sia disponibile. Se l'incidente ha interessato o coinvolto altri prestatori di servizi o terzi, redigere un elenco e fornire maggiori informazioni.

Il processo di gestione delle crisi (interna e/o esterna) è stato attivato? Indicare se è stato attivato il processo di gestione delle crisi (interna e/o esterna). In caso affermativo, fornire maggiori informazioni.

Data e ora di inizio dell'incidente: data e ora in cui l'incidente è iniziato, se noto.

Data e ora in cui l'incidente è stato risolto o in cui si prevede di risolverlo: indicare la data e l'ora in cui l'incidente è stato o sarà sotto controllo e l'attività è o sarà tornata alla normalità.

Aree funzionali interessate: indicare la fase o le fasi del processo di pagamento che sono state interessate dall'incidente, quali autenticazione/autorizzazione, comunicazione, compensazione, regolamento diretto, regolamento indiretto e altro.

Autenticazione/autorizzazione: procedure che consentono al PSP di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, compreso l'uso delle credenziali di sicurezza personalizzate dell'utente e il consenso dell'utente di servizi di pagamento (o di un terzo che agisce per conto dell'utente) al trasferimento di fondi.

Comunicazione: flusso di informazioni ai fini dell'identificazione, dell'autenticazione, della notifica e dell'informazione tra il PSP che gestisce il conto e i prestatori di servizi di ordine di pagamento, i prestatori di servizi di informazione sui conti, i pagatori, i beneficiari e altri PSP.

Compensazione: processo di trasmissione, riconciliazione e, in alcuni casi, conferma degli ordini di pagamento prima del regolamento, che potenzialmente include la compensazione degli ordini e la definizione delle posizioni finali per il regolamento.

Regolamento diretto: completamento di una transazione o di un'elaborazione allo scopo di adempiere gli obblighi dei partecipanti mediante il trasferimento di fondi, quando questa azione viene eseguita dal PSP interessato.

Regolamento indiretto: completamento di un'operazione o di un'elaborazione allo scopo di adempiere gli obblighi dei partecipanti mediante il trasferimento di fondi, quando questa azione viene eseguita da un altro PSP per conto del PSP interessato.

Altro: l'area funzionale interessata non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Modifiche apportate ai rapporti precedenti: indicare le modifiche apportate alle informazioni fornite nei rapporti precedenti relativi allo stesso incidente (ad esempio, il rapporto iniziale o, ove applicabile, un rapporto intermedio).

B 2 – Classificazione dell'incidente / informazioni sull'incidente

Transazioni interessate: i PSP dovrebbero indicare quali soglie sono state o saranno probabilmente raggiunte dall'incidente, se del caso, e i relativi dati: il numero di transazioni interessate, la percentuale di transazioni interessate in relazione al numero di operazioni di pagamento effettuate con gli stessi servizi di pagamento che sono stati interessati dall'incidente e al valore totale delle transazioni. Per queste variabili, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. Come regola generale, i PSP dovrebbero considerare come «transazioni interessate» tutte le transazioni nazionali e transfrontaliere che sono state o probabilmente saranno interessate, direttamente o indirettamente, dall'incidente e, in particolare, quelle transazioni che potrebbero non essere iniziate o elaborate, quelle per le quali il contenuto del messaggio di pagamento è stato alterato e quelle ordinate in modo fraudolento (a prescindere dal fatto che i fondi siano stati recuperati o meno). Inoltre, i PSP dovrebbero intendere come livello normale di operazioni di pagamento la media annuale giornaliera delle operazioni di pagamento nazionali e transfrontaliere effettuate con gli stessi servizi di pagamento interessati dall'incidente, prendendo l'anno precedente come periodo di riferimento per i calcoli. Se i PSP non ritengono che tale dato sia rappresentativo (ad esempio, a causa della stagionalità), essi dovrebbero utilizzare un'altra metrica, più rappresentativa, e comunicare all'autorità competente la motivazione alla base di tale approccio compilando il campo «Osservazioni». Nei casi in cui ad essere interessate dall'incidente siano operazioni di pagamento in valute diverse dall'euro, nel calcolare le soglie e segnalare il valore delle transazioni interessate i PSP dovrebbero convertire in euro l'importo di tali operazioni utilizzando il tasso di cambio giornaliero di riferimento della BCE relativo al giorno precedente la trasmissione del rapporto sull'incidente.

Utenti di servizi di pagamento interessati: i PSP dovrebbero indicare quali soglie sono state o saranno probabilmente raggiunte dall'incidente, se del caso, e i relativi dati: il numero totale di utenti di servizi di pagamento che sono stati interessati e la percentuale di utenti di servizi di pagamento interessati

rispetto al numero totale di utenti di servizi di pagamento. Per queste variabili, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. I PSP dovrebbero considerare come «utenti di servizi di pagamento interessati» tutti i clienti (nazionali o esteri, consumatori o imprese) che hanno un contratto con il PSP interessato che garantisce loro l'accesso al servizio di pagamento interessato e che hanno subito o probabilmente subiranno le conseguenze dell'incidente. I PSP dovrebbero ricorrere a stime basate sull'attività precedente al fine di determinare il numero di utenti di servizi di pagamento che potrebbero aver utilizzato il servizio di pagamento nel corso dell'incidente. Nel caso di gruppi, ogni PSP dovrebbe considerare solo i propri utenti di servizi di pagamento. Nel caso di un PSP che offre servizi operativi ad altri, tale PSP dovrebbe considerare solo i propri utenti di servizi di pagamento (se esistenti) e i PSP che ricevono tali servizi operativi dovrebbero valutare l'incidente in relazione ai propri utenti di servizi di pagamento. Inoltre, i PSP dovrebbero calcolare il numero totale degli utenti di servizi di pagamento considerando il totale degli utenti di servizi di pagamento nazionali e transfrontalieri contrattualmente vincolati al momento dell'incidente (o, in alternativa, il numero più recente disponibile) e aventi accesso al servizio di pagamento interessato, a prescindere dalla loro dimensione o dal fatto che siano considerati utenti attivi o passivi di servizi di pagamento.

Violazione della sicurezza della rete o dei sistemi informativi: i PSP dovrebbero determinare se un'azione dolosa ha 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.

Periodo di indisponibilità del servizio: i PSP dovrebbero indicare se la soglia è stata o sarà probabilmente raggiunta dall'incidente e il relativo dato: periodo totale di indisponibilità del servizio. Per questa variabile, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. I PSP dovrebbero considerare il periodo di tempo in cui qualsiasi attività, processo o canale che abbia un collegamento con la prestazione di servizi di pagamento è o sarà probabilmente interrotto, impedendo di conseguenza i) l'avvio e/o l'esecuzione di un servizio di pagamento e/o ii) l'accesso a un conto di pagamento. I PSP dovrebbero calcolare il periodo di indisponibilità del servizio dal momento del suo inizio e dovrebbero considerare sia gli intervalli di tempo in cui sono operativi, come richiesto per l'esecuzione dei servizi di pagamento, sia gli orari di chiusura e i periodi di manutenzione, se del caso e se applicabile. Se i prestatori di servizi di pagamento non sono in grado di determinare il momento di inizio del periodo di indisponibilità del servizio, essi dovrebbero eccezionalmente calcolare tale periodo a partire dal momento in cui l'indisponibilità è stata rilevata.

Impatto economico: i PSP dovrebbero indicare se la soglia è stata o sarà probabilmente raggiunta dall'incidente e i relativi dati: costi diretti e costi indiretti. Per queste variabili, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. I PSP dovrebbero considerare sia i costi che possono essere collegati direttamente all'incidente sia quelli che lo sono indirettamente. Tra le altre cose, i PSP dovrebbero tener conto dei fondi o dei beni espropriati, dei costi di sostituzione dell'hardware o del software, di altri costi di indagine o di riconfigurazione, delle penali dovute alla mancata osservanza di obblighi contrattuali, delle sanzioni, delle passività esterne e dei mancati guadagni. Per quanto riguarda i costi indiretti, i PSP dovrebbero considerare solo quelli già noti o molto probabili. Nei casi in cui i costi siano espressi in valute diverse dall'euro, nel calcolare la soglia e segnalare il valore dell'impatto economico i PSP dovrebbero convertire in euro l'importo di tali costi utilizzando il tasso di cambio giornaliero di riferimento della BCE relativo al giorno precedente la trasmissione del rapporto sull'incidente.

> **Costi diretti:** costi (euro) imputabili direttamente all'incidente, compresi i costi della risoluzione dell'incidente (ad esempio, fondi o beni espropriati, costi di sostituzione dell'hardware o del software, penali dovute alla mancata osservanza di obblighi contrattuali).
>
> **Costi indiretti**: costi (euro) imputabili indirettamente all'incidente (ad esempio, risarcimenti, possibili costi legali).

Alto livello di escalation interna: i PSP dovrebbero considerare se, in conseguenza dell'impatto dell'incidente sui servizi connessi ai pagamenti, l'organo di gestione quale definito negli orientamenti

dell'ABE sulla gestione dei rischi ICT e di sicurezza è stato o sarà probabilmente informato dell'accaduto, in linea con l'orientamento 60, lettera d), di detti orientamenti, in via straordinaria rispetto alla procedura di informazione periodica e in modo continuativo per tutta la durata dell'incidente. Inoltre, i prestatori di servizi di pagamento dovrebbero considerare se, a seguito dell'impatto dell'incidente sui servizi connessi ai pagamenti, è stata o sarà probabilmente attivata la modalità di gestione delle crisi.

Altri PSP o infrastrutture rilevanti potenzialmente interessati: i PSP dovrebbero valutare l'impatto dell'incidente sui mercati finanziari, intesi come le infrastrutture dei mercati finanziari e/o gli schemi di pagamento che li supportano e altri PSP. In particolare, i PSP dovrebbero valutare se l'incidente si è ripetuto o probabilmente si ripeterà presso altri PSP, se ha influenzato o probabilmente influenzerà il buon funzionamento delle infrastrutture dei mercati finanziari e se ha compromesso o probabilmente comprometterà il regolare funzionamento del sistema finanziario nel suo complesso. I PSP dovrebbero tener conto di vari elementi, ad esempio se il componente/software interessato è proprietario o genericamente disponibile, se la rete compromessa è interna o esterna e se il PSP ha smesso o probabilmente smetterà di adempiere i propri obblighi nelle infrastrutture dei mercati finanziari di cui è membro.

Impatto sulla reputazione: i PSP dovrebbero considerare il livello di visibilità che, per quanto di loro conoscenza, l'incidente ha ricevuto o probabilmente riceverà sul mercato. In particolare, i PSP dovrebbero considerare la probabilità che l'incidente causi danni alla società quale valido indicatore del suo potenziale di incidere sulla loro reputazione. I PSP dovrebbero considerare se i) gli utenti di servizi di pagamento e/o altri PSP si sono lamentati dell'impatto negativo dell'incidente, ii) l'incidente ha influito su un processo visibile collegato a servizi di pagamento e pertanto è probabile che riceva o ha già ricevuto copertura mediatica (non solo tramite i media tradizionali, come i quotidiani, ma anche blog, social network, ecc.; tuttavia, per copertura mediatica in questo contesto si intende non solo l'esistenza di alcuni commenti negativi da parte dei follower, bensì la presenza di un rapporto valido o di un numero significativo di commenti negativi/avvisi), iii) sono stati o saranno probabilmente disattesi obblighi contrattuali, con la conseguente pubblicazione di azioni legali contro il prestatore di servizi di pagamento, iv) non si sono adempiuti obblighi regolamentari, con la conseguente imposizione di misure di vigilanza o sanzioni che sono state o saranno probabilmente rese pubbliche, e v) un tipo analogo di incidente si è verificato in passato.

B 3 – Descrizione dell'incidente

Tipo di incidente: operativo o di sicurezza. Ulteriori spiegazioni sono fornite nel campo corrispondente del rapporto iniziale.

Causa dell'incidente: indicare la causa dell'incidente o, se questa non è ancora nota, quella più probabile. Sono ammesse scelte multiple.

In fase di analisi: selezionare questa casella se la causa è ancora sconosciuta.

Azione dolosa: azioni mirate intenzionalmente al PSP. Queste sono suddivise in codici malevoli, raccolta di informazioni, intrusioni, attacchi distributed/denial of service (D/DoS), azioni interne deliberate, danno fisico esterno deliberato, sicurezza del contenuto delle informazioni, azioni fraudolente e altro. Per maggiori informazioni, si rimanda alla sezione C2 di questo modello.

Malfunzionamento del processo: l'incidente è stato causato dall'inadeguata progettazione o esecuzione del processo di pagamento, dei controlli di processo e/o dei processi di supporto (ad esempio, processo per modifica/migrazione, test, configurazione, capacità, monitoraggio).

Malfunzionamento del sistema: la causa dell'incidente è associata a inadeguatezza di progettazione, esecuzione, componenti, specifiche, integrazione o complessità dei sistemi, delle reti, delle infrastrutture e delle banche dati che supportano l'attività di pagamento.

Errori umani: l'incidente è stato causato dall'errore involontario di una persona nell'ambito della procedura di pagamento (ad esempio, caricamento del file dei pagamenti errato nel sistema di

pagamento) o in qualche modo correlato (ad esempio, la corrente elettrica viene accidentalmente staccata e l'attività di pagamento viene messa in attesa).

Eventi esterni: la causa è associata a eventi che esulano generalmente dal controllo diretto dell'organizzazione (ad esempio, disastri naturali, inadempienza di un prestatore di servizi tecnici).

Altro: la causa dell'incidente non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

L'incidente vi ha interessati direttamente o indirettamente attraverso un prestatore di servizi? Indicare se l'incidente è stato direttamente mirato al PSP o se lo ha interessato indirettamente tramite un terzo, laddove questa informazione sia disponibile. In caso di impatto indiretto, fornire il nome del/i prestatore/i di servizi.

B 4 – Impatto dell'incidente

Impatto generale: indicare quali dimensioni sono state interessate dall'incidente operativo o di sicurezza. Sono ammesse scelte multiple.

Integrità: proprietà di salvaguardare l'esattezza e la completezza delle risorse (inclusi i dati).

Disponibilità: proprietà dei servizi connessi ai pagamenti di essere pienamente accessibili e utilizzabili da parte degli utenti di servizi di pagamento, secondo livelli accettabili predefiniti.

Riservatezza: proprietà per cui le informazioni non sono rese disponibili o divulgate a persone, entità o procedure non autorizzate.

Autenticità: proprietà di una fonte di essere quella che dichiara di essere.

Canali commerciali interessati: indicare il canale o i canali di interazione con gli utenti di servizi di pagamento che sono stati interessati dall'incidente. È possibile selezionare più caselle.

Succursali: sede di attività (diversa dalla sede centrale) facente capo a un PSP, che è sprovvista di personalità giuridica ed effettua direttamente alcune operazioni o l'insieme delle operazioni inerenti all'attività di un PSP. Tutte le sedi di attività costituite nello stesso Stato membro da un PSP avente la sede centrale in un altro Stato membro dovrebbero essere considerate come un'unica succursale.

E-banking: utilizzo di computer per effettuare transazioni finanziarie su internet.

Telephone banking: utilizzo di telefoni per effettuare transazioni finanziarie.

Mobile banking: utilizzo di un'applicazione bancaria specifica su smartphone o dispositivi simili per effettuare transazioni finanziarie.

Sportelli automatici per il prelievo di contante (ATM): dispositivi elettromeccanici che consentono agli utenti di servizi di pagamento di prelevare contanti dai propri conti e/o di accedere ad altri servizi.

Punto vendita: sede fisica del commerciante dalla quale viene avviata l'operazione di pagamento.

Commercio elettronico: operazione di pagamento avviata in un punto vendita virtuale (ad esempio, per i pagamenti avviati via internet utilizzando bonifici, carte di pagamento, trasferimenti tra conti di moneta elettronica).

Altro: il canale commerciale interessato non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Servizi di pagamento interessati: indicare i servizi di pagamento che non funzionano correttamente a seguito dell'incidente. È possibile selezionare più caselle.

Versamento di contante su un conto di pagamento: conferimento di denaro a un PSP allo scopo di accreditarlo su un conto di pagamento.

Prelievo di contante da un conto di pagamento: richiesta inoltrata a un PSP da un utente di servizi di pagamento allo scopo di prelevare contanti e addebitare l'importo corrispondente sul proprio conto di pagamento.

Operazioni necessarie per gestire un conto di pagamento: azioni che devono essere eseguite su un conto di pagamento per attivarlo, disattivarlo e/o mantenerlo (ad esempio, apertura e blocco).

Acquiring di strumenti di pagamento: servizio di pagamento fornito da un prestatore di servizi di pagamento che stipula un contratto con il beneficiario per l'accettazione e il trattamento delle operazioni di pagamento, che si traduce in un trasferimento di fondi al beneficiario.

Bonifici: servizio di pagamento per l'accredito sul conto di pagamento del beneficiario tramite un'operazione di pagamento o una serie di operazioni di pagamento dal conto di pagamento del pagatore eseguite dal PSP detentore del conto di pagamento del pagatore, sulla base di un'istruzione impartita dal pagatore.

Addebiti diretti: servizio di pagamento per l'addebito di un conto di pagamento del pagatore in cui un'operazione di pagamento è disposta dal beneficiario in base al consenso dato dal pagatore al beneficiario, al PSP del beneficiario o al PSP del pagatore stesso.

Pagamenti con carta: servizio di pagamento basato sull'infrastruttura e sulle regole commerciali di un circuito di carte di pagamento per effettuare un'operazione di pagamento con carte, dispositivi di telecomunicazione, dispositivi digitali o IT, o software, quando il risultato è una transazione tramite carta di debito o di credito. Tra le operazioni di pagamento basate su carta non rientrano le operazioni basate su altri tipi di servizi di pagamento.

Emissione di strumenti di pagamento: servizio di pagamento fornito da un PSP che stipula un contratto per fornire al pagatore uno strumento di pagamento per disporre e trattare le operazioni di pagamento del pagatore.

Rimessa di denaro: servizio di pagamento in cui i fondi sono consegnati da un pagatore, senza che siano stati aperti conti di pagamento intestati al pagatore o al beneficiario, unicamente allo scopo di trasferire una somma corrispondente a un beneficiario o a un altro PSP che agisce per conto del beneficiario, e/o in cui tali fondi sono riscossi per conto del beneficiario e resi disponibili a quest'ultimo.

Servizi di disposizione di ordini di pagamento: servizio che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro PSP.

Servizi di informazione sui conti: servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro PSP o presso più PSP.

B 5 – Mitigazione dell'incidente

Quali azioni/misure sono state adottate finora o sono previste per il ripristino in caso di incidente? Fornire informazioni dettagliate sulle azioni intraprese o pianificate per affrontare temporaneamente l'incidente.

Sono stati attivati il piano di continuità operativa e/o il piano di ripristino in caso di disastro (Disaster Recovery Plan)? Indicare se ciò è avvenuto e, in caso affermativo, fornire i dettagli principali di ciò che è accaduto (ossia specificare quando sono stati attivati e in cosa consistevano tali piani).

C – Rapporto finale

C 1 – Informazioni generali

Aggiornamento delle informazioni del rapporto iniziale e del/i rapporto/i intermedio/i (sintesi): fornire ulteriori informazioni sull'incidente, comprese le specifiche modifiche apportate alle informazioni fornite con il rapporto intermedio. Includere anche qualsiasi altra informazione rilevante.

Le misure di controllo originali sono state ripristinate? Indicare se il PSP ha dovuto annullare o attenuare l'intensità di alcune misure di controllo in qualsiasi momento nel corso dell'incidente. In caso

affermativo, indicare se tutte le misure di controllo sono state ripristinate e, in caso contrario, spiegare nel campo di testo libero quali misure di controllo non sono state ripristinate e il periodo di tempo supplementare richiesto per il loro ripristino.

C 2 – Analisi delle cause all'origine dell'incidente e follow-up

Quale è stata la causa all'origine dell'incidente, se già nota? Indicare qual è la causa all'origine dell'incidente o, se questa non è ancora nota, quella più probabile. Sono ammesse scelte multiple. (Si noti che la causa all'origine dell'incidente dovrebbe essere distinta dall'impatto dell'incidente.)

Azione dolosa: azioni interne o esterne mirate intenzionalmente al PSP. Sono disponibili le seguenti categorie:

Codice malevolo: ad esempio, virus, worm, trojan, spyware.

Raccolta di informazioni: ad esempio, scansione, sniffing, social engineering.

Intrusioni: ad esempio, compromissione di account privilegiati, compromissione di account non privilegiati, compromissione di applicazioni, bot.

Attacco distributed/denial of service (D/DoS): tentativo di rendere non disponibile un servizio online richiedendolo con traffico da più fonti.

Azioni interne deliberate: ad esempio, sabotaggio, furto.

Danno fisico esterno deliberato: ad esempio, sabotaggio, attacco fisico ai locali/centri dati.

Sicurezza del contenuto delle informazioni: accesso non autorizzato alle informazioni, modifica non autorizzata delle informazioni.

Azioni fraudolente: uso non autorizzato di risorse, copyright, masquerade, phishing.

Altro (specificare): la causa dell'incidente non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Malfunzionamento del processo: l'incidente è stato causato dall'inadeguata progettazione o esecuzione del processo di pagamento, dei controlli di processo e/o dei processi di supporto (ad esempio, processo per modifica/migrazione, test, configurazione, capacità, monitoraggio). Sono disponibili le seguenti categorie:

Monitoraggio e controllo carenti: ad esempio, in relazione a operazioni in corso, date di scadenza dei certificati, date di scadenza delle licenze, date di scadenza delle patch, valori massimi definiti dei contatori, livelli di riempimento dei database, gestione dei diritti degli utenti, principio del doppio controllo.

Problemi di comunicazione: ad esempio, tra i partecipanti al mercato o all'interno dell'organizzazione.

Operazioni improprie: ad esempio, nessuno scambio di certificati, cache piena.

Gestione inadeguata del cambiamento: ad esempio, errori di configurazione non identificati, attività di roll-out comprendenti aggiornamenti, problemi di manutenzione, errori imprevisti.

Inadeguatezza della documentazione e delle procedure interne: ad esempio, mancanza di trasparenza riguardo alle funzionalità, ai processi e al verificarsi di malfunzionamenti, assenza di documentazione.

Problemi di ripristino: ad esempio, gestione delle emergenze, ridondanza insufficiente.

Altro (specificare): la causa dell'incidente non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Malfunzionamento del sistema: la causa dell'incidente è associata a inadeguatezza di progettazione, esecuzione, componenti, specifiche, integrazione o complessità dei sistemi, delle reti, delle infrastrutture e dei database che supportano l'attività di pagamento. Sono disponibili le seguenti categorie:

Malfunzionamento dell'hardware: malfunzionamento delle apparecchiature tecnologiche fisiche che gestiscono i processi e/o archiviano i dati necessari ai PSP per

svolgere le attività relative ai pagamenti (ad esempio, malfunzionamento di hard drive, centri dati, altre infrastrutture).

Malfunzionamento della rete: malfunzionamento delle reti di telecomunicazione, pubbliche o private, che consentono lo scambio di dati e informazioni (ad esempio, tramite internet) durante il processo di pagamento.

Malfunzionamento dei database: malfunzionamento delle strutture in cui sono archiviate le informazioni personali e relative ai pagamenti necessarie per eseguire operazioni di pagamento.

Malfunzionamento di applicativi/software: malfunzionamento di programmi, sistemi operativi, ecc. che supportano la prestazione di servizi di pagamento da parte del PSP (ad esempio, guasti, funzioni sconosciute).

Danno fisico: ad esempio, danni involontari causati da condizioni inadeguate, lavori di costruzione.

Altro (specificare): la causa dell'incidente non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Errore umano: l'incidente è stato causato dall'errore involontario di una persona nell'ambito della procedura di pagamento (ad esempio, caricamento del file dei pagamenti errato nel sistema di pagamento) o in qualche modo correlato (ad esempio, la corrente elettrica viene accidentalmente staccata e l'attività di pagamento viene messa in attesa). Sono disponibili le seguenti categorie:

Non intenzionale: ad esempio, errori, omissioni, mancanza di esperienza e di conoscenza.

Inazione: ad esempio, a causa della mancanza di abilità, conoscenza, esperienza, consapevolezza.

Risorse insufficienti: ad esempio, mancanza di risorse umane, scarsa disponibilità di personale.

Altro (specificare): la causa dell'incidente non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Evento esterno: la causa è associata a eventi che esulano generalmente dal controllo dell'organizzazione. Sono disponibili le seguenti categorie:

Inadempienza di un fornitore/prestatore di servizi tecnici: ad esempio, blackout, interruzione di internet, problemi legali, problemi aziendali, dipendenze di servizio.

Forza maggiore: ad esempio, blackout, incendi, cause naturali come terremoti, inondazioni, precipitazioni intense, vento forte.

Altro (specificare): la causa dell'incidente non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Altro: la causa dell'incidente non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Altre informazioni rilevanti sulla causa all'origine dell'incidente: fornire eventuali ulteriori dettagli sulla causa all'origine dell'incidente, comprese le conclusioni preliminari tratte dalla relativa analisi.

Principali azioni/misure correttive adottate o pianificate per impedire che l'incidente si verifichi nuovamente in futuro, se già note: descrivere le principali azioni intraprese o pianificate per evitare che l'incidente si ripeta in futuro.

C 3 – Informazioni aggiuntive

L'incidente è stato condiviso con altri PSP a scopo informativo? Indicare quali PSP sono stati contattati, formalmente o informalmente, per essere informati in merito all'incidente; riportare i dettagli dei PSP informati, le informazioni che sono state condivise e le motivazioni alla base della condivisione di tali informazioni.

È stata intrapresa un'azione legale nei confronti del PSP? Indicare se, al momento della compilazione del rapporto finale, il PSP è soggetto a un'azione legale (ad esempio, se è stato citato in tribunale o ha perso la sua licenza) a seguito dell'incidente.
Valutazione dell'efficacia delle azioni intraprese: includere, se disponibile, un'autovalutazione dell'efficacia delle azioni intraprese durante dell'incidente, compresi eventuali insegnamenti appresi.