Giovedì 17 luglio 2025

Documento utilizzabile per commenti e feedback

Linee Guida

dell’8 luglio 2025 sulla solida gestione dei rischi di terze parti

Fine consultazione: 8 ottobre 2025

1.1.1

1.1.2 Domanda n.1 sul Capitolo 4.0 Linee guida per una sana gestione del rischio di terzi p.16

Partners4Innovation S.r.l.
Soggetta a direzione e controllo da parte di Digital360 S.p.A.
Viale L. Bodio, 37 20158 Milano
C.F. e P.IVA: 04841830963

Linee guida per una sana gestione del rischio di terzi (pg. 16)		
#	Titolo del macro-paragrafo	Sottoparagrafi
1.0	Conformità e obblighi di segnalazione	- Stato delle linee Guida (par.1-2) - Obblighi di segnalazione (par.3-4)
2.0	Oggetto, ambito di applicazione e definizioni	- Oggetto materia (par. 5-6-7) - Destinatari (par. 8-9-10-11) - Ambito di applicazione (par. 12-13-14) - Definizioni (par. 15-16)
3.0	Attuazione	- Data di applicazione (par.17-18) - Disposizioni transitorie (par. 20) - Abrogazione (par. 21)
Quesito n.1	L'oggetto, l'ambito di applicazione, le definizioni e le disposizioni transitorie sono adeguati e sufficientemente chiari?	
Risposta	*Par. 7 "Oggetto materia"* **Punti di attenzione**: - Che cosa si intende quando ci si riferisce ad un servizio non ICT?- - Come deve essere gestito un servizio non ICT se viene erogato tramite un servizio ICT quale componente del sevizio principale? - se la funzione non ICT viene erogata da un altro ente finanziario quali sono le conseguenze? - ai servizi ICT (anche se comprendono l'erogazione di una funzione) si applica solo ed esclusivamente il Regolamento Dora? *Par. 14 "Ambito di applicazione"* **wording non chiaro**: utilizzare lo stesso wording dell'orientamento 12 con riferimento a base consolidata invece di base di gruppo *Par. 16 "Definizioni"* **Punto di attenzione:** **- Accordi con terzi**: si distingue la categoria degli accordi con terzi, che hanno ad oggetto la fornitura di una funzione, con il sotto insieme degli accordi di esternalizzazione/ outsourcing di una funzione erogata su base periodica o continuativa (vedi definizione di accordi di outsourcing). È opportuno chiarire se la categoria "accordo con terzi" comprenda tutti i servizi anche quelli non connotati da continuità. Se così fosse, si avrebbe una categoria più ampia di quella considerata nel perimetro Dora, che comprenderebbe qualsiasi servizio erogato da terzi	

	wording non chiaro: Per la definizione di funzione "critica" o importante si suggerisce di riprendere la traduzione originale di **Funzione Essenziale o Importante** *Par. 17 "Data di applicazione"* **Punto di attenzione:** ci si riferisce a tutti gli accordi con terzi? *Par. 18 "Data di applicazione"* **Punto di attenzione:** ci si riferisce a tutti gli accordi con terzi? *Par. 19 "Data di applicazione"* **Punto di attenzione:** ci si riferisce a tutti gli accordi con terzi relativi a funzioni essenziali o importanti? ▪ contiene una chiara motivazione ▪ fornisce prove a sostegno delle opinioni espresse/delle motivazioni proposte;]
	[▪ descrizione di eventuali scelte normative alternative che l'EBA dovrebbe prendere in considerazione.]

1.1.3 Domande n.2-3-4-5 del Capitolo 4.1 (pg.24) inerenti il Titolo II, il Titolo III, il Titolo IV e l'Allegato I

Capitolo 4 - Linee Guida Sulla Corretta Gestione Del Rischio Di Terzi (Pg.24)		
#	**Titolo del macro-paragrafo**	**Sottoparagrafi**
1.1	Titolo I - Proporzionalità: applicazione di gruppo e schemi di protezione istituzionali	1. Proporzionalità (par. 22-23-24) 2. Gestione dei rischi di terzi da parte di entità finanziarie all'interno di gruppi e istituti aderenti a un sistema di tutela istituzionale (par. 25-26-27-28-29)
[…]	[…]	
Risposta/commento	*Par. 25 "Gestione dei rischi di terze parti da parte di entità finanziarie all'interno di gruppi e istituti aderenti a un sistema di tutela internazionale"* **Wording non chiaro**: l'impresa madre nell'UE o l'impresa madre in uno Stato membro (linguaggio poco chiaro, da riscrivere coerentemente) ▪ contiene una chiara motivazione ▪ fornisce prove a sostegno delle opinioni espresse/delle motivazioni proposte;]	
	[▪ descrizione di eventuali scelte normative alternative che l'EBA dovrebbe prendere in considerazione.]	
2.1	Titolo II – Valutazione degli accordi con terzi	3. Sana gestione dei rischi di terzi (par.30-31-32) 4. Funzioni critiche o importanti (par.33- 34-35-36-37)
Quesito n.2	Il Titolo II è appropriato e sufficientemente chiaro?	

Risposta/commento	*Par. 30 "Solida gestione dei rischi di terzi"* **Punto di attenzione** Rispetto a questi requisiti è opportuno chiarire in modo definito il perimetro di applicazione degli Orientamenti, che riguarda: - tutti gli accordi con terzi relativi all'erogazione di funzioni (anche non continuative); - tutti gli accordi di outsourcing relativi all'erogazzione di funzione su base periodica o continuativa. **È inoltre opportuno chiarire se gli accordi terzi possono riguardare anche funzioni essenziali o importanti** È interessante la precisazione che **sono esclusi i semplici acquisti di beni** **È opportuno che sia confermato se ai servizi ICT anche se comprendono l'erogazione di una funzione si applica solo il Regolamento Dora e qual è il confine tra i due perimetri** *Par. 33 "Funzioni critiche o importanti"* L'orientamento 33 potrebbe essere condensato con l'orientamento 37? Di fatto si tratta di due orientamenti che descrivono gli effetti dell'impatto. *Par. 34 "Funzioni critiche o importanti"* **Punto di attenzione:** tra le funzioni di controllo, c'è anche ICT RISK che potrebbe delegare compiti operativi in ambito ICT Consulting (S15 All.to Regolamento Delegato 2024/2956). Sarebbe opportuno prevedere una espressa specificazione di esclusione, per evitare una sovrapposizione *Par. 36 "Funzioni critiche o importanti"* **Punto di attenzione**: a fini di coerenza sarebbe opportuno chiarire che cosa si intende per "**linee di business principali oggetto degli accordi con terzi**" e qual è la differenza, se esiste, rispetto alle funzioni critiche o importanti. In caso di differenza rispetto a quest'ultima categoria sarebbe opportuno chiarire quali sono i criteri di individuazione degli stessi *Par. 37 "Funzioni critiche o importanti"* **Punto di attenzione:** Vedi ipotesi di unificazione con l'Orientamento 33 Inoltre, specificare che tale strategia è separata dalla strategia dei rischi ICT e Cyber (da valutare in coerenza con orientamento 50) prevista dal Regolamento Dora ▪ contiene una chiara motivazione ▪ fornisce prove a sostegno delle opinioni espresse/delle motivazioni proposte;]	
	[▪ descrizione di eventuali scelte normative alternative che l'EBA dovrebbe prendere in considerazione.]	
3.1	Titolo III – Governance quadro di riferimento	5. Disposizioni di governance solide e rischio di terzi 6. Politiche di gestione del rischio di terzi 7. Conflitto di interessi 8. Piani di continuità operativa 9. Funzione di revisione interna 10. Documentazione requisiti
Quesito n.3	Le sezioni da 5 a 10 (Titolo III) delle Linee guida sono sufficientemente chiare e appropriate?	

Risposta/commento	*Par. 39 "Disposizioni di governance solide e rischio di terzi"* **Punto di attenzione:** Il riferimento al quadro di gestione dei rischi informatici e delle tecnologie dell'informazione e della comunicazione (ICT), conformemente al regolamento (UE) 2022/2554 (DORA), potrebbe generare sovrapposizioni con gli obblighi derivati da tale normativa. Sembra che debba essere definito un processo unitario di gestione di tutti i rischi derivanti da terzi (Accordi con terzi, esternalizzazioni/ousourcing e ICT). **Interpretazione da confermare** *Par. 41 " Disposizioni di governance solide e rischio di terzi"* Punto di attenzione: valutare se l'orietamento non risulti ridondante, rispetto al fatto che l'obbligo deriva già dal GDPR ▪ contiene una chiara motivazione ▪ fornisce prove a sostegno delle opinioni espresse/delle motivazioni proposte;]	
	[▪ descrizione di eventuali scelte normative alternative che l'EBA dovrebbe prendere in considerazione.]	
4.1	Titolo IV – Processo di accordo con terzi	11. Analisi precontrattuale 11.1. Condizioni di vigilanza per la stipula dei contratti con terzi di servizi 11.2. Valutazione del rischio degli accordi con terzi 11.3. Due Diligence 12. Fase contrattuale 13. Monitoraggio 14. Strategie d'uscita
Quesito n.4	Il Titolo IV delle Linee guida è appropriato e sufficientemente chiaro?	
Risposta/commento	[▪ indicazione del punto specifico a cui si riferisce il commento; ▪ contiene una chiara motivazione ▪ fornisce prove a sostegno delle opinioni espresse/delle motivazioni proposte;]	
	[▪ descrizione di eventuali scelte normative alternative che l'EBA dovrebbe prendere in considerazione.]	
5.1	Titolo V - Linee guida sulle disposizioni relative ai rischi di terzi indirizzate alle autorità competenti	- Paragrafo 120 a 131 - Allegato I *Elenco non esaustivo delle funzioni che potrebbero essere fornite da un fornitore di servizi terzo*
Quesito n.5	L'Allegato I, fornito, come elenco di esempi non esaustivi, sufficientemente appropriato e chiaro?	
Risposta/commento	[▪ indicazione del punto specifico a cui si riferisce il commento; ▪ contiene una chiara motivazione ▪ fornisce prove a sostegno delle opinioni espresse/delle motivazioni proposte;]	
	[▪ descrizione di eventuali scelte normative alternative che l'EBA dovrebbe prendere in considerazione.]	

Le indicazioni tra parentesi quadra sono delle specificazioni fornite dalle Esas per rendere i commenti/feedback utili per la consultazione. Inoltre, i quesiti in blu chiaro non sono tassativi, in quanto possono essere presentati nuovi quesiti secondo la modalità indicata nel documento dell'8 luglio 2025, ovvero "invia i tuoi commenti" nell'apposita pagina di consultazione.

FAGGIOLI GABRIELE MARIA
2025.10.08 19:31:22
CN=FAGGIOLI GABRIELE MARIA
C=IT
2.5.4.4=FAGGIOLI
2.5.4.42=GABRIELE MARIA
RSA/2048 bits