



COMMISSIONE
EUROPEA

Bruxelles, 23.10.2024
C(2024) 7277 final

REGOLAMENTO DI ESECUZIONE (UE) .../... DELLA COMMISSIONE

del 23.10.2024

che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un incidente grave connesso alle TIC e notificare una minaccia informatica significativa

(Testo rilevante ai fini del SEE)

REGOLAMENTO DI ESECUZIONE (UE) .../... DELLA COMMISSIONE

del 23.10.2024

che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un incidente grave connesso alle TIC e notificare una minaccia informatica significativa

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011¹, in particolare l'articolo 20, quarto comma,

considerando quanto segue:

- (1) Al fine di garantire che le entità finanziarie segnalino gli incidenti gravi alle rispettive autorità competenti in modo coerente e far sì che trasmettano a tali autorità dati di buona qualità, è opportuno specificare quali campi di dati debbano essere compilati dalle entità finanziarie nelle varie fasi della segnalazione di cui all'articolo 19, paragrafo 4, del regolamento (UE) 2022/2554. È importante che tali informazioni siano presentate in modo da fornire un'unica panoramica dell'incidente. A tal fine è pertanto necessario definire un modello unico per la segnalazione.
- (2) Le entità finanziarie dovrebbero compilare i campi di dati del modello di segnalazione che corrispondono agli obblighi di informazione della rispettiva notifica o relazione. Tuttavia le entità finanziarie che dispongono già di informazioni che devono essere fornite in una fase successiva della segnalazione, ossia nella relazione intermedia o finale, dovrebbero essere autorizzate ad anticipare la trasmissione dei dati.
- (3) Poiché gli incidenti multipli o ricorrenti possono costituire un incidente grave ai sensi dell'articolo 8 del regolamento delegato (UE) 2024/1772 della Commissione², l'impostazione del modello di segnalazione e dei campi di dati dovrebbe consentire alle entità finanziarie di segnalare tali incidenti ricorrenti.

¹ Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>).

² Regolamento delegato (UE) 2024/1772 della Commissione, del 13 marzo 2024, che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri per la classificazione degli incidenti connessi alle TIC e delle minacce informatiche, stabiliscono le soglie di rilevanza e specificano i dettagli delle segnalazioni di gravi incidenti (GU L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

- (4) Per garantire la presentazione di informazioni accurate e aggiornate, il modello di segnalazione dovrebbe consentire alle entità finanziarie, all'atto della trasmissione della relazione intermedia e finale, di aggiornare le informazioni presentate in precedenza e, se necessario, di riclassificare gli incidenti gravi come non gravi.
- (5) L'identificazione giuridica delle entità dovrebbe essere allineata agli identificatori specificati nelle norme tecniche di attuazione adottate ai sensi dell'articolo 28, paragrafo 9, del regolamento (UE) 2022/2554.
- (6) Qualora le entità finanziarie esternalizzino a terzi gli obblighi di segnalazione di incidenti gravi connessi alle TIC, le autorità competenti dovrebbero essere a conoscenza dell'identità del terzo che effettua la segnalazione per conto dell'entità finanziaria prima della trasmissione della prima notifica o relazione, al fine di verificare la legittimità del terzo che effettua la segnalazione.
- (7) Per individuare agevolmente l'impatto di un incidente verificatosi presso un fornitore terzo o da esso causato e che interessa più entità finanziarie all'interno di un unico Stato membro, e per ridurre lo sforzo di segnalazione per le entità finanziarie, il modello di segnalazione dovrebbe consentire la trasmissione di una relazione aggregata contenente informazioni aggregate in merito all'impatto dell'incidente su tutte le entità finanziarie interessate che hanno classificato l'incidente come grave.
- (8) Il modello di segnalazione dovrebbe essere impostato in modo tecnologicamente neutro al fine di consentirne l'implementazione in varie soluzioni di segnalazione degli incidenti già esistenti o che possono essere sviluppate ai fini dell'attuazione degli obblighi di cui al regolamento (UE) 2022/2554.
- (9) L'impostazione del modello di segnalazione e dei campi di dati dovrebbe agevolare la segnalazione degli incidenti gravi connessi alle TIC da parte dei terzi ai quali le entità finanziarie hanno esternalizzato l'obbligo di segnalazione a norma dell'articolo 19, paragrafo 5, del regolamento (UE) 2022/2554.
- (10) Il presente regolamento si basa sui progetti di norme tecniche di attuazione che le autorità europee di vigilanza hanno presentato alla Commissione.
- (11) Le autorità europee di vigilanza hanno condotto consultazioni pubbliche aperte sui progetti di norme tecniche di attuazione sui quali è basato il presente regolamento, hanno analizzato i potenziali costi e benefici collegati e hanno chiesto la consulenza del gruppo delle parti interessate nel settore bancario istituito in conformità dell'articolo 37 rispettivamente dei regolamenti (UE) n. 1093/2010³, (UE) n. 1094/2010⁴ e (UE) n. 1095/2010⁵, del Parlamento europeo e del Consiglio.

³ 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, ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

⁴ Regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/79/CE della Commissione (GU L 331 del 15.12.2010, pag. 48, ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

⁵ Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione (GU L 331 del 15.12.2010, pag. 84, ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

- (12) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio⁶, il Garante europeo della protezione dei dati è stato consultato e ha formulato un parere positivo il 22 luglio 2024. Qualsiasi trattamento di dati personali che rientra nell'ambito di applicazione del presente regolamento dovrebbe essere effettuato conformemente ai principi applicabili in materia di protezione dei dati e alle disposizioni di cui al regolamento (UE) 2018/1725,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Modello per la segnalazione degli incidenti gravi connessi alle TIC

1. Le entità finanziarie utilizzano il modello di cui all'allegato I per trasmettere la notifica iniziale, la relazione intermedia e la relazione finale di cui all'articolo 19, paragrafo 4, del regolamento (UE) 2022/2554 come segue:
 - (a) le entità finanziarie che presentano una notifica iniziale compilano i campi di dati del modello che corrispondono alle informazioni da fornire a norma dell'articolo 2 del regolamento delegato (UE) 2024/xxx della Commissione [C (2024) 6901]⁷ e possono, qualora dispongano già di tali informazioni, completare i campi di dati la cui compilazione non è richiesta per una notifica iniziale ma è richiesta per una relazione intermedia o finale;
 - (b) le entità finanziarie che presentano una relazione intermedia compilano i campi di dati del modello che corrispondono alle informazioni da fornire a norma dell'articolo 3 del regolamento delegato (UE) 2024/xxx [C (2024) 6901] e possono, qualora dispongano già di tali informazioni, completare i campi di dati la cui compilazione non è richiesta per la relazione intermedia ma è richiesta per la relazione finale.
 - (c) le entità finanziarie che presentano una relazione finale compilano i campi di dati del modello che corrispondono alle informazioni da fornire a norma dell'articolo 4 del regolamento delegato (UE) 2024/xxx [C (2024) 6901].
2. Le entità finanziarie garantiscono che le informazioni contenute nella notifica iniziale, nella relazione intermedia e nella relazione finale siano complete e accurate.
3. Le entità finanziarie forniscono stime dei valori sulla base di altri dati e informazioni disponibili, nella misura del possibile, qualora non siano disponibili dati accurati al momento della trasmissione della notifica iniziale o della relazione intermedia.
4. All'atto della trasmissione di una relazione intermedia o finale, le entità finanziarie utilizzano il modello di cui all'allegato I per fornire tutte le informazioni richieste e

⁶ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n 1247/2002/CE

(GU L 295 del 21.11.2018, pag. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

⁷ Regolamento delegato (UE) 2024/xxx della Commissione che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano il contenuto e i termini della notifica iniziale, della relazione intermedia e della relazione finale per gli incidenti gravi connessi alle TIC nonché il contenuto della notifica volontaria per le minacce informatiche significative. (GU L, xxx/xxx, ELI: xxx). [OP: inserire il riferimento a C(2024) 6901]

aggiornare, se del caso, le informazioni precedentemente fornite nella notifica iniziale o nella relazione intermedia.

5. All'atto della compilazione del modello di cui all'allegato I le entità finanziarie seguono il glossario dei dati e le istruzioni di cui all'allegato II.

Articolo 2

Trasmissione congiunta della notifica iniziale, della relazione intermedia e della relazione finale

Le entità finanziarie possono combinare la presentazione della notifica iniziale, della relazione intermedia e della relazione finale per fornire due o tutte le informazioni contemporaneamente, qualora siano riprese le attività regolari o sia stata completata l'analisi delle cause profonde e purché siano rispettati i termini di cui all'articolo 5 del regolamento delegato (UE) 2024/xxx della Commissione [C (2024) 6901].

Articolo 3

Incidenti ricorrenti connessi alle TIC

Le entità finanziarie che forniscono informazioni su incidenti ricorrenti connessi alle TIC non gravi che soddisfano cumulativamente le condizioni per la sussistenza di un incidente grave connesso alle TIC di cui all'articolo 8, paragrafo 2, del regolamento delegato (UE) 2024/1772 trasmettono tali informazioni in forma aggregata.

Articolo 4

Uso di canali elettronici sicuri

1. Le entità finanziarie utilizzano canali elettronici sicuri messi a disposizione dalla rispettiva autorità competente per la trasmissione della notifica iniziale e delle relazioni intermedia e finale.
2. Le entità finanziarie che non sono in grado di utilizzare i canali elettronici sicuri messi a disposizione dalla rispettiva autorità competente informano la propria autorità competente in merito a un incidente grave connesso alle TIC mediante altri mezzi sicuri, d'intesa con l'autorità competente. Se richiesto dall'autorità competente, le entità finanziarie trasmettono nuovamente la notifica iniziale oppure la relazione intermedia o finale, attraverso il canale elettronico sicuro messo a disposizione dalla rispettiva autorità competente appena sono in grado di farlo.

Articolo 5

Riclassificazione degli incidenti gravi connessi alle TIC

Se, dopo un'ulteriore valutazione, l'entità finanziaria conclude che l'incidente connesso alle TIC precedentemente segnalato come grave non soddisfaceva in alcun momento i criteri e le soglie di classificazione di cui all'articolo 8 del regolamento delegato (UE) 2024/1772, l'entità finanziaria notifica all'autorità competente di aver riclassificato l'incidente connesso alle TIC da grave a non grave fornendo le informazioni relative a tale riclassificazione nel modello di cui all'allegato II del presente regolamento nei campi "tipo di segnalazione" e "altre informazioni".

Articolo 6

Notifica dell'esternalizzazione degli obblighi di segnalazione

1. Le entità finanziarie che hanno esternalizzato l'obbligo di segnalazione degli incidenti gravi connessi alle TIC a norma dell'articolo 19, paragrafo 5, del regolamento (UE) 2022/2554 informano l'autorità competente di tale accordo di esternalizzazione non appena quest'ultimo è stato concluso e al più tardi prima della prima notifica o relazione.
2. Le entità finanziarie forniscono all'autorità competente il nome, le informazioni di contatto e il codice identificativo del terzo che trasmetterà per loro conto le notifiche o le relazioni in merito agli incidenti gravi connessi alle TIC.
3. Le entità finanziarie informano la rispettiva autorità competente non appena cessano di esternalizzare i propri obblighi di segnalazione di cui all'articolo 19, paragrafo 5, del regolamento (UE) 2022/2554.

Articolo 7

Segnalazione aggregata

1. Un fornitore terzo di servizi cui sono stati esternalizzati obblighi di segnalazione conformemente all'articolo 19, paragrafo 5, del regolamento (UE) 2022/2554 può utilizzare il modello di cui all'allegato I del presente regolamento per fornire informazioni aggregate in merito a un incidente grave connesso alle TIC che ha un impatto su più entità finanziarie in un'unica notifica o relazione e trasmettere tale notifica o relazione all'autorità competente per conto di tutte le entità finanziarie interessate, purché siano soddisfatte tutte le condizioni seguenti:
 - (a) l'incidente grave connesso alle TIC da segnalare ha origine presso un fornitore terzo di servizi TIC o è causato da quest'ultimo;
 - (b) il fornitore terzo di servizi presta il servizio TIC pertinente a più di un'entità finanziaria o a un gruppo;
 - (c) l'incidente connesso alle TIC è classificato come grave da ciascuna entità finanziaria interessata nella notifica o relazione aggregata;
 - (d) l'incidente grave connesso alle TIC interessa entità finanziarie all'interno di un unico Stato membro e la relazione aggregata si riferisce a entità finanziarie sottoposte alla vigilanza della medesima autorità competente;
 - (e) le autorità competenti hanno esplicitamente consentito a questo tipo di entità finanziarie di aggregare le loro segnalazioni.
2. Il paragrafo 1 non si applica agli enti creditizi considerati significativi di cui all'articolo 2, punto 16), del regolamento (UE) n. 468/2014⁸, ai gestori delle sedi di negoziazione e alle controparti centrali, che utilizzano il modello di cui all'allegato I solo per trasmettere notifiche o relazioni individuali in merito a incidenti gravi connessi alle TIC alla rispettiva autorità competente.

⁸ REGOLAMENTO (UE) N. 468/2014 DELLA BANCA CENTRALE EUROPEA, del 16 aprile 2014, che istituisce il quadro di cooperazione nell'ambito del Meccanismo di vigilanza unico tra la Banca centrale europea e le autorità nazionali competenti e con le autorità nazionali designate (GU L 141 del 14.5.2014, pag. 1).

3. Qualora le autorità competenti richiedano informazioni sull'impatto individuale dell'incidente grave connesso alle TIC su un'unica entità finanziaria, su richiesta dell'autorità competente l'entità finanziaria trasmette una notifica o una relazione individuale in merito all'incidente grave connesso alle TIC.

Articolo 8

Notifica delle minacce informatiche significative

1. Le entità finanziarie che notificano minacce informatiche significative alle autorità competenti a norma dell'articolo 19, paragrafo 2, del regolamento (UE) 2022/2554 utilizzano il modello di cui all'allegato III del presente regolamento e seguono il glossario dei dati e le istruzioni di cui all'allegato IV del presente regolamento.
2. Le entità finanziarie garantiscono che le informazioni contenute nella notifica delle minacce informatiche significative siano complete e accurate.

Articolo 9

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 23.10.2024

Per la Commissione

La presidente

Ursula VON DER LEYEN