

ATTUALITÀ

Le nuove Linee Guida EBA sul rischio di fornitori terzi di servizi

22 Settembre 2025

Donato Varani, Partner, Annunziata&Conso

Luciano Murtas, Senior manager, RbyC

Antonio Viviano, Consultant, RbyC

Daniele Dinicolamaria, Junior Consultant, RbyC



Donato Varani, Partner, Annunziata & Conso

Luciano Murtas, Senior manager, RbyC

Antonio Viviano, Consultant, RbyC

Daniele Dinicolamaria, Junior Consultant, RbyC

> Donato Varani

Donato Varani è Dottore Commercialista e Revisore legale dei conti dal 1993. Vanta una ultra ventennale esperienza nell'ambito della vigilanza bancaria e finanziaria maturata in Banca d'Italia e quale responsabile di funzioni di controllo in banche anche quotate. Dal 2008, consulente di intermediari bancari e finanziari, nel 2016 diviene partner del network Annunziata&Conso. Specializzato nella consulenza in materia organizzativa e dei sistemi di controllo interno, è un punto di riferimento nell'ambito delle materie di vigilanza prudenziale, regolamentare e antiriciclaggio degli intermediari bancari e finanziari. Tra le sue specializzazioni figurano altresì le materie relative alla Responsabilità amministrativa degli Enti e delle Persone Giuridiche.

Sommario: 1. Premessa; 2. Le principali novità delle LG TPSP; 2.1 L'estensione dell'ambito di applicazione soggettivo; 2.2 L'estensione dell'ambito di applicazione oggettivo; 2.3 I contratti con terze parti che rientrano nell'ambito di applicazione delle LG TPSP; 2.4 La tenuta dei registri dei fornitori; 3. Conclusioni

1. Premessa

Lo scorso 8 luglio 2025 l'Autorità Bancaria Europea ("**EBA**") ha avviato una consultazione pubblica per l'ema nazione di "Linee guida per la corretta gestione del rischio di terze parti" (di seguito, per brevità, le "**LG TPSP**"). La consultazione pubblica si concluderà l'8 ottobre 2025.

Si tratta, più precisamente, dell'aggiornamento delle Linee Guida EBA sull'outsourcing emanate nel 2019 (EBA/GL/2019/02, di seguito, per brevità, "**LG 2019**") con la finalità di:

- estenderne l'ambito di applicazione soggettivo e oggettivo;
- assicurare l'armonizzazione della disciplina della gestione del rischio di terze parti per la fornitura di servizi diversi dalle tecnologie di informazione e comunicazione (di seguito: "servizi "non-ICT") rispetto a quella dei fornitori di servizi ICT contenuta nel Regolamento UE 2022/2554 ("**DORA**") per non pregiudicare il *level playing field*, tenendo anche conto di altre normative nel frattempo emanate (quali MICAR, ESG).

In relazione a ciò, il presente contributo intende sintetizzare le principali novità e gli elementi di attenzione contenuti nel documento in consultazione, al fine di fornire agli operatori uno strumento utile per valutare gli impatti operativi della nuova disciplina.

¹ Linee Guida in materia di *Third Party Service Providers*

2. Le principali novità delle LG TPSP

2.1 L'estensione dell'ambito di applicazione soggettivo

Uno tra gli strumenti a disposizione dell'EBA per conseguire la più ampia armonizzazione delle discipline applicabili a diverse tipologie di intermediari vigilati consiste nell'allargamento del novero dei destinatari delle Linee Guida.

Rispetto alle LG 2019 - che erano indirizzate soltanto a enti creditizi e imprese di investimento soggette alla Direttiva 2013/36/UE (CRD), agli istituti di pagamento (IP) e agli istituti di moneta elettronica (IMEL) - le LG TPSP sono destinate anche:

- alle imprese di investimento che non possiedono i requisiti per essere classificate come piccole e non interconnesse ai sensi dell'art. 12, par. 1, del Regolamento UE 2019/2033 (IFR);
- agli emittenti di *asset-referenced tokens* (ARTs) soggetti al Regolamento UE 2023/1114 (MICAR);
- ai creditori come definiti dall'art. 4, par. 2 della Direttiva 2014/17/UE - Mortgage Credit Directive (MCD) -, quando essi sono istituti finanziari.

Poiché, come accennato in premessa, una delle finalità della revisione delle LG 2019 consiste nell'armonizzazione con la normativa DORA, è di immediata evidenza come, sotto il profilo in esame, il conseguimento dell'obiettivo appaia ancora lontano.

La platea dei soggetti destinatari di DORA (collettivamente definiti come "entità finanziarie") è infatti significativamente più ampia dal momento che - fatte salve le esenzioni espressamente previste - comprende anche:

- i prestatori di servizi di informazioni sui conti;
- le imprese di investimento senza distinzioni;
- i fornitori di servizi per le cripto-attività senza distinzioni;

- i depositari centrali di titoli;
- le controparti centrali;
- le sedi di negoziazione;
- i repertori di dati sulle negoziazioni;
- i gestori di fondi di investimento alternativi;
- le società di gestione;
- i fornitori di servizi di comunicazione dati;
- le imprese di assicurazione e riassicurazione;
- gli intermediari assicurativi e riassicurativi;
- gli enti pensionistici;
- le agenzie di rating del credito;
- gli amministratori di indici di riferimento critici;
- i fornitori di servizi di crowdfunding;
- i repertori di dati sulle cartolarizzazioni;
- i fornitori terzi di servizi ITC.

È ben vero che l'EBA non ha competenza diretta su buona parte dei soggetti appena indicati; sarebbe tuttavia auspicabile che almeno per i soggetti finanziari sottoposti a forme di vigilanza prudenziale nei settori creditizio, dei servizi di investimento e assicurativo, i provvedimenti di *soft law* che trattano argomenti di carattere trasversale che dovrebbero opportunamente essere disciplinati per tutti allo stesso modo fossero adottati in modo coordinato dalle rispettive autorità europee di supervisione

(ESAs) e non lasciati alle iniziative delle singole autorità di settore, pena l'inevitabile frammentazione del quadro normativo di riferimento che invece si vorrebbe evitare.

Ciò, in particolare, alla luce dell'impatto che darà determinato dall'estensione dell'ambito di applicazione oggettivo, come meglio evidenziato nel paragrafo successivo.

2.2 L'estensione dell'ambito di applicazione oggettivo

Le LG TPSP introducono una definizione molto ampia di "accordo con terze parti".

Questo, infatti, è individuato in **qualsunque accordo** – compresi quelli infragruppo – tra un'entità finanziaria e un terzo **per la fornitura di una o più funzioni**.

La "**funzione**", in base alle definizioni medesime, è da intendersi come "**qualsunque processo, servizio o attività o parte di essi**".

È espressamente chiarito nella definizione che l'esternalizzazione (che, come noto, individuava ed esauriva l'ambito di applicazione delle LG 2019) rappresenta solo un sottoinsieme dell'accordo con terze parti rilevante per le LG TPSP.

Ne deriva un significativo allargamento dell'ambito di applicazione oggettivo. Sebbene permangano le esclusioni già previste nelle LG 2019 (quali gli accordi per il mero acquisto di beni, le funzioni che obbligatoriamente devono essere svolte da terzi come ad esempio la revisione legale, l'utilizzo di infrastrutture globali come ad esempio Visa, Mastercard, l'acquisizione di pareri di professionisti che non hanno impatto effettivo sui rischi connessi all'attività finanziaria autorizzata ecc.) è di tutta evidenza che l'inclusione nell'ambito di applicazione di funzioni fornite da terzi ma estranee al concetto di esternalizzazione in senso stretto (intesa come attività che, se non affidata a un terzo, sarebbe svolta direttamente dall'intermediario finanziario in quanto rientrante nei limiti delle attività ad esso consentite) possa determinare l'attrazione nel perimetro delle nuove disposizioni di un novero di attività davvero ampio. La stessa distinzione tra "funzioni essenziali o importanti" e funzioni che non hanno tale caratteristica, fondamentale ai fini dell'applicazione di un quadro disciplinare più o meno stringente, è ora da riferire ai servizi non-ICT in generale.

Non potendo individuare analiticamente tutte le attività che possono concretamente rientrare nell'ambito di applicazione, l'approccio adottato dall'EBA prevede:

- **la responsabilizzazione degli stessi soggetti obbligati** ai quali è demandato il compito di svolgere una valutazione preliminare, tenendo anche conto del principio di proporzionalità, per individuare e classificare le attività affidate ai terzi che rientrano effettivamente nell'ambito di applicazione delle LG TPSP;
- l'elaborazione di un elenco di attività (contenuto nell'**Allegato 1 al documento di consultazione**) quale contributo all'attività di autovalutazione al fine di salvaguardare un certo grado di uniformità. L'EBA, tuttavia, chiarisce che tale elenco è da intendersi come indicativo e non vincolante, incoraggiando i soggetti obbligati ad adattare l'individuazione e classificazione delle attività alle proprie specifiche caratteristiche operative.

In sede di primo commento, in attesa di analizzare il testo definitivo delle LG TPSP, non ci si può esimere dal manifestare qualche perplessità sull'approccio adottato.

Considerato infatti, come si è detto, che l'allargamento dell'ambito di applicazione al di fuori dell'esternalizzazione in senso stretto può determinare l'applicazione degli adempimenti a un numero potenzialmente molto ampio di attività, lasciare alle scelte dei singoli intermediari l'individuazione e classificazione delle attività alle quali in concreto gli adempimenti saranno applicati rischia di generare comportamenti disomogenei e di compromettere il raggiungimento delle finalità perseguite.

In primis, il *level playing field* appare difficilmente conseguibile in assenza di limiti oggettivi fissati dall'Autorità di vigilanza ai confini dell'ambito di applicazione della disciplina. Al riguardo, si osserva che anche il citato Allegato contenente indicazioni non vincolanti per l'individuazione e la classificazione delle attività da attrarre nell'ambito di applicazione delle LG TPSP alimenta qualche interrogativo nella parte in cui elenca attività ("*Depositary tasks & administration for UCIs*") che sono riservate ai gestori di fondi comuni di investimento, soggetti che, come detto, non rientrano nella competenza dell'EBA. Ciò, per inciso, conferma la già rilevata opportunità di interventi coordinati delle ESAs per indirizzare al sistema disposizioni uniformi che assicurino omogeneità di comportamenti in aree di operatività trasversali, non connesse a specificità delle diverse attività riservate in concreto esercitate.

In secondo luogo, la valenza delle informazioni che dovranno essere rese alle autorità di vigilanza nazionali per monitorare, soprattutto, il rischio di concentrazione di determinate attività significative in capo a un numero limitato di fornitori e prevenire effetti sistemici indesiderati, potrebbe essere affievolita da interpretazioni individuali non coerenti. La moltiplicazione delle informazioni da inserire nei registri dedicati (inizialmente limitati alle esternalizzazioni in senso stretto e con DORA già estesi alle forniture di servizi ICT) dai quali le Autorità di Vigilanza attingeranno gli indicatori utili per le analisi di competenza sui rischi sistemici potrebbe, in un contesto di eccessiva discrezionalità lasciata ai soggetti obbligati, portare all'accumulazione di dati superflui o, all'opposto, alla mancata rilevazione di dati essenziali, con conseguenze non desiderabili da un lato sull'efficienza e dall'altro sull'efficacia dell'azione di supervisione.

Un ulteriore spunto di riflessione è poi dato dalla circostanza che nel documento in consultazione è stato eliminato ogni riferimento ai "servizi cloud"; nelle LG 2019 erano presenti alcune definizioni anche se l'argomento non era poi stato disciplinato; esso era stato oggetto specifico degli Orientamenti in materia di esternalizzazione a fornitori di servizi cloud emanate dall'ESMA nel 2020 (ESMA50-157-2403). Sebbene esuli dai limiti del presente lavoro, pare interessante notare che in virtù della dichiarata intenzione di lasciare a DORA tutto ciò che riguarda i fornitori di servizi ICT, anche il tema della fornitura di servizi cloud confluisce in tale disciplina. Non a caso, l'ESMA è intervenuta nel luglio 2025 aggiornando i citati orientamenti con il Final Report ESMA65-294529287-2639. Per effetto delle modifiche apportate, le linee guida ESMA del 2020 continueranno ad applicarsi soltanto a soggetti esclusi dall'applicazione di DORA, e segnatamente ai depositari di fondi di investimento alternativi e ai depositari di UCITS, laddove non già rientranti tra i destinatari delle disposizioni DORA.

2.3 I contratti con terze parti che rientrano nell'ambito di applicazione delle LG TPSP

Il principale elemento di novità, a tale riguardo, è rappresentato dall'ampliamento del novero delle tipologie di contratto interessate dalle disposizioni contenute all'interno delle LG TPSP, conseguenza diretta dell'estensione dell'ambito di applicazione oggettivo commentato nel paragrafo precedente.

Se, infatti, le LG 2019 facevano espresso riferimento ai soli **contratti di esternalizzazione**, le LG TPSP in consultazione prevedono esplicite disposizioni relative a **tutti i contratti perfezionati con fornitori**

terzi di servizi.

Ne deriva che gli enti destinatari delle nuove Linee Guida saranno chiamati a rispettare, per ogni fornitore terzo, lo stesso processo di *due diligence*, lo stesso contenuto contrattuale minimo e le stesse modalità di monitoraggio della prestazione del fornitore finora prescritti soltanto per i contratti di esternalizzazione in senso stretto.

Anche l'individuazione delle funzioni essenziali o importanti – con conseguente applicazione del quadro disciplinare più rigoroso richiesto dagli Orientamenti – riguarderà tutti gli accordi con terze parti.

Tale impostazione, se confermata all'esito della consultazione, potrebbe comportare impatti significativi sulle procedure organizzative e sui processi decisionali dei soggetti destinatari, introducendo altresì un approccio del tutto nuovo per categorie di fornitori per le quali certi protocolli tipici degli intermediari finanziari vigilati non sono abituali (si pensi all'obbligo del TPSP di cooperare pienamente con le autorità competenti, di sottostare a rigorosi livelli di servizio, di accettare maggiori poteri del committente di risolvere anticipatamente il contratto per ragioni connesse a esigenze di vigilanza prudenziale).

Le LG TPSP prevedono quale meccanismo di bilanciamento degli interessi in gioco – oltre che il principio di proporzionalità che generalmente connota i provvedimenti di *soft law* – anche, come si è accennato, l'enfaticizzazione della responsabilità dei soggetti destinatari ai quali è demandato il compito di individuare in concreto gli accordi con terze parti ai quali gli orientamenti si applicheranno.

Questa strada rischia di lasciare spazio eccessivo a scelte discrezionali che, se da un lato consentono la mitigazione dei divisati impatti organizzativi (potenzialmente dirompenti se applicati in misura lineare) dall'altro però potrebbero vanificare uno dei principali obiettivi perseguiti, cioè quel livellamento del campo di gioco più difficile da conseguire in presenza di valutazioni fortemente disomogenee da parte dei destinatari anche nei confronti di funzioni o fornitori identici.

2.4 La tenuta dei registri dei fornitori

Come detto, tutti i servizi ICT forniti dai TPSP agli enti finanziari rientrano nell'ambito di applicazione del Regolamento DORA, il quale ha previsto l'istituzione del Registro delle Informazioni ("ROI").

Allo stesso tempo, le LG TPSP rappresentano il quadro normativo di riferimento per tutti i servizi non-ICT forniti dai TPSP.

In ragione di ciò, le LG TPSP hanno l'obiettivo di garantire uno stretto allineamento tra i due quadri normativi in materia di gestione del rischio di terze parti, al fine di garantire condizioni di parità e favorire la convergenza in materia di vigilanza.

Sul punto, uno degli elementi di maggiore rilievo è rappresentato dalle previsioni relative all'**istituzione di un registro** ("Registro TPSP") contenente informazioni relative a tutti gli accordi perfezionati con TPSP (non-ICT), distinguendo tra accordi per la fornitura di funzioni essenziali o importanti e altri accordi con terzi.

La struttura del registro dovrebbe essere coerente con il ROI, tenuto anche conto che le LG TPSP consentono di **optare per la tenuta di un registro unificato**.

Le LG TPSP descrivono il contenuto minimo delle informazioni che il registro dovrebbe contenere, specificando ulteriori elementi per gli accordi perfezionati con terzi di funzioni essenziali o importanti.

In particolare, il registro TPSP dovrà contenere almeno le seguenti informazioni:

- un numero di riferimento per ciascun accordo con terzi e il tipo di accordo contrattuale;
- data di inizio e, se del caso, la data del successivo rinnovo;
- data di scadenza, comprese cause di risoluzione o cessazione del rapporto contrattuale e/o termini di preavviso per il TPSP e l'intermediario;
- dove applicabile, gli enti finanziari che rientrano nell'ambito di applicazione del consolidamento prudenziale o del sistema di protezione istituzionale che si avvalgono del TPSP;

- una breve descrizione delle funzioni fornite dai TPSP;
- la categoria, e tutte le categorie corrispondenti al servizio fornito, assegnata dall'ente finanziario al TPSP, tenuto conto dell'allegato 1 alle Linee Guida TPSP;
- il nome del TPSP, un identificativo LEI, il numero di registrazione della Società, la sede legale e altri recapiti pertinenti;
- il paese o i paesi in cui la funzione viene svolta e vengono trattati i dati, compresa la loro conservazione;
- la valutazione circa la essenzialità o importanza del servizio fornito dal TPSP;
- la data dell'ultima valutazione circa l'essenzialità o importanza svolta sul TPSP;
- la spesa totale annuale e il costo stimato di ciascun TPSP diretto.

Sono previste ulteriori informazioni per i fornitori terzi di servizi di funzioni essenziali o importanti.

Ne consegue, tra l'altro, l'abrogazione del registro delle informazioni relative agli accordi di esternalizzazione di servizi cloud disciplinata dagli Orientamenti ESMA del 2020 (ad eccezione dei soggetti, sopra indicati, che dovranno continuare ad applicarli).

È auspicabile che, non appena definite le nuove Linee Guida e prima che esse diventino vincolanti, siano diffuse al sistema istruzioni tecniche per la compilazione del registro e per la trasmissione delle informazioni alle autorità allineate a quelle già introdotte per il ROI dal Regolamento di Esecuzione 2024/2956. Ciò, in particolare, a beneficio dei destinatari che non optassero per la tenuta di un registro unico.

3. Conclusioni

Le LG TPSP modificano significativamente le precedenti LG 2019 estendendone l'ambito di applicazione soggettivo ed oggettivo. In particolare, l'attenzione della Vigilanza non è più concentrata soltanto sull'esternalizzazione in senso stretto di funzioni aziendali, ma si allarga a qualunque accordo con terze parti per la fornitura di servizi non-ICT significativi.

In tal senso può dirsi raggiunto l'obiettivo di allineare la disciplina a quella di DORA relativa ai servizi ICT.

Restano tuttavia alcuni punti interrogativi concernenti:

- l'effettivo raggiungimento del *level playing field* per tutti gli intermediari vigilati del settore bancario, finanziario e assicurativo. I limiti alla competenza dell'EBA fanno sì che ampie categorie di intermediari di rilevanza anche sistemica (si pensi in particolare alle imprese di assicurazioni e alle società di gestione di fondi comuni di investimento, oltre a situazioni peculiari dell'ordinamento nazionale quali gli intermediari iscritti nell'elenco di cui all'art. 106 del Testo unico bancario) resteranno esclusi dalla loro applicazione fino all'adozione di specifici provvedimenti da parte delle autorità europee o nazionali competenti. A tale riguardo merita evidenziare l'opportunità che interventi normativi su aree trasversali comuni a tutti gli intermediari vigilati siano adottate a livello di ESAs e non lasciate a iniziative di autorità settoriali;
- l'omogeneità delle informazioni che saranno comunicate alle autorità di vigilanza e da queste utilizzate per valutazioni del rischio sistemico soprattutto in presenza di elevati indici di concentrazione dei TPSP. Su tale obiettivo pesa l'elevato grado di discrezionalità che le LG TPSP riconoscono ai soggetti obbligati nel determinare quali funzioni affidate a terzi saranno attratte nell'ambito di applicazione delle linee guida;
- i potenziali impatti sui processi organizzativi e decisionali dei soggetti obbligati derivanti dal significativo ampliamento dell'ambito di applicazione oggettivo delle linee guida.

Con riserva di ritornare sugli argomenti esposti una volta che le linee guida saranno emanate, è auspicabile che gli esiti della consultazione contribuiscano a superare almeno in parte le criticità evidenzia-

te in vista degli obiettivi posti dall'EBA.

DB non solo
diritto
bancario

A NEW DIGITAL EXPERIENCE

 **dirittobancario.it**

