EBA/GL/2017/10

19/12/2017

Orientamenti

in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (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 (UE) n. 1093/2010[1]. Conformemente all'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti e gli enti finanziari compiono ogni sforzo per conformarsi agli orientamenti.

2. Gli orientamenti presentano 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. Ai sensi dell'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010, le autorità competenti sono tenute a conformarsi a detti orientamenti integrandoli opportunamente nelle rispettive prassi di vigilanza (per 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 (UE) n. 1093/2010, le autorità competenti devono comunicare all'ABE entro 19/02/2018 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 all'indirizzo compliance@eba.europa.eu con il riferimento "EBA/GL/2017/10" 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 comunicazioni 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 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 gravi 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 dall'articolo 96, paragrafo 1, della suddetta direttiva.

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, di detta direttiva, 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 d'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 direttiva (UE) 2015/2366.

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 colpita 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 qualche altro modo a causa dell'incidente).

Destinatari

12. La prima parte degli orientamenti (sezione 4) è rivolta ai prestatori di servizi di pagamento ai sensi dell'articolo 4, paragrafo 11, della direttiva (UE) 2015/2366 e di cui all'articolo 4, paragrafo 1, del regolamento (UE) n. 1093/2010.

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

Definizioni

14. Se non diversamente specificato, i termini utilizzati e definiti nella direttiva (UE) 2015/2366 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, autenticità e/o continuità dei servizi connessi ai pagamenti.
Integrità	Proprietà della salvaguardia dell'esattezza e completezza delle risorse (inclusi i dati).
Disponibilità	Proprietà dei servizi connessi ai pagamenti di essere accessibili e utilizzabili da parte degli utenti dei 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.
Continuità	Proprietà delle procedure, attività e risorse di un'organizzazione funzionali all'erogazione dei servizi connessi ai pagamenti di essere pienamente fruibili e operative a livelli di servizio accettabili e predefiniti.
Servizi connessi ai pagamenti	Attività commerciali definite nell'articolo 4, paragrafo 3, della PSD2 e tutte le attività di supporto tecnico necessarie per la corretta fornitura dei servizi di pagamento.

3. Attuazione

Data di applicazione

15. I presenti orientamenti si applicano a partire dal 13 gennaio 2018.

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 in quanto 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 al punto 1.4 degli orientamenti 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 transazioni di pagamento effettuate mediante i servizi di pagamento interessati.

ii. Utenti del servizio di pagamento interessati

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

iii. Periodo di indisponibilità del servizio

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

iv. 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 del prestatore di servizi di pagamento (ossia al capitale di tipo Tier 1 del prestatore di servizi di pagamento).

v. Alto livello di escalation interna

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

vi. 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 carte di pagamento.

vii. 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).

Inoltre, i prestatori di servizi di pagamento dovrebbero intendere come livello normale di transazioni di pagamento la media annuale giornaliera delle transazioni 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 prestatori di servizi di pagamento 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 corrispondente dello schema (cfr. allegato 1).

ii. Utenti del servizio di pagamento interessati

I prestatori di servizi di pagamento dovrebbero considerare come «utenti del servizio di pagamento interessati» tutti i clienti (nazionali o stranieri, 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 per determinare il numero di utenti del servizio 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 a terzi, tale prestatore di servizi di pagamento dovrebbe considerare solo i propri utenti dei servizi di pagamento (se ve ne sono) 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.

Inoltre, i prestatori di servizi di pagamento dovrebbero considerare quale numero totale di utenti di servizi di pagamento il numero aggregato 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 ritenuti utenti attivi o passivi.

iii. 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 inattività del servizio, essi dovrebbero eccezionalmente calcolare tale periodo a partire dal momento in cui l'indisponibilità è stata rilevata.

iv. 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 delle perdite di entrate. Per quanto riguarda i costi indiretti, i prestatori di servizi di pagamento dovrebbero considerare solo quelli già noti o molto probabili.

v. *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, il direttore della funzione informatica (CIO o posizione analoga) è stato o sarà probabilmente informato dell'accaduto in via straordinaria rispetto alle 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 crisi aziendale.

vi. *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, inteso come infrastrutture dei mercati finanziari e/o schemi di pagamento con carte 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 del mercato finanziario di cui è membro.

vii. *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 influenzare la loro reputazione. I prestatori di servizi di pagamento dovrebbero considerare se (i) l'incidente ha influito su un processo visibile e pertanto riceverà probabilmente o ha già ricevuto copertura mediatica (non solo tramite i media tradizionali, come i giornali, ma anche blog, social networks, ecc.), (ii) non si sono adempiuti o probabilmente non si adempiranno obblighi regolamentari, (iii) sono state o probabilmente saranno violate sanzioni o (iv) lo stesso tipo di incidente si è già 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** > 100 000 EUR	> 25 % del livello normale delle transazioni del prestatore di servizi di pagamento (in termini di numero di transazioni) **o** > 5 milioni di EUR
Utenti di servizi di pagamento interessati	> 5 000 **e** > 10 % degli utenti di servizi di pagamento del prestatore di servizi di pagamento	> 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
Impatto economico	Non applicabile	> Max (0,1 % capitale di tipo "Tier 1"(*), 200 000 EUR) **o** > 5 milioni di EUR
Alto livello di escalation interna	Sì	Sì e probabilmente si ricorrerà alla modalità di crisi aziendale (o equivalente)
Altri prestatori di servizi di pagamento o infrastrutture connesse potenzialmente coinvolti	Sì	Non applicabile
Impatto sulla reputazione	Sì	Non applicabile

(*) Capitale di tipo "Tier 1", come definito nell'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. I prestatori di servizi di pagamento dovrebbero ricorrere a stime laddove non dispongano di dati effettivi sulla base dei quali valutare se una determinata soglia è o sarà probabilmente raggiunta prima che l'incidente sia risolto (ad esempio, questo potrebbe avvenire durante la fase iniziale di indagine).

1.6. I prestatori di servizi di pagamento dovrebbero effettuare tale valutazione in modo continuo per l'intera durata dell'incidente, per individuare eventuali cambiamenti di stato, sia verso l'alto (da non grave a grave) sia verso il basso (da grave a non grave).

Orientamento 2: procedura di segnalazione

2.1. I prestatori di servizi di pagamento dovrebbero raccogliere tutte le informazioni pertinenti, produrre un rapporto sull'incidente utilizzando il modulo di cui all'allegato 1 e sottometterlo all'autorità competente dello Stato membro di origine. I prestatori di servizi di pagamento dovrebbero compilare il modulo seguendo le istruzioni fornite nell'allegato 1.

2.2. I prestatori di servizi di pagamento dovrebbero utilizzare lo stesso modulo per tenere informata l'autorità competente durante tutto lo svolgimento dell'incidente (ossia per la segnalazione iniziale, intermedia e finale, come descritto nei paragrafi da 2.7 a 2.21). I prestatori di servizi di pagamento dovrebbero compilare il modulo in modo incrementale, con la massima diligenza possibile, mano a mano che nuove informazioni divengono prontamente disponibili nel corso delle loro indagini interne.

2.3. I prestatori di servizi di pagamento dovrebbero inoltre presentare all'autorità competente dello Stato membro di origine, se applicabile, una copia delle comunicazioni che sono state effettuate (o saranno effettuate) 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 fornire all'autorità competente dello Stato membro di origine eventuali informazioni aggiuntive, se disponibili e considerate rilevanti per l'autorità competente, integrando il modulo standardizzato con documentazione integrativa, sotto forma di uno o più allegati.

2.5. 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.

2.6. I prestatori di servizi di pagamento dovrebbero, in ogni momento, mantenere la riservatezza e l'integrità delle informazioni scambiate con l'autorità competente del loro Stato membro di origine e dovrebbero altresì autenticarsi opportunamente nei confronti dell'autorità competente del loro Stato membro di origine.

Rapporto iniziale

2.7. I prestatori di servizi di pagamento dovrebbero sottomettere un rapporto iniziale all'autorità competente dello Stato membro di origine alla prima rilevazione di un grave incidente operativo o di sicurezza.

2.8. I prestatori di servizi di pagamento dovrebbero inviare il rapporto iniziale all'autorità competente entro 4 ore dalla prima rilevazione di un grave incidente operativo o di sicurezza, oppure, essendo a conoscenza che i canali di segnalazione dell'autorità competente non sono disponibili o operativi in quel momento, non appena essi lo diventino nuovamente.

2.9. I prestatori di servizi di pagamento dovrebbero inoltrare un rapporto iniziale all'autorità competente dello Stato membro di origine anche quando un incidente classificato in precedenza come non grave diventi grave. In questo caso particolare, i prestatori di servizi di pagamento dovrebbero inviare il rapporto iniziale all'autorità competente immediatamente dopo la rilevazione della modifica di stato o, essendo a conoscenza che i canali di segnalazione dell'autorità competente non sono disponibili o operativi in quel momento, non appena essi lo diventino nuovamente.

2.10. I prestatori di servizi di pagamento dovrebbero includere nei loro rapporti iniziali le informazioni basilari (ossia quelle di cui alla sezione A del modulo), indicando alcune caratteristiche fondamentali dell'incidente e le sue conseguenze previste sulla base delle informazioni disponibili subito dopo che è stato rilevato o riclassificato. I prestatori di servizi di pagamento dovrebbero ricorrere a stime quando non sono disponibili i dati effettivi. I prestatori di servizi di pagamento dovrebbero includere nel loro rapporto iniziale anche la data del successivo aggiornamento, che dovrebbe essere il più presto possibile e in nessun caso oltre i tre giorni lavorativi successivi.

Segnalazione intermedia

2.11. I prestatori di servizi di pagamento dovrebbero sottomettere rapporti intermedi ogniqualvolta ritengano che vi sia un aggiornamento dello stato dell'incidente rilevante e, come minimo, entro la data del successivo aggiornamento indicato nel rapporto precedente (rapporto iniziale o precedente rapporto intermedio).

2.12. I prestatori di servizi di pagamento dovrebbero sottomettere all'autorità competente un primo rapporto intermedio con una descrizione più dettagliata dell'incidente e delle sue conseguenze (sezione B del modulo). Inoltre, i prestatori di servizi di pagamento dovrebbero produrre ulteriori rapporti intermedi, almeno aggiornando le informazioni già inserite nelle sezioni A e B del modulo, quando vengano a conoscenza di nuove informazioni rilevanti o di cambiamenti significativi rispetto al rapporto precedente (ad esempio, se la gravità dell'incidente aumenta o diminuisce, nuove cause identificate o azioni intraprese per risolvere il problema). In ogni caso, i prestatori di servizi di pagamento dovrebbero presentare un rapporto intermedio su richiesta dell'autorità competente dello Stato membro di origine.

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

2.14. Inoltre, i prestatori di servizi di pagamento dovrebbero indicare in ogni rapporto la data dell'aggiornamento successivo che dovrebbe avvenire il più presto possibile e in nessun caso oltre i tre giorni lavorativi. Nell'impossibilità di rispettare la data prevista per il successivo aggiornamento, il prestatore di servizi di pagamento dovrebbe contattare l'autorità competente per spiegare i motivi del ritardo, proporre un nuovo termine di presentazione plausibile (non oltre i tre giorni lavorativi successivi) e inviare una nuovo rapporto intermedio, aggiornando esclusivamente le informazioni relative alla data stimata per l'aggiornamento successivo.

2.15. I prestatori di servizi di pagamento dovrebbero inviare l'ultimo rapporto intermedio quando le normali 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 (SLA), in termini di tempi di elaborazione, capacità, requisiti di sicurezza, ecc., e le misure di emergenza non sono più in vigore.

2.16. Se l'attività dovesse ritornare alla normalità prima che siano trascorse quattro ore dalla rilevazione dell'incidente, i prestatori di servizi di pagamento dovrebbero adoperarsi per presentare simultaneamente sia il rapporto iniziale sia l'ultimo rapporto intermedio (ossia compilando le sezioni A e B del modulo) entro le quattro ore di scadenza.

Rapporto finale

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

2.18. I prestatori di servizi di pagamento dovrebbero sottomettere il rapporto finale all'autorità competente entro un termine massimo di due settimane 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, se non sono ancora disponibili dati effettivi sull'impatto) dovrebbero contattare l'autorità competente prima della scadenza di suddetto termine e dovrebbero fornire una giustificazione adeguata per il 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 (ossia sezione C del modulo) entro quattro ore dalla rilevazione dell'incidente, essi dovrebbero adoperarsi per includere nel rapporto iniziale le informazioni relative a rapporto iniziale, ultimo rapporto intermedio e rapporto finale.

2.20. I prestatori di servizi di pagamento dovrebbero adoperarsi per includere nei loro rapporti finali informazioni complete, ovvero (i) dati effettivi relativi all'impatto anziché stime (nonché eventuali altri aggiornamenti necessari nelle sezioni A e B del modulo) e (ii) sezione C del modulo, che comprende la causa che ha originato l'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 data prevista per il rapporto successivo. In questa particolare situazione, invece di compilare la sezione C del modulo, i prestatori di servizi di pagamento dovrebbero selezionare la casella «incidente riclassificato come non grave» e spiegare le ragioni 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 una terza parte dovrebbero informare l'autorità competente dello Stato membro di origine e assicurare che siano soddisfatte le condizioni specificate di seguito.

a. Il contratto formale o, se applicabile, le disposizioni esistenti interne a un gruppo che disciplinano la segnalazione delegata tra il prestatore di servizi di pagamento e la terza parte definiscono inequivocabilmente l'assegnazione delle responsabilità di tutte le parti. In particolare, suddetti accordi stabiliscono chiaramente che, a prescindere dall'eventuale delega degli obblighi di segnalazione, il prestatore di servizi di pagamento interessato rimane pienamente responsabile dell'adempimento dei requisiti di cui all'articolo 96 della PSD2 e del contenuto delle informazioni fornite alle autorità competenti dello Stato membro di 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 (EMD) o

   ii. agli orientamenti del CEBS sull'esternalizzazione relativa agli enti creditizi.

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 una terza parte designata di adempiere gli obblighi di segnalazione in modo consolidato (ossia inoltrando un unico rapporto riferito a diversi prestatori di servizi di pagamento interessati dallo stesso grave incidente operativo o di sicurezza) dovrebbero informarne l'autorità competente dello Stato membro di origine, includere le informazioni di contatto di cui alla sezione «PSP interessati» del modulo 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 dalla terza parte.

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

d. Assicurare che la terza parte 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.

e. Assicurare che, laddove in alcuni campi del modulo non sia possibile inserire una risposta comune (ad esempio, sezione B 2, B 4 o C 3), la terza parte (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 si riferiscono le informazioni; oppure (ii) utilizzi intervalli di valori, nei campi dove ciò è consentito, indicando il valore più basso e quello più alto osservati o stimati per i diversi prestatori di servizi di pagamento.

f. I prestatori di servizi di pagamento dovrebbero assicurare che la terza parte li tenga costantemente informati comunicando tutte le informazioni rilevanti in merito all'incidente e tutte le interazioni che la terza parte avesse con l'autorità competente nonché il loro contenuto, nei limiti consentiti dall'esigenza di 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 di origine o dopo essere stati messi al corrente che l'accordo di esternalizzazione non soddisfa i requisiti di cui al punto 3.1, lettera b), dei presenti orientamenti.

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 di 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 la terza parte designata e influenzi la sua capacità di adempiere gli obblighi di segnalazione.

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

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 gli utenti dei servizi di pagamento su larga scala;
d. è probabile che l'incidente riceva o abbia ricevuto un'ampia copertura mediatica.

5.2. Le autorità competenti dello Stato membro di origine dovrebbero effettuare questa valutazione in modo continuo 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 identificate ai sensi dell'orientamento 5.1 (ossia «altre autorità nazionali rilevanti») 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 l'ultimo rapporto intermedio).

6.2. Le autorità competenti dovrebbero fornire ad altre 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 indicate dal

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

- 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 possa interessare altri PSP 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 riservatezza o restrizioni di proprietà intellettuale prima di condividere informazioni relative agli incidenti con altre autorità nazionali rilevanti. Tuttavia, le autorità competenti dovrebbero fornire alle altre 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 sempre preservare la riservatezza e l'integrità delle informazioni conservate e scambiate con altre autorità nazionali competenti e dovrebbero autenticarsi opportunamente nei confronti delle altre autorità nazionali competenti. 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 tutte i rapporti ricevuti da (o per conto di) prestatori di servizi di pagamento interessati da un grave incidente operativo o di sicurezza (ossia i rapporti iniziali, intermedi e finali).

Orientamento 8: comunicazione

8.1. Le autorità competenti dovrebbero sempre preservare la riservatezza e l'integrità delle informazioni conservate e scambiate con l'ABE e la BCE e dovrebbero inoltre autenticarsi opportunamente 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 1 – Modulo di segnalazione per i prestatori di servizi di pagamento

CLASSIFICATION: RESTRICTED

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date	DD/MM/YYYY	Time	HH:MM
Incident identification number, if applicable (for interim and final reports)			

A - Initial report

A 1 - GENERAL DETAILS

Type of report					
Type of report	☐ Individual	☐ Consolidated			
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected — ☐ Actual figure ☐ Estimation As a % of regular number of transactions — ☐ Actual figure ☐ Estimation Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure ☐ Estimation As a %-of total payment service users — ☐ Actual figure ☐ Estimation
Service downtime[4]	Total service downtime: DD:HH:MM — ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR — ☐ Actual figure ☐ Estimation Indirect costs in EUR — ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)

B 3 - INCIDENT DESCRIPTION

Type of Incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack → Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other — If Other, specify ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other — If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly — If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs

PSP Name	PSP Unique Identification Number	PSP Authorisation number

ISTRUZIONI PER LA COMPILAZIONE DEGLI SCHEMI

I prestatori di servizi di pagamento dovrebbero compilare la pertinente sezione del modulo, 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. Tutti i campi sono obbligatori, a meno che non diversamente specificato.

Titolo

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

Rapporto intermedio: aggiornamento di un rapporto precedente (iniziale o intermedio) relativo allo stesso incidente.

Ultimo rapporto intermedio: rapporto che informa l'autorità competente dello Stato membro di origine che le normali attività sono state ripristinate e che le operazioni sono tornate alla normalità, per cui non verranno presentati nuovi rapporti intermedi.

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.

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 le ragioni di questa riclassificazione.

Data e ora del rapporto: data e ora esatte di sottomissione del rapporto all'autorità competente.

Numero di identificazione dell'incidente, se applicabile (per i rapporti intermedi e finali): numero di riferimento rilasciato dall'autorità competente al momento della segnalazione iniziale per identificare in modo univoco l'incidente, se applicabile (ossia se tale riferimento è fornito dall'autorità competente).

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 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 del PSP, se pertinente: il numero di identificazione univoco utilizzato in ciascuno Stato membro per identificare il PSP, da comunicare se il campo «Numero di autorizzazione PSP» non è compilato.

Numero di autorizzazione del PSP: numero di autorizzazione dello Stato membro di origine.

Capogruppo: in caso di gruppi di entità, come definiti nell'articolo 4, paragrafo 40, 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 che abroga la direttiva 2007/64/CE, indicare il nome dell'entità capogruppo.

Paese di origine: Stato membro in cui è situata la sede legale del PSP o, laddove il PSP, ai sensi della propria legislazione nazionale, non disponga di una sede legale, lo Stato membro in cui è situata la sede centrale.

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). 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, se una terza parte effettua 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'e-mail personale o aziendale.

Telefono: numero di telefono cui 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. Se una terza parte effettua 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 cui richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

Entità segnalante: questa sezione dovrebbe essere compilata se un terza parte adempie gli obblighi di segnalazione per conto del PSP interessato.

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

Numero di identificazione, se pertinente: numero di identificazione univoco utilizzato nel paese in cui ha sede la terza parte per identificare l'entità che effettua la segnalazione dell'incidente, fornito dall'entità segnalante se il campo «Numero di autorizzazione» non è compilato.

Numero di autorizzazione, se applicabile: numero di autorizzazione della terza parte nel paese dove questo ha sede, se applicabile.

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'e-mail personale o aziendale.

Telefono: numero di telefono per 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 da contattare non è disponibile.

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

Telefono: numero di telefono della seconda persona di contatto per richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

A 2 – Rilevazione dell'incidente e classificazione iniziale

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

Incidente rilevato da: indicare se l'incidente è stato rilevato da un utente di servizi di pagamento, da un'altra funzione interna del PSP (ad esempio, la funzione di audit interno) o da una entità esterna (ad esempio, un prestatore di servizi esterno). Se nessuno dei casi precedenti fosse applicabile, fornire una spiegazione nel campo corrispondente.

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

Qual è il momento stimato del prossimo aggiornamento?: indicare data e ora stimate per la presentazione dell'aggiornamento successivo (rapporto intermedio o finale).

B – Rapporto intermedio

B 1 – Informazioni generali

Descrizione più dettagliata dell'incidente: descrivere le caratteristiche principali dell'incidente, trattando quantomeno i punti contenuti nel questionario (qual è il problema specifico che il PSP deve affrontare, come ha avuto inizio e come si è sviluppato, possibile collegamento con un incidente precedente, conseguenze, in particolare per gli utenti di servizi di pagamento, ecc.).

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

Status dell'incidente

Diagnosi: le caratteristiche dell'incidente sono appena state identificate.

Riparazione: gli elementi impattati sono in riconfigurazione.

Recupero: gli elementi impattati vengono ripristinati all'ultimo salvataggio recuperabile.

Ripristino: i servizi connessi ai pagamenti sono nuovamente forniti.

Data e ora in cui l'incidente è stato risolto o 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.

B 2 – Classificazione degli incidenti/Informazioni sull'incidente

Impatto generale: indicare quali dimensioni sono state interessate dall'incidente. È possibile contrassegnare più caselle.

Integrità: proprietà di salvaguardia dell'esattezza e della completezza delle risorse (inclusi i dati).

Disponibilità: proprietà dei servizi connessi ai pagamenti di essere accessibili e utilizzabili da parte degli utenti dei servizi di pagamento.

Riservatezza: proprietà per cui l'informazione non è resa disponibile o divulgata a persone, entità o procedure non autorizzate.

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

Continuità: Proprietà delle procedure, attività e risorse di un'organizzazione funzionali all'erogazione dei servizi connessi ai pagamenti di essere pienamente fruibili e operative a livelli di servizio accettabili e predefiniti.

Transazioni interessate: i PSP dovrebbero indicare quali soglie sono 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 transazioni 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. Le entità che effettuano la segnalazione per conto di più PSP (ossia la segnalazione consolidata) possono invece indicare intervalli di valori che rappresentano i valori più bassi e più elevati osservati o stimati all'interno del gruppo di PSP inclusi nel rapporto, separati da un trattino. Come regola generale, i prestatori di servizi di pagamento dovrebbero considerare come «transazioni interessate» tutte le transazioni nazionali e transfrontaliere che sono state o saranno probabilmente interessate, direttamente o indirettamente, dall'incidente e, in particolare, quelle transazioni che potrebbero non essere avviate o gestite, quelle per le quali è stato modificato il contenuto del messaggio di pagamento 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 transazioni di pagamento la media annuale giornaliera delle transazioni di pagamento nazionali e transfrontaliere effettuate con gli stessi servizi di pagamento interessati dall'incidente, considerando l'anno precedente come periodo di riferimento per i calcoli. Se i prestatori di servizi di pagamento 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 «Commenti».

Utenti di servizi di pagamento interessati: i PSP dovrebbero indicare quali soglie sono 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. Le entità che effettuano la segnalazione per conto di più PSP (ossia la segnalazione consolidata) possono invece indicare intervalli di valori che rappresentano i valori più bassi e più elevati osservati o stimati all'interno del gruppo di PSP inclusi nel rapporto, separati da un trattino. I PSP dovrebbero considerare come «utenti di servizi di pagamento interessati» tutti i clienti (nazionali o stranieri, consumatori o imprese) che hanno un contratto con il prestatore di servizi di pagamento interessato che fornisce loro accesso al servizio di pagamento interessato e che hanno subito o probabilmente subiranno le conseguenze dell'incidente. I PSP, per determinare il numero di utenti di servizi di pagamento che potrebbero aver utilizzato il servizio di pagamento durante l'incidente, dovrebbero ricorrere a stime basate sulla propria attività passata. Nel caso di gruppi, ogni PSP dovrebbe considerare solo i propri utenti dei 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 dei 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.

Periodo di indisponibilità del servizio: i PSP dovrebbero indicare se la soglia è stata o probabilmente sarà raggiunta dall'incidente e i dati relativi: periodo totale di indisponibilità del servizio. Per questa variabile, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. Le entità che effettuano la segnalazione per conto di più PSP (ossia la segnalazione consolidata) possono invece indicare un intervallo di valori che includa i valori più bassi e più elevati osservati o stimati all'interno del gruppo di PSP inclusi nella rapporto, separati da un trattino. I PSP dovrebbero considerare il periodo di tempo in cui qualsiasi attività, processo o canale connesso alla prestazione di servizi di pagamento è o sarà probabilmente interrotto e, di conseguenza, impedirà (i) l'iniziazione e/o l'esecuzione di un servizio di pagamento e/o (ii)

l'accesso a un conto di pagamento. I PSP dovrebbero considerare 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 si rileva l'indisponibilità.

Impatto economico: i PSP dovrebbero indicare se la soglia è stata o probabilmente sarà raggiunta dall'incidente e i relativi dati: costi diretti e indiretti. Per queste variabili, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. Le entità che effettuano la segnalazione per conto di più PSP (ossia la segnalazione consolidata) possono invece indicare un intervallo di valori che includa i valori più bassi e più elevati osservati o stimati all'interno del gruppo di PSP inclusi nella rapporto, separati da un trattino. 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 delle attività espropriati, dei costi di sostituzione dell'hardware o del software, di altri costi forensi o di bonifica, delle spese dovute alla mancata osservanza di obblighi contrattuali, delle sanzioni, delle responsabilità esterne e delle perdite sulle entrate. Per quanto riguarda i costi indiretti, i PSP dovrebbero considerare solo quelli già noti o molto probabili.

Costi diretti: importo di denaro (euro) imputabile direttamente all'incidente, compresi i fondi necessari per risolvere l'incidente (ad esempio, fondi o beni espropriati, costi di sostituzione di hardware e software, penali dovute alla mancata osservanza degli obblighi contrattuali).

Costi indiretti: importo di denaro (euro) imputabile indirettamente all'incidente (ad esempio, risarcimenti, perdita di entrate a causa della mancata operatività, possibili costi legali).

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, il direttore della funzione informatica (CIO o posizione analoga) è stato o sarà probabilmente informato dell'accaduto in via straordinaria rispetto alle procedura di informazione periodica e in modo continuativo per tutta la durata dell'incidente

Nel caso di notifiche delegate, l'escalation avrebbe luogo all'interno della terza parte. 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 crisi aziendale.

Altri PSP o infrastrutture rilevanti potenzialmente interessati: i prestatori di servizi di pagamento dovrebbero valutare l'impatto dell'incidente sui mercati finanziari, inteso come infrastrutture dei mercati finanziari e/o schemi di pagamento con carte 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 la solidità 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 cessato o

probabilmente cesserà di adempiere i propri obblighi nelle infrastrutture del mercato finanziario di cui è membro.

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 indicatore affidabile del suo potenziale di influenzare la loro reputazione. I prestatori di servizi di pagamento dovrebbero considerare se (i) l'incidente ha influito su un processo visibile e pertanto riceverà probabilmente o ha già ricevuto copertura mediatica (non solo tramite i media tradizionali, come i giornali, ma anche blog, social networks, ecc.), (ii) non si sono adempiuti o probabilmente non si adempiranno obblighi regolamentari, (iii) sono state o probabilmente saranno violate sanzioni o (iv) lo stesso tipo di incidente si è già verificato in passato.

B 3 – Descrizione dell'incidente

Tipo di incidente: indicare se, per quanto noto, si tratta di un incidente operativo o di sicurezza.

Operativo: incidente derivante da processi inadeguati o malfunzionanti, persone e sistemi o eventi di forza maggiore che influenzano l'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi di pagamento.

Di sicurezza: accesso, uso, divulgazione, interruzione, modifica o distruzione non autorizzati delle risorse del PSP che influenzano l'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi di pagamento. Ciò può avvenire quando, tra le altre cose, il PSP è soggetto ad attacchi informatici, inadeguata progettazione o implementazione di politiche di sicurezza o inadeguata sicurezza fisica.

Causa dell'incidente: indicare la causa dell'incidente o, se questa non è ancora nota, quella più probabile. È possibile contrassegnare più caselle.

In fase di analisi: la causa non è ancora stata determinata.

Attacco esterno: l'origine della causa è esterna ed è intenzionalmente mirato al PSP (ad esempio, attacchi mediante malware).

Attacco interno: l'origine della causa è interna ed è intenzionalmente mirato al PSP (ad esempio, frode interna).

Tipo di attacco

Distributed/Denial of Service (D/DoS): tentativo di rendere non disponibile un servizio online richiedendolo con traffico da più fonti.

Contagio dei sistemi interni: attività malevola verso sistemi informatici che cerca di rubare spazio su disco rigido o tempo sulla CPU, accedere a informazioni private, alterare dati, mandare messaggi ai contatti, ecc.

Intrusione mirata: atto non autorizzato di spionaggio e sottrazione di informazioni attraverso il cyber-spazio.

Altro: qualsiasi altro tipo di attacco che il PSP possa aver subito, direttamente o tramite un prestatore di servizi tecnologici. In particolare, questa casella dovrebbe essere contrassegnata se vi è stato un attacco mirato al processo di autorizzazione e autenticazione. Dettagli dovrebbero essere aggiunti nel campo di testo libero.

Eventi esterni: la causa è associata a eventi generalmente al di fuori del controllo dell'organizzazione (ad esempio, disastri naturali, problemi legali, problemi aziendali e interdipendenze dei servizi).

Errore umano: l'incidente è stato causato dall'errore involontario di una persona nella 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).

Malfunzionamento del processo: la causa dell'incidente è stata l'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 che supportano l'attività di pagamento.

Altro: la causa dell'incidente non è nessuna di quelle precedentemente elencate. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

L'incidente vi ha interessati direttamente o indirettamente attraverso un fornitore di servizi?: un incidente può essere direttamente mirato a un PSP o interessarlo indirettamente, tramite un terza parte. In caso di impatto indiretto, fornire il nome del/i prestatore/i di servizi.

B 4 – Impatto dell'incidente

Edificio/i interessato/i (indirizzo), se applicabile: se è interessato un edificio fisico, indicarne l'indirizzo.

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 contrassegnare 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.

Servizi bancari telefonici: uso 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 accedere ad altri servizi.

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

Altro: il canale commerciale interessato non è uno di quelli citati in precedenza. 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 contrassegnare più caselle.

Deposito di contanti su un conto di pagamento: consegna di denaro a un PSP per accredito su un conto di pagamento.

Prelievo di contanti da un conto di pagamento: richiesta ricevuta da un PSP da parte del suo utente di servizi di pagamento relativa all'erogazione di contante e conseguente addebito dell'importo corrispondente sul suo 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 che consiste in un contratto tra PSP e un merchant per accettare ed elaborare le transazioni di pagamento, con un conseguente trasferimento di fondi al merchant.

Bonifici: servizio di pagamento per l'accredito sul conto di pagamento del beneficiario mediante una transazione di pagamento o una serie di transazioni di pagamento dal conto di pagamento del pagatore eseguite dal prestatore di servizi di pagamento 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 una transazione di pagamento è disposta dal beneficiario in base al consenso dato dal pagatore al beneficiario, al prestatore di servizi di pagamento del beneficiario o al prestatore di servizi di pagamento del pagatore stesso.

Pagamento basato su carta: servizio di pagamento basato sull'infrastruttura e le 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 transazioni 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: servizi di pagamento che dispongono 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: servizi online che forniscono 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.

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

Aree funzionali interessate: indicare la fase o le fasi del processo di pagamento interessate dall'incidente. È possibile contrassegnare più caselle.

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 terzi che agiscono per conto di quell'utente) al trasferimento di fondi o titoli.

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.

Sistemi e componenti interessati: indicare quale parte o quali parti dell'infrastruttura tecnologica del PSP sono state interessate dall'incidente. È possibile contrassegnare più caselle.

Applicativi/software: programmi, sistemi operativi, ecc. che supportano la prestazione di servizi di pagamento da parte del PSP.

Base di dati: struttura in cui sono archiviate le informazioni personali e di pagamento necessarie per eseguire operazioni di pagamento.

Hardware: apparecchiature tecnologiche fisiche che gestiscono i processi e/o archiviano i dati necessari ai PSP per svolgere le attività relative ai pagamenti.

Rete/infrastruttura: reti di telecomunicazione, pubbliche o private, che consentono lo scambio di dati e informazioni durante il processo di pagamento (ad esempio, Internet).

Altro: il sistema e il componente interessati non sono tra quelli precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Personale interessato: indicare se l'incidente ha avuto effetti sul personale del PSP e, in caso affermativo, fornire dettagli nel campo di testo libero.

B 5 – Mitigazione degli incidenti

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 i piani di continuità operativa e/o il piano di Disaster Recovery?: indicare se sono stati attivati o meno e, in caso affermativo, fornire i dettagli principali di ciò che è accaduto (ossia specificare quando sono stati attivatie in cosa consistevano tali piani).

Il PSP ha annullato o attenuato l'intensità di alcune misure di controllo a causa dell'incidente?: indicare se il PSP ha dovuto ignorare alcune misure di controllo (ad esempio, interrompendo l'applicazione del principio del doppio controllo) per affrontare l'incidente e, in caso affermativo, fornire dettagli relativi alle motivazioni alla base dell'attenuazione o dell'annullamento delle misure di controllo.

C – Rapporto finale

C 1 – Informazioni generali

Aggiornamento delle informazioni del rapporto intermedio (sintesi): fornire ulteriori informazioni sulle azioni intraprese per ripristinare l'attività a seguito dell'incidente e per evitare che questo si ripeta, sull'analisi delle cause all'origine, sulle lezioni apprese, ecc.

Data e ora di chiusura dell'incidente: indicare la data e l'ora in cui l'incidente è stato considerato chiuso.

Le misure di controllo originali sono stati ripristinate?: laddove il PSP abbia dovuto annullare o attenuare l'intensità di alcune misure di controllo a causa dell'incidente, indicare se le misure di controllo sono nuovamente attive e fornire ulteriori informazioni nel campo di testo libero.

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

Quale è stata la causa all'origine dell'incidente, se già nota?: spiegare qual è la causa all'origine dell'incidente o, se non ancora nota, le conclusioni preliminari tratte dall'analisi delle cause all'origine dell'incidente. I PSP possono allegare un file con informazioni dettagliate se ritenuto necessario.

Principali azioni correttive/misure adottate o pianificate per impedire che l'incidente si verifichi nuovamente in futuro, se già note: descrivere le principali azioni intraprese o previste per evitare il ripetersi dell'incidente 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 qualunque azione legale (ad esempio, se è stato citato in tribunale o ha perso la sua licenza) a seguito dell'incidente.