REGOLAMENTO DELEGATO (UE) 2025/295 DELLA COMMISSIONE

del 24 ottobre 2024

che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione sull'armonizzazione delle condizioni che consentono lo svolgimento delle attività di sorveglianza

(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 41, paragrafo 2, secondo comma,

considerando quanto segue:

(1) Il quadro sulla resilienza operativa digitale per il settore finanziario istituito dal regolamento (UE) 2022/2554 introduce un quadro di sorveglianza dell'Unione per i fornitori terzi di servizi delle tecnologie dell'informazione e della comunicazione (TIC) al settore finanziario designati come critici a norma dell'articolo 31 di tale regolamento.

(2) Il fornitore terzo di servizi TIC che decida di presentare una domanda di designazione volontaria quale fornitore critico dovrebbe fornire all'autorità europea di vigilanza (AEV) ricevente tutte le informazioni necessarie per dimostrare la propria criticità conformemente ai principi e ai criteri di cui al regolamento (UE) 2022/2554. Per questo motivo, le informazioni da includere nella domanda volontaria dovrebbero essere sufficientemente dettagliate e complete in modo da consentire una valutazione chiara e completa della criticità ai sensi dell'articolo 31, paragrafo 11, di tale regolamento. L'AEV competente dovrebbe respingere qualsiasi domanda incompleta e richiedere le informazioni mancanti.

(3) L'identificazione giuridica dei fornitori terzi di servizi TIC che rientrano nell'ambito di applicazione della presente norma tecnica di regolamentazione dovrebbe essere in linea con il codice identificativo di cui al regolamento di esecuzione della Commissione adottato in conformità dell'articolo 28, paragrafo 9, del regolamento (UE) 2022/2554.

(4) L'autorità di sorveglianza capofila, per dare seguito alle raccomandazioni da essa rivolte ai fornitori terzi critici di servizi TIC, dovrebbe monitorare il rispetto delle raccomandazioni da parte di questi ultimi. Al fine di garantire un monitoraggio efficiente ed efficace delle azioni adottate o dei rimedi applicati dai fornitori terzi critici di servizi TIC in relazione a tali raccomandazioni, l'autorità di sorveglianza capofila dovrebbe poter richiedere le relazioni di cui all'articolo 35, paragrafo 1, lettera c), del regolamento (UE) 2022/2554, vale a dire le relazioni intermedie sullo stato di avanzamento e le relazioni finali.

(5) Ai fini della valutazione di cui all'articolo 42, paragrafo 1, del regolamento (UE) 2022/2554, secondo cui l'autorità di sorveglianza capofila è tenuta a valutare se la spiegazione fornita dal fornitore terzo critico di servizi TIC sia sufficiente, la notifica all'autorità di sorveglianza capofila da parte del fornitore terzo critico di servizi TIC della sua intenzione di attenersi alle raccomandazioni ricevute dovrebbe essere integrata da una descrizione delle azioni e delle misure adottate per attenuare i rischi delineati nelle raccomandazioni, unitamente alla rispettiva tempistica. Tale spiegazione dovrebbe assumere la forma di un piano correttivo.

(6) Poiché l'autorità di sorveglianza capofila dovrebbe valutare gli accordi di subappalto del fornitore terzo critico di servizi TIC, è necessario elaborare un modello per la trasmissione di informazioni su tali accordi. Il modello dovrebbe tenere conto del fatto che i fornitori terzi critici di servizi TIC hanno strutture diverse rispetto alle entità finanziarie.

([1]) GU L 333 del 27.12.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Una volta che l'autorità di sorveglianza capofila ha formulato le raccomandazioni a un fornitore terzo critico di servizi TIC e che le autorità competenti hanno informato le entità finanziarie interessate dei rischi individuati in tali raccomandazioni, l'autorità di sorveglianza capofila dovrebbe monitorare e valutare l'attuazione, da parte del fornitore terzo critico di servizi TIC, delle azioni e dei rimedi per conformarsi alle raccomandazioni. Le autorità competenti dovrebbero monitorare e valutare in che misura le entità finanziarie sono esposte ai rischi individuati in tali raccomandazioni. Al fine di mantenere condizioni di parità nello svolgimento dei rispettivi compiti, in particolare quando i rischi individuati nelle raccomandazioni sono gravi e condivisi da un gran numero di entità finanziarie in più Stati membri, sia le autorità competenti che l'autorità di sorveglianza capofila dovrebbero condividere tra loro tutte le risultanze pertinenti necessarie per svolgere i rispettivi compiti. L'obiettivo della condivisione delle informazioni è garantire che il feedback dell'autorità di sorveglianza capofila al fornitore terzo critico di servizi TIC in relazione alle azioni e ai rimedi che quest'ultimo sta attuando tenga conto dell'impatto sui rischi delle entità finanziarie e che la valutazione effettuata dall'autorità di sorveglianza capofila informi le attività di vigilanza svolte dalle autorità competenti.

(8) Al fine di consentire una condivisione efficiente ed efficace delle informazioni, le autorità competenti dovrebbero valutare, nell'ambito delle rispettive attività di vigilanza, in che misura le entità finanziarie sottoposte alla loro vigilanza siano esposte ai rischi individuati nelle raccomandazioni. Tale valutazione dovrebbe essere effettuata in modo proporzionato e seguendo un approccio basato sul rischio. L'autorità di sorveglianza capofila dovrebbe chiedere alle autorità competenti di condividere i risultati di tale valutazione nei casi specifici in cui i rischi associati alle raccomandazioni sono gravi e comuni a un gran numero di entità finanziarie in diversi Stati membri. Al fine di utilizzare al meglio le risorse delle autorità competenti, l'autorità di sorveglianza capofila, quando chiede di fornire i risultati di tale valutazione, dovrebbe sempre tenere conto del fatto che l'obiettivo di tali richieste è valutare l'attuazione delle azioni e dei rimedi da parte dei fornitori terzi critici di servizi TIC.

(9) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([2]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 22 luglio 2024.

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

(11) Il comitato congiunto delle AEV ha condotto consultazioni pubbliche aperte sui progetti di norme tecniche di regolamentazione su cui si basa il presente regolamento, ne ha analizzato i potenziali costi e benefici e ha chiesto la consulenza del gruppo delle parti interessate nel settore bancario, istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio ([3]), del gruppo delle parti interessate nel settore dell'assicurazione e della riassicurazione e del gruppo delle parti interessate nel settore dei fondi pensionistici aziendali e professionali, istituiti ai sensi dell'articolo 37 del regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio ([4]), e del gruppo delle parti interessate nel settore degli strumenti finanziari e dei mercati, istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio ([5]),

([2]) 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).

([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).

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Informazioni che il fornitore terzo di servizi TIC deve fornire nella domanda di designazione quale fornitore critico

1. Nella domanda motivata di cui all'articolo 31, paragrafo 11, del regolamento (UE) 2022/2554 di designazione volontaria quale fornitore critico a norma dell'articolo 31, paragrafo 1, lettera a), del medesimo regolamento il fornitore terzo di servizi delle tecnologie dell'informazione e della comunicazione (TIC) fornisce le informazioni seguenti:

a) la denominazione della persona giuridica;

b) il codice identificativo della persona giuridica;

c) il nome del referente e le informazioni di contatto del fornitore terzo critico di servizi TIC;

d) il paese in cui la persona giuridica ha la propria sede sociale;

e) la descrizione della struttura aziendale comprendente almeno informazioni sull'impresa madre e su altre imprese collegate che forniscono servizi TIC a entità finanziarie dell'Unione. Tali informazioni comprendono, se del caso:

   i) la denominazione delle persone giuridiche;

   ii) il codice identificativo della persona giuridica;

   iii) il paese in cui la persona giuridica ha la propria sede sociale;

f) una stima della quota di mercato del fornitore terzo di servizi TIC nel settore finanziario dell'Unione e una stima della quota di mercato per tipo di entità finanziaria di cui all'articolo 2, paragrafo 1, del regolamento (UE) 2022/2554 per l'anno di presentazione della domanda di designazione quale fornitore critico e l'anno precedente la presentazione di tale domanda;

g) una descrizione di ciascun servizio TIC prestato alle entità finanziarie dell'Unione, comprendente:

   i) una descrizione della natura dell'attività e del tipo di servizi TIC prestati alle entità finanziarie;

   ii) un elenco delle funzioni delle entità finanziarie supportate dai servizi TIC prestati, se disponibile;

   iii) informazioni che indichino se i servizi TIC prestati alle entità finanziarie supportano funzioni essenziali o importanti, se disponibili;

h) un elenco delle entità finanziarie che ricorrono ai servizi TIC prestati dal fornitore terzo di servizi TIC, comprese le informazioni seguenti per ciascuna delle entità finanziarie che ricorrono ai servizi, se disponibili:

   i) la denominazione della persona giuridica;

   ii) il codice identificativo della persona giuridica, se noto al fornitore terzo di servizi TIC;

   iii) il tipo di entità finanziaria quale specificata all'articolo 2, paragrafo 1, del regolamento (UE) 2022/2554;

   iv) la località geografica dalla quale i servizi TIC sono prestati a tale persona giuridica specifica;

i) un elenco dei fornitori terzi critici di servizi TIC inclusi nel più recente elenco disponibile di tali fornitori pubblicato dalle AEV a norma dell'articolo 31, paragrafo 9, del regolamento (UE) 2022/2554 che dipendono dai servizi prestati dal richiedente, se disponibile;

j) un'autovalutazione per quanto riguarda:

   (i) il grado di sostituibilità di ciascun servizio TIC prestato dal richiedente, prendendo in considerazione gli aspetti seguenti:

      — la quota di mercato del fornitore terzo di servizi TIC nel settore finanziario dell'Unione;

— il numero di concorrenti pertinenti noti per tipo di servizi TIC o gruppo di servizi TIC;

— la descrizione delle specificità relative ai servizi TIC offerti, anche per quanto riguarda eventuali tecnologie proprietarie, o le caratteristiche specifiche dell'organizzazione o attività del fornitore terzo di servizi TIC;

(ii) il possesso di informazioni circa la disponibilità di fornitori terzi alternativi di fornire gli stessi servizi TIC prestati dal fornitore terzo di servizi TIC che presenta la domanda;

k) informazioni sulla futura strategia commerciale in relazione alla fornitura di servizi e infrastrutture TIC a entità finanziarie nell'Unione, compresi eventuali cambiamenti previsti nel gruppo o nella struttura gestionale, l'ingresso in nuovi mercati o attività;

l) l'identificazione dei subappaltatori del fornitore terzo di servizi TIC che sono stati designati quali fornitori terzi critici di servizi TIC;

m) qualsiasi altro motivo pertinente per la domanda di designazione del fornitore terzo di servizi TIC quale fornitore critico.

2. Laddove il fornitore terzo di servizi TIC appartenga a un gruppo, le informazioni di cui al paragrafo 1 sono fornite in relazione ai servizi TIC prestati dal gruppo nel suo insieme.

Articolo 2

Contenuto, struttura e formato delle informazioni da trasmettere, diffondere o segnalare da parte dei fornitori terzi critici di servizi TIC

1. I fornitori terzi critici di servizi TIC forniscono all'autorità di sorveglianza capofila, su richiesta di quest'ultima, tutte le informazioni necessarie all'autorità di sorveglianza capofila per adempiere i suoi compiti di sorveglianza conformemente ai requisiti del regolamento (UE) 2022/2554.

2. Tra le informazioni di cui al paragrafo 1 rientrano tra l'altro:

a) informazioni sugli accordi, e copie dei documenti contrattuali, tra:

i) il fornitore terzo critico di servizi TIC e le entità finanziarie di cui all'articolo 2, paragrafo 1, del regolamento (UE) 2022/2554;

ii) il fornitore terzo critico di servizi TIC e i suoi subappaltatori al fine di rispecchiare la catena del valore tecnologico dei servizi TIC prestati alle entità finanziarie nell'Unione;

b) informazioni sulla struttura organizzativa e di gruppo del fornitore terzo critico di servizi TIC, compresa l'identificazione di tutte le entità appartenenti al medesimo gruppo che prestano direttamente o indirettamente servizi TIC a entità finanziarie nell'Unione;

c) informazioni sui principali azionisti, compresa la loro struttura ed estensione geografica, di uno qualunque dei soggetti seguenti:

i) entità che detengono, da sole o congiuntamente con le loro entità collegate, il 25 % o più del capitale o dei diritti di voto del fornitore terzo critico di servizi TIC;

ii) entità che hanno il diritto di nominare o revocare la maggioranza dei membri dell'organo di amministrazione, direzione o vigilanza del fornitore terzo critico di servizi TIC;

iii) entità che controllano, in virtù di un accordo, la maggioranza dei diritti di voto degli azionisti o dei soci del fornitore terzo critico di servizi TIC;

d) informazioni sulla quota di mercato del fornitore terzo critico di servizi TIC per tipo di servizi, nei mercati rilevanti in cui opera;

e) informazioni sui meccanismi di governance interna del fornitore terzo critico di servizi TIC, compresa la struttura con linee di responsabilità di governance e norme in materia di responsabilità;

f) i verbali delle riunioni dell'organo di gestione e di altri comitati interni pertinenti del fornitore terzo critico di servizi TIC che riguardino in qualsiasi modo le attività e i rischi relativi ai servizi TIC di terzi volti a supportare le funzioni di entità finanziarie all'interno dell'Unione;

g) informazioni sulla sicurezza delle TIC del fornitore terzo critico di servizi TIC, in particolare le strategie, gli obiettivi, le politiche, le procedure, i protocolli, i processi, le misure di controllo pertinenti per proteggere i dati sensibili, i controlli sull'accesso, le pratiche di cifratura, i piani di risposta agli incidenti, nonché informazioni sul rispetto di tutta la normativa pertinente e delle norme nazionali e internazionali, se del caso;

h) informazioni sulle misure tecniche e organizzative volte a garantire la protezione e la riservatezza dei dati, compresi i dati personali e non personali, le misure di controllo attuate per proteggere i dati sensibili, i controlli sull'accesso, le pratiche di cifratura, il piano di risposta alle violazioni dei dati; l'elenco dei paesi e le leggi applicabili quando, in relazione al trattamento di dati personali, il fornitore terzo di servizi TIC è soggetto alla legislazione di paesi terzi, compresa la richiesta di accesso da parte del governo di paesi terzi;

i) informazioni sui meccanismi che il fornitore terzo critico di servizi TIC offre alle entità finanziarie dell'Unione per la portabilità dei dati, la portabilità e l'interoperabilità delle applicazioni;

j) informazioni sull'ubicazione dei centri dati e dei centri di produzione di TIC utilizzati per prestare servizi alle entità finanziarie, compreso un elenco di tutti i locali e strutture pertinenti del fornitore terzo critico di servizi TIC, anche al di fuori dell'Unione;

k) informazioni sulla fornitura di servizi da parte del fornitore terzo critico di servizi TIC di paesi terzi, comprese le informazioni sulle pertinenti disposizioni giuridiche applicabili ai dati personali e non personali trattati dal fornitore terzo di servizi TIC;

l) informazioni sulle misure adottate per affrontare i rischi derivanti dalla fornitura di servizi TIC da parte del fornitore terzo critico di servizi TIC e dei suoi subappaltatori di paesi terzi;

m) informazioni sul quadro di gestione dei rischi e sul quadro di gestione degli incidenti, comprese le politiche, le procedure, gli strumenti, i meccanismi e i meccanismi di governance del fornitore terzo critico di servizi TIC e dei suoi subappaltatori, tra cui l'elenco e la descrizione degli incidenti gravi che hanno un impatto diretto o indiretto sulle entità finanziarie all'interno dell'Unione, compresi i dettagli pertinenti per determinare la rilevanza dell'incidente per le entità finanziarie e valutare i possibili impatti transfrontalieri;

n) informazioni sul quadro di gestione delle modifiche, compresi le politiche, le procedure e i controlli del fornitore terzo critico di servizi TIC e dei suoi subappaltatori;

o) informazioni sul quadro generale di risposta e ripristino del fornitore terzo critico di servizi TIC, compresi i piani di continuità operativa con relative modalità e procedure, la politica del ciclo di vita di sviluppo del software, i piani di risposta e ripristino con relative modalità e procedure, le politiche di backup con relative modalità e procedure;

p) informazioni sul monitoraggio delle prestazioni, sul monitoraggio della sicurezza e sul tracciamento degli incidenti, nonché informazioni sui meccanismi di segnalazione relativi alle prestazioni del servizio, agli incidenti e al rispetto degli accordi sul livello dei servizi e degli obiettivi sul livello dei servizi concordati o di accordi analoghi tra fornitori terzi critici di servizi TIC ed entità finanziarie nell'Unione;

q) informazioni sul quadro di gestione dei rischi informatici derivanti da terzi del fornitore terzo critico di servizi TIC, comprese le strategie, le politiche, le procedure, i processi e i controlli, tra cui i dettagli sul dovere di diligenza e sulla valutazione dei rischi effettuata dal fornitore terzo critico di servizi TIC nei confronti dei suoi subappaltatori prima di concludere un accordo con questi ultimi, e per monitorare il rapporto tra tutti i pertinenti rischi di controparte e in materia di TIC;

r) estrazioni dai sistemi di monitoraggio e scansione del fornitore terzo critico di servizi TIC e dei suoi subappaltatori, riguardanti, tra l'altro, il monitoraggio della rete, il monitoraggio dei server, il monitoraggio delle applicazioni, il monitoraggio della sicurezza, la scansione delle vulnerabilità, la gestione dei log, il monitoraggio delle prestazioni, la gestione degli incidenti e le misurazioni rispetto agli obiettivi di affidabilità, quali gli obiettivi sul livello dei servizi;

s) estrazioni da qualsiasi sistema o applicazione di produzione, pre-produzione e test utilizzati dal fornitore terzo critico di servizi TIC e dai suoi subappaltatori per prestare direttamente o indirettamente servizi a entità finanziarie nell'Unione;

t) le relazioni di conformità e di audit disponibili, nonché tutte le risultanze di audit pertinenti, compresi gli audit effettuati dalle autorità nazionali nell'Unione e al di fuori dell'Unione, qualora gli accordi di cooperazione con le autorità competenti prevedano tale scambio di informazioni, oppure le certificazioni ottenute dal fornitore terzo critico di servizi TIC o dai suoi subappaltatori, comprese le relazioni di revisori interni ed esterni, le certificazioni o le valutazioni del rispetto delle norme di settore specifiche. Sono comprese le informazioni su qualsiasi tipo di test indipendente disponibile della resilienza dei sistemi TIC del fornitore terzo critico di servizi TIC, compreso qualsiasi tipo di test di penetrazione basato sulle minacce effettuato dal fornitore terzo di servizi TIC;

u) informazioni su eventuali valutazioni effettuate dal fornitore terzo critico di servizi TIC, su sua richiesta o per suo conto, per valutare l'idoneità e l'integrità delle persone che ricoprono posizioni chiave all'interno del fornitore terzo critico di servizi TIC;

v) informazioni su eventuali piani correttivi per dare seguito alle raccomandazioni a norma dell'articolo 3 e le relative informazioni pertinenti per confermare l'attuazione dei rimedi;

w) informazioni sui programmi di formazione dei dipendenti e sui programmi di sensibilizzazione alla sicurezza disponibili, comprese, se del caso, informazioni sugli investimenti, sulle risorse e sui metodi del fornitore terzo critico di servizi TIC per formare il proprio personale a gestire dati finanziari sensibili e a mantenere livelli elevati di sicurezza;

x) informazioni sulle attività del fornitore terzo critico di servizi TIC e sui bilanci d'esercizio, comprese le informazioni sulla dotazione finanziaria e sulle risorse connesse alle TIC e alla sicurezza.

Articolo 3

Informazioni che i fornitori terzi critici di servizi TIC devono fornire dopo la formulazione di raccomandazioni

1. Il fornitore terzo critico di servizi TIC presenta all'autorità di sorveglianza capofila una relazione contenente un piano correttivo in relazione alle raccomandazioni e ai rimedi che il fornitore terzo critico di servizi TIC intende attuare ai fini dell'attenuazione dei rischi individuati nelle raccomandazioni di cui all'articolo 35, paragrafo 1, lettera d), del regolamento (UE) 2022/2554. La relazione è coerente con il calendario fissato dall'autorità di sorveglianza capofila per ciascuna raccomandazione.

2. Al fine di consentire il monitoraggio dell'attuazione delle azioni adottate o dei rimedi applicati dal fornitore terzo critico di servizi TIC in relazione alle raccomandazioni ricevute, il fornitore terzo critico di servizi TIC condivide con l'autorità di sorveglianza capofila, su richiesta:

a) le relazioni intermedie sullo stato di avanzamento e i relativi documenti giustificativi che specifichino i progressi compiuti nell'attuazione delle azioni e delle misure indicate nella relazione trasmessa dal fornitore terzo critico di servizi TIC all'autorità di sorveglianza capofila entro il termine stabilito dall'autorità di sorveglianza capofila;

b) le relazioni finali e i relativi documenti giustificativi che specifichino le azioni adottate o i rimedi applicati dal fornitore terzo critico di servizi TIC ai fini dell'attenuazione dei rischi individuati nelle raccomandazioni ricevute.

Articolo 4

Struttura e formato delle informazioni trasmesse dai fornitori terzi critici di servizi TIC

1. Il fornitore terzo critico di servizi TIC trasmette le informazioni richieste all'autorità di sorveglianza capofila tramite gli appositi canali elettronici sicuri indicati nella richiesta dall'autorità di sorveglianza capofila e nella forma stabilita da quest'ultima.

2. All'atto della trasmissione delle informazioni all'autorità di sorveglianza capofila, i fornitori terzi critici di servizi TIC:

a) seguono la struttura indicata dall'autorità di sorveglianza capofila nella sua richiesta di informazioni;

b) indicano chiaramente l'informazione pertinente nella documentazione presentata.

3. Le informazioni trasmesse, diffuse o segnalate all'autorità di sorveglianza capofila da parte del fornitore terzo critico di servizi TIC sono redatte in una lingua comunemente utilizzata negli ambienti della finanza internazionale.

Articolo 5

Modello per la trasmissione di informazioni relative agli accordi di subappalto

Il fornitore terzo critico di servizi TIC che è tenuto a condividere informazioni relative agli accordi di subappalto trasmette le informazioni all'autorità di sorveglianza capofila conformemente al modello di cui all'allegato.

Articolo 6

Valutazione da parte delle autorità competenti dei rischi trattati nelle raccomandazioni dell'autorità di sorveglianza capofila

1. Nell'ambito della vigilanza sulle entità finanziarie, l'autorità competente valuta l'impatto su queste ultime delle misure adottate dal fornitore terzo critico di servizi TIC sulla base delle raccomandazioni dell'autorità di sorveglianza capofila conformemente al principio di proporzionalità.

2. Nell'effettuare la valutazione di cui al paragrafo 1, l'autorità competente tiene conto di tutti gli aspetti seguenti:

a) l'adeguatezza e la coerenza delle misure correttive e di riparazione attuate dalle entità finanziarie ai fini dell'attenuazione dei rischi individuati nelle raccomandazioni;

b) la valutazione effettuata dall'autorità di sorveglianza capofila del rispetto, da parte del fornitore terzo critico di servizi TIC, delle misure e delle azioni incluse nella relazione qualora abbia un impatto sull'esposizione delle entità finanziarie che rientrano nel suo ambito di competenza ai rischi individuati nelle raccomandazioni;

c) il parere di qualsiasi altra autorità competente che sia stata consultata conformemente all'articolo 42, paragrafo 5, del regolamento (UE) 2022/2554;

d) se l'autorità di sorveglianza capofila ha ritenuto che le azioni e i rimedi attuati dal fornitore terzo critico di servizi TIC erano adeguati per attenuare l'esposizione delle entità finanziarie che rientrano nel suo ambito di competenza ai rischi individuati nelle raccomandazioni.

3. Su richiesta dell'autorità di sorveglianza capofila, l'autorità competente fornisce in tempi ragionevoli i risultati della valutazione di cui al paragrafo 1. Nel richiedere i risultati di tale valutazione, l'autorità di sorveglianza capofila tiene conto del principio di proporzionalità e della dimensione dei rischi associati alle raccomandazioni, compresi gli impatti transfrontalieri di tali rischi quando incidono su entità finanziarie che operano in più di uno Stato membro.

4. Se del caso, l'autorità competente chiede alle entità finanziarie di fornire tutte le informazioni necessarie per effettuare la valutazione di cui al paragrafo 1.

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 24 ottobre 2024

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

MODELLO PER LA CONDIVISIONE DI INFORMAZIONI RELATIVE AGLI ACCORDI DI SUBAPPALTO

Categoria di informazioni	Elementi di informazione principali
Informazioni generali	— Nome del fornitore terzo critico di servizi TIC. — Codice identificativo del fornitore terzo critico di servizi TIC. — Il nome del referente e le informazioni di contatto del fornitore terzo critico di servizi TIC. — Data di presentazione del modello.
Panoramica degli accordi di subappalto	— Mappatura degli accordi di subappalto, compresa una breve descrizione della finalità e della portata dei rapporti di subappalto (tra cui un'indicazione del livello di criticità o di importanza degli accordi di subappalto per il fornitore terzo critico di servizi TIC). — Specificazione e descrizione dei tipi di servizi TIC subappaltati e della loro rilevanza per i servizi TIC prestati alle entità finanziarie, in linea con le norme tecniche di attuazione adottate ai sensi dell'articolo 28, paragrafo 9, del regolamento (UE) 2022/2554. — Nello specificare i tipi di servizi TIC, fare riferimento all'elenco di cui all'allegato IV delle norme tecniche di attuazione adottate ai sensi dell'articolo 28, paragrafo 9, del regolamento (UE) 2022/2554.
Informazioni sui subappaltatori	— Denominazione e dati della persona giuridica (compreso il codice identificativo) di ciascun subappaltatore. — Recapiti dei membri del personale responsabili di ciascuno dei rapporti di subappalto in seno alla struttura di gestione del fornitore terzo critico di servizi TIC. — Panoramica, per ciascun subappaltatore, delle competenze, dell'esperienza e delle qualifiche relative ai servizi TIC appaltati.
Descrizione dei servizi prestati dai subappaltatori	— Descrizione dettagliata dei servizi TIC specifici prestati da ciascun subappaltatore. — Ripartizione delle responsabilità e dei compiti assegnati ai subappaltatori, specificando i diversi ruoli nelle diverse fasi dei processi TIC. — Informazioni sul livello di accesso da parte dei subappaltatori a dati personali o altrimenti sensibili o sistemi relativi ai servizi TIC prestati alle entità finanziarie. — Informazioni sui siti da cui vengono prestati i servizi dei subappaltatori e sulle misure adottate per affrontare i rischi derivanti dai servizi prestati al di fuori dell'Unione.
Governance e sorveglianza dei subappalti	— Descrizione del quadro contrattuale e di governance in atto per gestire i rapporti di subappalto, comprese le clausole che limitano l'uso di dati sensibili. — Spiegazione dei processi di selezione, assunzione e monitoraggio dei subappaltatori. — Panoramica delle metriche di prestazione, degli obiettivi e degli accordi sul livello dei servizi e degli indicatori chiave di prestazione utilizzati per valutare le prestazioni e il monitoraggio dell'affidabilità del subappaltatore.
Gestione dei rischi e conformità	— Valutazione dei profili di rischio del subappaltatore e del potenziale impatto sui servizi TIC prestati alle entità finanziarie. — Spiegazione delle misure di attenuazione dei rischi attuate per far fronte ai rischi connessi al subappalto. — Informazioni dettagliate sul rispetto, da parte del subappaltatore, della normativa pertinente, anche per quanto riguarda la protezione dei dati e le norme di settore.

Categoria di informazioni	Elementi di informazione principali
Continuità operativa e pianificazione di emergenza	— Panoramica della continuità operativa e dei piani di risposta e ripristino del subappaltatore. — Descrizione dei meccanismi in essere per garantire la continuità del servizio in caso di perturbazioni o di risoluzione da parte del subappaltatore. — Frequenza dei test dei piani di continuità operativa e dei piani di risposta e ripristino da parte dei subappaltatori, date dei test più recenti effettuati negli ultimi tre anni e indicazione dell'eventuale coinvolgimento del fornitore terzo critico di servizi TIC in tali test.
Segnalazione	— Descrizione dei meccanismi di segnalazione e frequenza delle segnalazioni tra il fornitore terzo critico di servizi TIC e i suoi subappaltatori.
Adozione di rimedi e gestione degli incidenti	— Descrizione delle procedure per affrontare gli incidenti, le violazioni o l'inosservanza connessi ai subappaltatori.
Certificazioni e audit	— Informazioni su eventuali certificazioni, audit o valutazioni indipendenti condotti sui subappaltatori per convalidarne i controlli di sicurezza, le norme di qualità o la conformità alla normativa. — Data e frequenza degli audit sui subappaltatori condotti dal fornitore terzo critico di servizi TIC.