COMMISSIONE
EUROPEA

Bruxelles, 23.10.2024
C(2024) 6901 final

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

del 23.10.2024

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

(Testo rilevante ai fini del SEE)

RELAZIONE

1. CONTESTO DELL'ATTO DELEGATO

Uno degli obiettivi del regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (DORA) è quello di armonizzare e semplificare il regime di segnalazione degli incidenti connessi alle TIC per le entità finanziarie nell'Unione europea (UE).

L'articolo 20 del regolamento DORA conferisce alle autorità europee di vigilanza (AEV) il mandato di elaborare, tramite il comitato congiunto e in consultazione con la Banca centrale europea e l'Agenzia dell'Unione europea per la cibersicurezza, quanto segue:

- progetti di norme tecniche di regolamentazione che stabiliscano il contenuto delle segnalazioni relative agli incidenti connessi alle TIC e della notifica per le minacce informatiche significative nonché i termini entro i quali le entità finanziarie sono tenute a segnalare tali incidenti alle autorità competenti.

L'articolo 20 del regolamento DORA impone inoltre alle AEV di garantire che gli obblighi imposti da detto regolamento siano proporzionati e coerenti con l'approccio per la segnalazione degli incidenti di cui alla direttiva (UE) 2022/2555 (NIS 2).

2. CONSULTAZIONI PRECEDENTI L'ADOZIONE DELL'ATTO

Nell'ambito dell'elaborazione delle norme di cui al presente regolamento, l'8 dicembre 2023 le autorità europee di vigilanza hanno pubblicato il progetto di norme tecniche di regolamentazione per una consultazione di tre mesi, che si è conclusa il 4 marzo 2024. Sono pervenute alle AEV 109 risposte da parte di una varietà di partecipanti al mercato del settore finanziario. La relazione finale delle AEV fornisce una panoramica completa delle risposte dei portatori di interessi.

Alla luce delle osservazioni ricevute, le AEV hanno concordato con la maggior parte delle proposte e delle relative argomentazioni e hanno apportato modifiche alle norme tecniche di regolamentazione. Tali modifiche riguardano i termini per la trasmissione della notifica iniziale, della relazione intermedia e della relazione finale, la segnalazione durante il fine settimana e nei giorni festivi, la segnalazione aggregata e la razionalizzazione del contenuto del modello di segnalazione.

Per quanto riguarda i termini per la segnalazione, le AEV hanno prolungato il termine per la trasmissione della relazione intermedia fino a 24 ore e quello per la trasmissione della relazione finale ad almeno 72 ore, iniziando il calcolo di decorrenza dei termini dalla trasmissione della notifica/relazione precedente invece che dal momento della classificazione dell'incidente, come previsto nel progetto iniziale di norme tecniche di regolamentazione proposto per la consultazione.

Per quanto riguarda la segnalazione durante il fine settimana e nei giorni festivi, le AEV hanno ridotto l'ambito degli incidenti da segnalare, hanno eliminato l'obbligo per le entità finanziarie di minori dimensioni di trasmettere la notifica iniziale e hanno prolungato il termine per la trasmissione delle notifiche e delle relazioni fino alle ore 12:00 del primo giorno lavorativo anziché entro un'ora, come previsto nel progetto iniziale di norme tecniche di regolamentazione proposto per la consultazione.

Infine le AEV hanno introdotto segnalazioni aggregate a livello nazionale per le entità finanziarie sottoposte a vigilanza da parte di un'unica autorità competente, in presenza di determinate condizioni.

3. ELEMENTI GIURIDICI DELL'ATTO DELEGATO

L'articolo 1 stabilisce il formato del tipo di informazioni che devono essere fornite da parte delle entità finanziarie.

L'articolo 2 stabilisce la natura delle informazioni generali che le entità finanziarie devono fornire nel caso della notifica iniziale dell'incidente grave connesso alle TIC e delle relazioni intermedie e finali.

L'articolo 3 definisce le informazioni che le entità finanziarie devono fornire in merito all'incidente grave connesso alle TIC nella loro notifica iniziale.

L'articolo 4 definisce le informazioni che le entità finanziarie devono fornire in merito all'incidente grave connesso alle TIC nella loro relazione intermedia.

L'articolo 5 definisce le informazioni che le entità finanziarie devono fornire in merito all'incidente grave connesso alle TIC nella loro relazione finale.

L'articolo 6 stabilisce i termini per la trasmissione della notifica iniziale, della relazione intermedia e della relazione finale di cui all'articolo 19, paragrafo 4, del regolamento (UE) 2022/2554.

L'articolo 7 stabilisce il contenuto della notifica volontaria per le minacce informatiche significative.

L'articolo 8 contiene le disposizioni finali relative all'entrata in vigore.

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

del 23.10.2024

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

(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) 2016/1011[1], in particolare l'articolo 20, terzo comma,

considerando quanto segue:

(1) Al fine di garantire l'armonizzazione e la semplificazione degli obblighi di notifica e di segnalazione degli incidenti gravi connessi alle TIC di cui all'articolo 19, paragrafo 4, del regolamento (UE) 2022/2554, i termini per la segnalazione degli incidenti gravi connessi alle TIC dovrebbero seguire un approccio coerente per tutti i tipi di entità finanziarie. Per tali motivi, nella misura del possibile, i termini dovrebbero seguire un approccio coerente anche con le disposizioni di cui alla direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[2] ed avere almeno un effetto equivalente alle stesse.

(2) Onde evitare di imporre un onere di segnalazione eccessivo alle entità finanziarie nel momento in cui trattano l'incidente connesso alle TIC, il contenuto della notifica iniziale dovrebbe essere limitato alle informazioni più significative. Per poter adottare misure di vigilanza adeguate è necessario che le autorità competenti ricevano le informazioni sugli incidenti gravi connessi alle TIC il più rapidamente possibile dopo che l'entità finanziaria ha classificato un incidente connesso alle TIC come grave. Di conseguenza il termine per la trasmissione della notifica iniziale di cui all'articolo 19, paragrafo 4, lettera a), del regolamento (UE) 2022/2554 dovrebbe essere il più breve possibile dopo che un incidente connesso alle TIC è stato classificato come grave, pur consentendo flessibilità, soprattutto per i modelli operativi dei servizi che non sono

[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] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

particolarmente critici in termini di tempo, nel caso in cui le entità finanziarie abbiano bisogno di più tempo per trattare l'incidente connesso alle TIC dopo esserne venute a conoscenza.

(3) Dopo aver ricevuto la notifica iniziale, le autorità competenti dovrebbero ricevere informazioni più dettagliate sull'incidente connesso alle TIC nella relazione intermedia e tutte le informazioni pertinenti nella relazione finale. Le informazioni contenute in tali relazioni dovrebbero consentire alle autorità competenti di esaminare ulteriormente l'incidente connesso alle TIC e di valutare le misure di vigilanza che potrebbero considerare di adottare.

(4) I termini per la segnalazione di cui all'articolo 20, primo comma, lettera a), punto ii), del regolamento (UE) 2022/2554 dovrebbero pertanto trovare un equilibrio tra la necessità per le autorità competenti di ricevere le informazioni rapidamente e la necessità di concedere alle entità finanziarie il tempo sufficiente per ottenere informazioni complete e accurate.

(5) Tenendo conto dei criteri di cui all'articolo 20, primo comma, lettera a), del regolamento (UE) 2022/2554, i termini per la segnalazione non dovrebbero comportare un onere sproporzionato per le microimprese e le altre entità finanziarie che non sono significative. Inoltre, per evitare un onere sproporzionato per le entità finanziarie, i termini per la segnalazione dovrebbero tenere conto dei fine settimana e dei giorni festivi.

(6) Poiché le minacce informatiche significative devono essere notificate su base volontaria, il contenuto di tali notifiche non dovrebbe costituire un onere per le entità finanziarie e dovrebbe essere più limitato rispetto alle informazioni richieste per gli incidenti gravi connessi alle TIC.

(7) Il presente regolamento si basa sui progetti di norme tecniche di regolamentazione che le autorità europee di vigilanza hanno presentato alla Commissione.

(8) Le autorità europee di vigilanza hanno condotto consultazioni pubbliche aperte sui progetti di norme tecniche di regolamentazione sui quali è basato il presente regolamento, hanno analizzato i potenziali costi e benefici collegati e hanno chiesto la consulenza dei gruppi delle parti interessate istituiti in conformità dell'articolo 37 rispettivamente dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e UE) n. 1095/2010, del Parlamento europeo e del Consiglio[3].

(9) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[4], il Garante europeo della protezione dei dati è

---

[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); 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) e 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). http://data.europa.eu/eli/reg/2010/1095/oj);

[4] 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

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 del regolamento (UE) 2018/1725,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Informazioni generali da fornire nelle notifiche iniziali e nelle relazioni intermedie e finali in merito agli incidenti gravi connessi alle TIC

Le entità finanziarie includono nella notifica iniziale, nella relazione intermedia e nella relazione finale di cui all'articolo 19, paragrafo 4, del regolamento (UE) 2022/2554 le informazioni generali seguenti:

(a) il tipo di segnalazione (notifica iniziale, relazione intermedia o relazione finale);

(b) la denominazione dell'entità finanziaria, il rispettivo codice LEI e il tipo di entità finanziaria di cui all'articolo 2, paragrafo 1, del regolamento (UE) 2022/2554;

(c) la denominazione e il codice identificativo dell'entità che trasmette la notifica iniziale, la relazione intermedia o la relazione finale per l'entità finanziaria;

(d) se del caso, le denominazioni e i codici LEI di tutte le entità finanziarie interessate dalla notifica iniziale o dalla relazione intermedia o finale aggregate;

(e) le informazioni di contatto delle persone responsabili della comunicazione con l'autorità competente in merito all'incidente grave connesso alle TIC;

(f) se del caso, l'identificazione dell'impresa madre del gruppo cui appartiene l'entità finanziaria;

(g) in caso di impatto monetario, la valuta su cui si basano gli importi.

Articolo 2

Informazioni specifiche da fornire nelle notifiche iniziali

Le notifiche iniziali di cui all'articolo 19, paragrafo 4, lettera a), del regolamento (UE) 2022/2554 contengono almeno tutte le informazioni specifiche seguenti:

(a) il codice di riferimento dell'incidente assegnato dall'entità finanziaria;

(b) la data e l'ora di individuazione e la classificazione dell'incidente a norma dell'articolo 8 del regolamento delegato (UE) 2024/1772 della Commissione[5];

(c) una descrizione dell'incidente connesso alle TIC;

(d) i criteri di cui agli articoli da 1 a 8 del regolamento delegato (UE) 2024/1772 in base ai quali l'entità finanziaria ha classificato l'incidente connesso alle TIC come grave;

---

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).

[5] 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).

(e) gli Stati membri interessati dall'incidente connesso alle TIC;

(f) informazioni sulle modalità di constatazione dell'incidente connesso alle TIC;

(g) se disponibili, informazioni sull'origine dell'incidente connesso alle TIC;

(h) informazioni che indichino se l'entità finanziaria abbia attivato un piano di continuità operativa;

(i) se del caso, informazioni sulla riclassificazione dell'incidente connesso alle TIC da grave a non grave;

(j) se disponibile, ogni altra informazione pertinente.

Articolo 3
Informazioni specifiche da fornire nelle relazioni intermedie

Le relazioni intermedie di cui all'articolo 19, paragrafo 4, lettera b), del regolamento (UE) 2022/2554 contengono almeno tutte le informazioni specifiche seguenti:

(a) se del caso, il codice di riferimento dell'incidente fornito dall'autorità competente;

(b) la data e l'ora in cui si è verificato l'incidente connesso alle TIC;

(c) se del caso, la data e l'ora in cui l'entità finanziaria ha ripreso le sue regolari attività;

(d) informazioni sul modo in cui sono stati soddisfatti i criteri di cui agli articoli da 1 a 8 del regolamento delegato (UE) 2024/1772, in base ai quali l'entità finanziaria ha classificato l'incidente connesso alle TIC come grave;

(e) il tipo di incidente connesso alle TIC;

(f) se del caso, le minacce e le tecniche utilizzate dall'autore della minaccia;

(g) le aree funzionali e i processi commerciali interessati;

(h) le componenti infrastrutturali interessate che sostengono i processi commerciali;

(i) l'impatto sugli interessi finanziari dei clienti;

(j) informazioni sulla segnalazione dell'incidente connesso alle TIC ad altre autorità;

(k) le azioni o misure temporanee adottate o previste dall'entità finanziaria per effettuare il ripristino a seguito dell'incidente connesso alle TIC;

(l) se del caso, informazioni sugli indicatori di compromissione.

Articolo 4
Informazioni specifiche da fornire nelle relazioni finali

Le relazioni finali di cui all'articolo 19, paragrafo 4, lettera c), del regolamento (UE) 2022/2554 contengono tutte le informazioni specifiche seguenti:

(a) informazioni sulle cause di fondo dell'incidente connesso alle TIC;

(b) la data e l'ora in cui l'incidente connesso alle TIC è stato risolto e in cui sono state affrontate le cause di fondo;

(c) informazioni sulla risoluzione dell'incidente connesso alle TIC;

(d) se del caso, informazioni pertinenti per le autorità di risoluzione;

(e) informazioni sui costi diretti e indiretti e sulle perdite derivanti dall'incidente connesso alle TIC e informazioni sui recuperi finanziari;

(f) se del caso, informazioni sugli incidenti ricorrenti connessi alle TIC.

Articolo 5
Termini per la notifica iniziale e per le relazioni intermedia e finale

1. Le entità finanziarie trasmettono la notifica iniziale e le relazioni intermedia e finale di cui all'articolo 19, paragrafo 4, lettere a), b) e c), del regolamento (UE) 2022/2554 entro i termini seguenti:

   (a) per la relazione iniziale: quanto prima, ma in ogni caso entro quattro ore dalla classificazione dell'incidente connesso alle TIC come grave ed entro 24 ore dal momento in cui l'entità finanziaria è venuta a conoscenza dell'incidente connesso alle TIC;

   (b) per la relazione intermedia: al più tardi entro 72 ore dalla trasmissione della notifica iniziale, anche se lo stato o il trattamento dell'incidente non sono cambiati conformemente all'articolo 19, paragrafo 4, lettera b), del regolamento (UE) 2022/2554. Le entità finanziarie trasmettono una relazione intermedia aggiornata senza indebito ritardo e in ogni caso quando sono state riprese le regolari attività;

   (c) per la relazione finale: entro un mese dalla trasmissione della relazione intermedia o, se del caso, dall'ultima relazione intermedia aggiornata.

2. Se l'entità finanziaria non ha classificato un incidente connesso alle TIC come grave entro 24 ore dal momento in cui ne è venuta a conoscenza, ma lo classifica come grave in una fase successiva, l'entità finanziaria trasmette la notifica iniziale entro quattro ore dalla classificazione dell'incidente connesso alle TIC come grave.

3. Le entità finanziarie che non sono in grado di trasmettere la notifica iniziale, la relazione intermedia o la relazione finale entro i termini di cui al paragrafo 1 ne informano l'autorità competente senza indebito ritardo, e comunque entro i rispettivi termini per la trasmissione della notifica o della relazione, spiegando i motivi del ritardo.

4. Se il termine per la trasmissione di una notifica iniziale, di una relazione intermedia o di una relazione finale cade in un giorno del fine settimana o in un giorno festivo nello Stato membro dell'entità finanziaria che effettua la segnalazione, l'entità finanziaria può trasmettere la notifica iniziale, la relazione intermedia o la relazione finale entro le ore 12:00 del giorno lavorativo successivo.

5. Il paragrafo 4 non si applica alla trasmissione di una notifica iniziale o di una relazione intermedia da parte di enti creditizi, controparti centrali, gestori delle sedi di negoziazione e altre entità finanziarie identificate come soggetti essenziali o importanti ai sensi dell'articolo 3 della direttiva (UE) 2022/2555.

6. Le autorità competenti possono decidere che il paragrafo 4 non si applichi alla trasmissione di una notifica iniziale o di una relazione intermedia da parte di entità finanziarie, diverse da quelle di cui al paragrafo 5, che sono significative o hanno carattere sistemico per il settore finanziario a livello nazionale o dell'Unione. Le autorità competenti notificano la loro decisione alle entità finanziarie individuate. La decisione dell'autorità competente si applica solo agli incidenti segnalati dopo la data

di notifica della decisione da parte dell'autorità competente alle entità finanziarie individuate.

Articolo 6
Contenuto della notifica volontaria delle minacce informatiche significative

Il contenuto della notifica volontaria delle minacce informatiche significative di cui all'articolo 19, paragrafo 2, del regolamento (UE) 2022/2554 comprende tutti gli elementi seguenti:

(a) informazioni generali sull'entità finanziaria che effettua la notifica di cui all'articolo 1;

(b) la data e l'ora dell'individuazione della minaccia informatica significativa e qualsiasi altra validazione temporale pertinente relativa alla minaccia informatica significativa;

(c) una descrizione della minaccia informatica significativa;

(d) informazioni relative al potenziale impatto della minaccia informatica significativa sull'entità finanziaria, sui suoi clienti o sulle controparti finanziarie;

(e) i criteri di classificazione che avrebbero determinato una segnalazione di incidente grave di cui agli articoli da 1 a 8 del regolamento delegato (UE) 2024/1772 se la minaccia informatica si fosse concretizzata;

(f) informazioni sullo stato della minaccia informatica significativa e su eventuali cambiamenti nell'attività di minaccia;

(g) se del caso, una descrizione delle azioni adottate dall'entità finanziaria per prevenire il concretizzarsi delle minacce informatiche significative;

(h) informazioni su qualsiasi notifica della minaccia informatica significativa ad altre entità finanziarie o autorità;

(i) se del caso, informazioni sugli indicatori di compromissione;

(j) se disponibile, ogni altra informazione pertinente.

Articolo 7
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