

Outsourcing

Il punto sulle Linee Guida EBA

Milano, 19 gennaio 2021

Indice

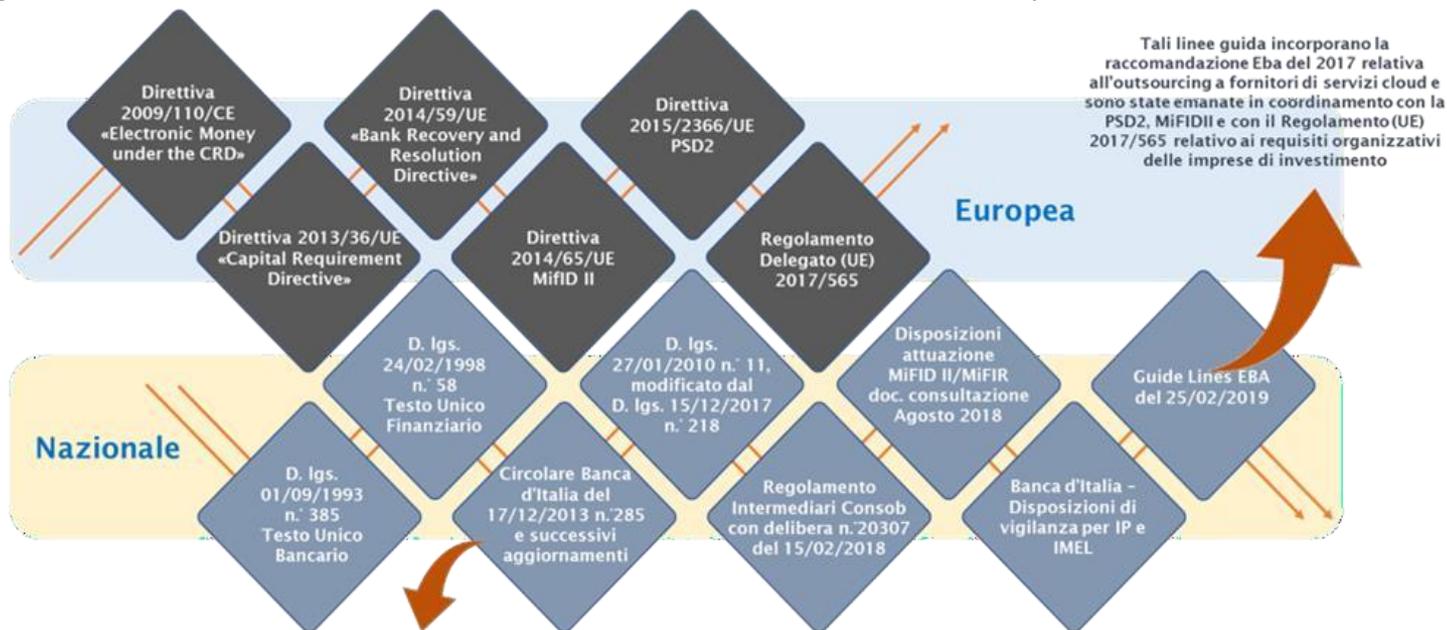
1. Il nuovo framework in materia di esternalizzazioni	3
2. I contenuti delle linee guida EBA in materia di Outsourcing	5
3. L'esternalizzazione delle funzioni aziendali ai sensi della Circ. 285 Bdl	42
4. L'esternalizzazione del sistema informativo ai sensi della Circ, 285 Bdl	45
5. La disciplina dell'esternalizzazione ai sensi della Mifid II	51
6. Il processo di esternalizzazione	88
7. Key contacts	92



Il nuovo framework in materia di esternalizzazioni

Il framework di riferimento

Negli ultimi anni gli enti regolatori nazionali ed europei sono intervenuti numerose volte su questa tema, sia in tutti gli aggiornamenti della Circolare 285/13 di Banca d'Italia fino all'emanazione più recente delle *Linee Guida (EBA/GL/2019/02)*:



«Disposizioni di vigilanza per le banche» che nell'ambito dell'obiettivo di dotare le stesse di un Sistema di Controlli Interni (SCI) completo, adeguato, funzionale e affidabile pone uno specifico focus relativamente al controllo delle esternalizzazioni di funzioni aziendali outsourcing

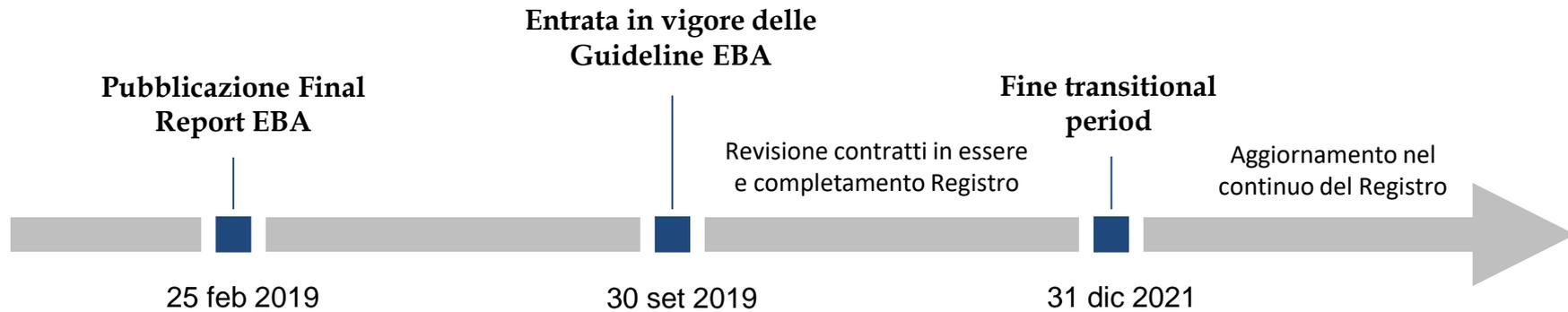
Il nuovo framework in materia di esternalizzazioni

Il framework di riferimento

La European Banking Authority (EBA), in data 25 febbraio 2019, ha pubblicato le Guidelines on Outsourcing arrangements, che aggiornano le esistenti linee guida CEBS sull'outsourcing, pubblicate nel 2006, e incorporano le disposizioni in tema di cloud outsourcing di dicembre 2017. Queste linee guida hanno l'obiettivo di istituire un quadro normativo più robusto relativamente agli accordi di outsourcing per tutti gli istituti rientranti nel perimetro di azione dell'EBA.

Le linee guida si applicheranno a tutti gli istituti, su base individuale e consolidata, a partire dal 30 settembre 2019. Gli istituti dovranno operare secondo un framework più robusto e:

- individuare una figura responsabile degli accordi di outsourcing o una soluzione organizzativa a presidio
- istituire un nuovo registro contenente le informazioni relative a tutti gli accordi di esternalizzazione in essere
- adeguare i nuovi contratti e ricontrattare quelli in essere, entro il 31 dicembre 2021



I contenuti delle linee guida EBA in materia di Outsourcing

Timing

OBIETTIVI

Garantire una maggiore **armonizzazione** degli accordi di esternalizzazione stipulati da tutte le istituzioni finanziarie soggette all'Autorità dell'EBA.

ABROGAZIONI

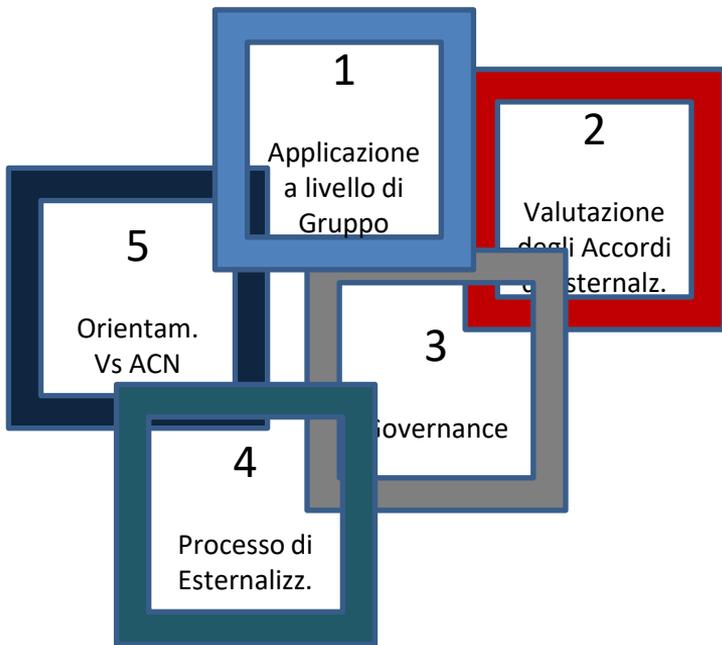
All'entrata in vigore delle linee guida, saranno abrogate le "Recommendations on cloud providers" emanate dall'EBA nel dicembre 2017

TEMPISTICHE

I destinatari delle Guidelines dovranno adeguarsi alle relative previsioni entro **il 30 settembre 2019**, mentre - con riferimento agli accordi di esternalizzazione già in essere - l'adeguamento è atteso alla prima data di rinnovo contrattuale (in ogni caso non oltre il **31 dicembre 2021**).

Le Linee Guida trovano applicazione nei confronti di tutte le istituzioni finanziarie soggette all'autorità dell'EBA, in particolare banche, imprese di investimento soggette alla CRD, istituti di pagamento e di moneta elettronica.

Principali ambiti di Intervento



La declinazione del **principio di proporzionalità** è richiamata dalle Linee Guida all'interno del Titolo I, nel quale assumono particolare rilievo taluni parametri, fra cui, a titolo esemplificativo e non esaustivo:

- (i) il profilo di rischio individuale;
- (ii) la natura e il modello di business dell'istituzione finanziaria;
- (iii) la dimensione e la complessità operativa dell'istituzione finanziaria;
- (iv) l'essenzialità o l'importanza della funzione esternalizzata e l'impatto potenziale dell'esternalizzazione sulla continuità delle loro attività

I contenuti delle linee guida EBA in materia di Outsourcing

Oggetto e Ambito di Applicazione

Le Linee Guida rivolgono una particolare attenzione all'ambito connesso ai sistemi e meccanismi di governance del processo di outsourcing, con particolare riferimento alla necessità – da parte dei destinatari – di garantire la conservazione delle capacità necessarie a mantenere un presidio di monitoraggio interno in merito alla funzione oggetto di esternalizzazione. Pertanto:

- ❑ richiedono di condurre una puntuale attività di identificazione, valutazione e gestione - da parte delle istituzioni finanziarie - dei rischi derivanti dalla stipula di accordi con parti terze, ai quali le stesse possono essere esposte;
- ❑ individuano elementi minimi delle Politiche aziendali in materia di esternalizzazione predisposte dai destinatari (e.g. una puntuale formalizzazione delle principali fasi del processo di outsourcing e di redazione dei relativi contratti);
- ❑ richiedono ai destinatari l'implementazione di strumenti e l'esecuzione di attività volte ad evitare potenziali conflitti di interesse, specie nell'ambito delle ipotesi di esternalizzazione infragruppo (e.g. le istituzioni devono verificare e assicurare che le condizioni contrattuali siano in linea con le condizioni di mercato);
- ❑ prevedono che i destinatari elaborino un Business Continuity Plan che tenga conto, tra gli altri, di possibili eventi che mettano a repentaglio l'adeguata gestione, da parte del provider, della funzione esternalizzata, testandone periodicamente la tenuta;
- ❑ sottolineano la rilevanza, altresì, della Funzione di Internal Audit, ai fini del presidio in merito al processo di outsourcing, fornendo specifiche indicazioni circa le attività che detta Funzione è tenuta a svolgere in relazione alle attività esternalizzate (e.g. analisi indipendente in ottica risk based sulle esternalizzazioni);
- ❑ prevedono l'implementazione di un Registro, nel quale catalogare e documentare tutti gli accordi di esternalizzazione stipulati dai destinatari.

I contenuti delle linee guida EBA in materia di Outsourcing

Are di Intervento

Gli istituti devono **mantenere un registro** (a livello individuale e di Gruppo) che documenti l'esistenza e le caratteristiche principali di tutti gli accordi di outsourcing, distinguendo tra l'outsourcing di funzioni critiche o importanti (CIF) e altri accordi di Outsourcing

Gli istituti devono identificare, valutare e gestire i **conflitti di interesse** con riferimento agli accordi di outsourcing
Nel momento in cui l'accordo di outsourcing, anche se stipulato all'interno dello stesso Gruppo, crea un conflitto di interesse rilevante, gli istituti devono **adottare misure appropriate** al fine di gestire tali conflitti

Gli istituti dovrebbero introdurre una **Funzione Outsourcing** o individuare un **senior staff member** direttamente responsabile nei confronti del management per il monitoraggio dei singoli accordi di outsourcing

Il senior management e l'Outsourcing Officer/senior staff member devono assicurare la **presenza di risorse sufficienti**, e disporre delle **adeguate competenze** per assicurare la conformità alle Guidelines EBA



Nell'**Audit Plan** deve essere inclusa la **revisione indipendente dell'efficacia del framework** di outsourcing, effettuata seguendo un **approccio risk based**

L'Internal Audit deve assicurarsi che il framework di outsourcing sia in linea con la strategia dell'istituto e che sia **efficacemente implementato**, assicurando l'adeguatezza, la qualità e l'efficacia della valutazione dei rischi relativi alle funzioni esternalizzate

Gli istituti devono definire, **mantenere** e periodicamente **testare** piani di **business continuity** appropriati con riferimento all'outsourcing di funzioni critiche o importanti, assicurando i livelli di qualità di fornitura del servizio (**SLA**)

La politica deve normare le principali fasi del ciclo di vita dell'accordo di outsourcing, definendo i **principi guida**, le **responsabilità** e le **attività rilevanti** relative alla gestione delle esternalizzazioni

Il documento deve definire: (i) **ruoli e responsabilità**; (ii) le **attività propedeutiche** alla sottoscrizione degli accordi di outsourcing; (iii) le modalità di implementazione, **monitoraggio** e gestione degli accordi; (iv) le modalità di **tenuta del Registro**; (v) le linee guida per la definizione delle **exit strategy** e dei processi di risoluzione del ctr

Gli istituti devono **valutare tutti i rischi prima dell'esternalizzazione** e, come parte del monitoraggio, focalizzarsi sui rischi operativi, reputazionali e di concentrazione; e devono considerare il rischio risultante da sub-outsourcing delle attività sottostanti l'accordo o di parte di esse

I contenuti delle linee guida EBA in materia di Outsourcing

Alcune Definizioni

Cultura del
rischio / dei
rischi

L'insieme delle regole, degli atteggiamenti e dei comportamenti della banca che incidono sul grado di consapevolezza, sull'assunzione e gestione dei rischi, nonché sulle attività di controllo, che determinano le decisioni in materia di rischi. La cultura del rischio influenza le decisioni degli organi aziendali e del personale nello svolgimento quotidiano delle proprie attività e influisce sui rischi assunti dalla banca

Esternalizzaz

L'accordo in qualsiasi forma tra una banca e un fornitore di servizi in base al quale il fornitore realizza un processo, un servizio o un'attività che sarebbe altrimenti svolto dalla stessa banca

Subesternaliz

La situazione in cui il fornitore di servizi nell'ambito di un accordo di esternalizzazione trasferisce ulteriormente una funzione esternalizzata a un altro fornitore di servizi

Fornit di serv

Un soggetto terzo che realizza, in tutto o in parte, un processo, un servizio o un'attività esternalizzata nell'ambito di un accordo di esternalizzazione;

Alcune Definizioni – I servizi Cloud

“**servizi cloud**”: servizi in cloud computing, ossia un modello che consente l’accesso in rete diffuso, conveniente e su richiesta a un gruppo condiviso di risorse informatiche configurabili (ad esempio reti, server, memorie, applicazioni e servizi), che possono essere forniti e messi a disposizione rapidamente con un minimo di attività gestionale o di interazione con il fornitore del servizio. Si forniscono, di seguito, le definizioni delle diverse tipologie rilevanti di cloud computing:

- ❑ Cloud pubblico (**public cloud**): infrastruttura cloud in cui i servizi sono erogati a un vasto numero di clienti con funzionalità offerte in maniera aperta e condivisa;
- ❑ Cloud privato (**private cloud**): infrastruttura cloud disponibile per l’utilizzo esclusivo da parte della banca;
- ❑ Cloud di comunità (**community cloud**): infrastruttura cloud disponibile per l’utilizzo esclusivo da parte di una specifica comunità di banche, compresa una pluralità di banche e altre società appartenenti a un unico gruppo;
- ❑ Cloud ibrido (**hybrid cloud**): infrastruttura cloud costituita da due o più infrastrutture cloud distinte.

Alcune Definizioni - Funzione essenziale o importante

- “**Funzione essenziale o importante**”: una funzione per la quale risulta verificata almeno una delle seguenti condizioni:
- i. un’anomalia nella sua esecuzione o la sua mancata esecuzione possono compromettere gravemente:
 - a. i risultati finanziari, la solidità o la continuità dell’attività della banca; ovvero
 - b. la capacità della banca di conformarsi nel continuo alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;
 - ii. riguarda funzioni relative ad attività sottoposte a riserva di legge, nella misura in cui la prestazione di tali attività richiede l’autorizzazione da parte di un’autorità di vigilanza;
 - iii. riguarda compiti operativi delle funzioni aziendali di controllo, a meno che la valutazione dell’essenzialità e dell’importanza della funzione svolta dalla banca non stabilisca che la mancata o inadeguata esecuzione di questi compiti operativi non avrebbe impatti negativi sull’efficacia delle funzioni aziendali di controllo.

Alcune Definizioni - Funzione essenziale o importante

Nel valutare se un accordo di esternalizzazione riguarda una funzione essenziale o importante, gli enti e gli istituti di pagamento dovranno considerare, oltre all'esito della valutazione del rischio, una serie di fattori tra cui:

- i) il potenziale impatto che un'interruzione della funzione esternalizzata o la mancata prestazione del servizio ai livelli di servizio concordati su base continuativa da parte del fornitore potrebbe avere sulla propria solidità e sostenibilità finanziaria a breve e a lungo termine, sulla propria continuità operativa e sui rischi reputazionali e operativi;
- ii) l'impatto potenziale dell'accordo di esternalizzazione sulla propria capacità di individuare, monitorare e gestire tutti i rischi nonché di rispettare le previsioni di legge e gli obblighi normativi;
- iii) l'impatto potenziale sui servizi forniti alla clientela, sulle dimensioni e la complessità di qualsiasi area operativa interessata; e
- iv) la possibilità di trasferire l'accordo di esternalizzazione proposto a un altro provider.

Titolo I – Governance degli Accordi

Il principio di proporzionalità dovrà tenere conto:

- **dimensioni,**
- **profilo di rischio** individuale,
- **organizzazione interna,**
- **natura e scopo,**
- **complessità delle attività.**

Gli enti e gli istituti di pagamento dovranno tenere in considerazione la complessità delle funzioni esternalizzate, i rischi derivanti dall'accordo di outsourcing, l'essenzialità o l'importanza della funzione esternalizzata e l'impatto potenziale dell'esternalizzazione sulla continuità operativa.

Il soggetto che esternalizza rimane responsabile per le attività esternalizzate, e a tal fine i relativi organi amministrativi devono essere dotati di **adeguate risorse, procedure scritte e allocazione di responsabilità** per realizzare **un controllo costante, efficace e mirato** sulle attività esternalizzate.

Qualora l'esternalizzazione avvenga nell'ambito dello stesso gruppo di appartenenza, l'ente garantisce che la selezione del fornitore si fondi su elementi oggettivi e che l'accordo sia stato concluso alle normali condizioni di mkt.

Requisiti di Governance

I requisiti di governance:

- **non pregiudichino la capacità** dell'organo di gestione di svolgere i propri compiti;
- la **possibilità di prendere e attuare decisioni** anche in relazione alle attività e alle funzioni aziendali esternalizzate;
- il mantenimento della **regolarità del *business***;
- **funzioni di controllo interno adeguate**;
- i **rischi connessi** agli accordi, siano **adeguatamente identificati, valutati, gestiti e mitigati**, anche con riferimento ai rischi ICT;

Requisiti di Governance



- adeguati **flussi informativi** con i fornitori di servizi;
- possibilità di **trasferire** la funzione critica o importante ad un **fornitore di servizi alternativo**;
- di **reinternalizzare** la funzione critica o importante nell'ambito dell'istituzione;
- l'attuazione di misure di controllo appropriate ed un'archiviazione dei dati in conformità al **Regolamento 2016/679 (GDPR)**;

Titolo II - Valutazione degli accordi di esternalizzazione

Spetta agli enti e agli istituti di pagamento valutare se un accordo con un soggetto terzo rientri nella definizione di esternalizzazione. In tale valutazione si dovrà infatti tenere conto se la funzione esternalizzata (o parte di essa):

- i) viene svolta dal terzo su base ricorrente o permanente; e se
- ii) ricadrebbe, in linea di principio, nell'ambito delle attività normalmente svolte dall'ente o dall'IP.

Non sarebbero da considerare come esternalizzazione:

- i) una funzione che, per legge, deve essere svolta da un fornitore di servizi (ad esempio, la revisione legale dei conti);
- ii) servizi di informazione sui mercati (ad esempio, le informazioni rese dalle agenzie di rating);
- iii) le infrastrutture di rete globali (ad esempio, Visa e MasterCard);
- iv) gli accordi di compensazione e regolamento tra organismi di compensazione, controparti centrali e istituti di regolamento e loro membri;
- v) le infrastrutture globali di messaggistica finanziaria soggette alla vigilanza delle pertinenti autorità;
- vi) i servizi bancari di corrispondenza; e
- vii) l'acquisizione di servizi che altrimenti non sarebbero forniti dall'ente o dall'istituto di pagamento (ad esempio, la consulenza di un professionista).

Titolo II - Valutazione degli accordi di esternalizzazione

Le funzioni che sono necessarie allo svolgimento delle attività delle principali linee di business o delle funzioni essenziali dovrebbero essere considerate funzioni essenziali o importanti, a meno che la valutazione dell'ente non stabilisca che la mancata esecuzione della funzione esternalizzata o un'esecuzione inadeguata della stessa non avrebbe un impatto negativo sulla continuità operativa della linea di business principale o della funzione essenziale.

Titolo II - Valutazione degli accordi di esternalizzazione

Nel valutare se un accordo di esternalizzazione riguarda una funzione essenziale o importante, gli enti e gli istituti di pagamento dovrebbero considerare, insieme all'esito della valutazione del rischio, almeno i seguenti fattori:

- a. se l'accordo di esternalizzazione è direttamente collegato alla prestazione di attività bancarie o di servizi di pagamento per i quali gli enti o gli istituti di pagamento sono autorizzati;
- b. il potenziale impatto che un'interruzione nell'esecuzione della funzione esternalizzata o la mancata prestazione del servizio ai livelli di servizio concordati su base continuativa da parte del fornitore di servizi potrebbe avere su:
 - i. la propria solidità e sostenibilità finanziaria a breve e a lungo termine, compresi, se del caso, gli attivi, il capitale, i costi, le fonti di finanziamento (funding), la liquidità, i profitti e le perdite;
 - ii. la propria continuità e solidità operativa;
 - iii. i rischi operativi, compresi i rischi di condotta, i rischi legati alle tecnologie dell'informazione e della comunicazione («information and communication technologies, ICT») e i rischi legali;
 - iv. i rischi reputazionali;
 - v. ove opportuno, la pianificazione del risanamento e della risoluzione delle crisi, la possibilità di risoluzione (resolvability) e la continuità operativa in una situazione di intervento precoce, risanamento o risoluzione;

Titolo II - Valutazione degli accordi di esternalizzazione (segue)

Nel valutare se un accordo di esternalizzazione riguarda una funzione essenziale o importante, gli enti e gli istituti di pagamento dovrebbero considerare, insieme all'esito della valutazione del rischio, almeno i seguenti fattori:

- c. l'impatto potenziale dell'accordo di esternalizzazione sulla propria capacità di:
 - i. individuare, monitorare e gestire tutti i rischi;
 - ii. rispettare tutte le previsioni di legge e tutti gli obblighi normativi;
 - iii. condurre opportune verifiche di audit sulla funzione esternalizzata;
- d. l'impatto potenziale sui servizi forniti ai propri clienti;
- e. tutti gli accordi di esternalizzazione, l'esposizione complessiva dell'ente o dell'IP nei confronti dello stesso fornitore di servizi e il potenziale impatto cumulativo degli accordi di esternalizzazione nella medesima area operativa;
- f. le dimensioni e la complessità di qualsiasi area operativa interessata;
- g. la possibilità di ampliare (scale up) l'accordo di esternalizzazione proposto senza sostituire o rivedere l'accordo sottostante;
- h. la possibilità di trasferire l'accordo di esternalizzazione proposto a un altro fornitore di servizi, se necessario o auspicabile, sia contrattualmente sia nella pratica, compresi i rischi stimati, gli ostacoli alla continuità operativa, i costi e le tempistiche di esecuzione («sostituibilità»);
- i. la capacità di reintegrare la funzione esternalizzata all'interno dell'ente o dell'istituto di pagamento, se necessario o auspicabile;
- j. la protezione dei dati e l'impatto potenziale di una violazione dell'obbligo di riservatezza o della mancata disponibilità e integrità dei dati relativi all'ente o all'istituto di pagamento e ai suoi clienti

Titolo III - Quadro di governance

Si ravvisa la necessità che, nell'ambito del sistema generale dei controlli interni, gli enti e gli istituti di pagamento pongano in essere adeguati dispositivi di governance e rischio, vale a dire meccanismi atti a identificare, valutare e gestire i rischi derivanti dalla stipula di accordi con soggetti terzi, a prescindere dal fatto che tali accordi abbiano per oggetto l'esternalizzazione di funzioni aziendali.

Le linee guida chiariscono che l'esternalizzazione di alcune funzioni non determina in ogni caso il venir meno della responsabilità dell'Organo di amministrazione. Detto Organo è infatti in ogni momento pienamente responsabile dell'assetto organizzativo interno, dell'identificazione, valutazione e gestione dei conflitti di interesse, della definizione di strategie e di politiche aziendali (ad esempio, modello di business e propensione al rischio), di vigilanza sulla gestione corrente, compresa la gestione dei rischi legati all'esternalizzazione. A tal fine, si richiede agli enti e agli istituti di pagamento di:

- i) attribuire in modo chiaro le responsabilità per le attività di documentazione, gestione e controllo degli accordi di esternalizzazione;
- ii) stanziare risorse sufficienti ad assicurare il pieno rispetto degli obblighi normativi; e
- iii) istituire una funzione di outsourcing o individuare tra le persone che occupano posizioni apicali un senior staf member che risponda direttamente all'Organo di amministrazione e che sia responsabile della gestione e supervisione dei rischi connessi con gli accordi stipulati.

Titolo III

In caso di esternalizzazione, gli enti e gli istituti di pagamento dovranno:

- i) prendere e attuare decisioni anche in relazione alle attività e alle funzioni esternalizzate;
- ii) garantire l'ordinato svolgimento delle proprie attività e dei servizi bancari e di pagamento resi alla clientela;
- iii) individuare, monitorare, gestire e mitigare i rischi connessi con gli accordi di esternalizzazione, sia attuali che prospettici, anche con riferimento ai rischi ICT;
- iv) porre in essere disposizioni adeguate in materia di riservatezza dei dati e di altre informazioni;
- v) prevedere adeguati flussi informativi con i fornitori di servizi; e
- vi) mantenere, per le funzioni esternalizzate, su base continuativa e nell'ambito di un ragionevole lasso di tempo, la capacità di trasferire la funzione a fornitori di servizi alternativi, di reintegrare la funzione oppure di sospendere le attività operative che dipendono dalla funzione esternalizzata.

Si attribuisce all'Organo di amministrazione il compito di approvare, rivedere e aggiornare, una "policy di outsourcing", curandone l'attuazione, che delinei le principali fasi del ciclo di vita dell'accordo di esternalizzazione e definisca i principi guida, le responsabilità e le attività rilevanti relative alla gestione delle esternalizzazioni.

La regolamentazione interna

Un ruolo di particolare rilievo nell'ambito delle *Linee Guida EBA* è assunto dalla **regolamentazione interna** al fine di risultare in ogni momento *compliant* alla normativa di riferimento.

- Occorre **approvare e mantenere una policy di outsourcing** che descriva **le fasi principali del ciclo di vita degli accordi di ristrutturazione** e che riporti **i principi, le responsabilità e le funzioni coinvolte** nel processo di esternalizzazione.

- Riportare la **distinzione** tra:
 - i. funzioni **essenziali o importanti e altri accordi**
 - ii. fornitori di servizi **autorizzati da un'autorità competente**
 - iii. accordi di esternalizzazione **infragruppo** e ad **entità esterne**
 - iv. fornitori di servizi situati in uno Stato membro e **in paesi terzi**

Il contenuto della Policy di Outsourcing

Il **contenuto** informativo della policy è **più ampio** rispetto alle vigenti disposizioni per gli enti creditizi. La policy in parola, infatti, dovrebbe almeno stabilire:

- **Ruoli** e connesse **responsabilità**;
- il **coinvolgimento** delle linee di business, delle funzioni di controllo interno e di altri soggetti con riferimento agli accordi di esternalizzazione;
- **i criteri adottati per l'identificazione di funzioni critiche** o importanti (FOI);
- i controlli di **due diligence** sui potenziali fornitori di servizi;
- **gestione dei rischi connessi** con l'esternalizzazione;
- la gestione dei **potenziali conflitti di interesse** che potrebbero insorgere con i fornitori di servizi, specie nell'ambito delle ipotesi di esternalizzazione infragruppo;
- Il **piano di continuità operativa** e test di disaster recovery, al fine di limitare le perdite in caso di grave interruzione dell'attività anche a seguito del fallimento del fornitore o di rischi politici nel Paese del fornitore;
- Il **processo di approvazione** dei nuovi accordi di esternalizzazione;
- le **valutazioni continuative delle prestazioni del fornitore** di servizi: es.
 - i. *assicurare la ricezione di relazioni appropriate dai fornitori di servizi;*
 - ii. *valutare le prestazioni dei fornitori di servizi utilizzando strumenti quali KPI (key performance indicator);*
 - iii. *diritto di accesso per le verifiche di audit indipendenti;*
- **le strategie di uscita** (*sviluppare e attuare piani di uscita e identificare soluzioni alternative*);
- la documentazione e **la tenuta dei registri per tutti** gli accordi di outsourcing.

Istituzione di un Registro relativo ai contratti di outsourcing

In un'ottica di rafforzamento dei presidi in materia di monitoraggio e di tracciabilità delle funzioni/attività oggetto di esternalizzazione e dei relativi accordi contrattuali, l'EBA ha introdotto specifiche previsioni relativamente alla necessità - in capo ai destinatari - di dotarsi di un apposito Registro, finalizzato a documentare gli accordi di esternalizzazione in essere.

Le Guidelines forniscono puntuali indicazioni (in termini di requisiti generali e contenuti minimi) che dovranno guidare i destinatari nell'implementazione e nell'aggiornamento periodico del Registro. Una parte di tali requisiti minimi (i.e. informazioni sui contratti nonché sui provider) trovano applicazione con riferimento alle attività rientranti nella definizione di "outsourcing", mentre altri rilevano relativamente all'esternalizzazione di funzioni critiche o importanti.

Sono previsti inoltre specifici obblighi di informazione e messa a disposizione del Registro nei confronti delle competenti Autorità di Vigilanza.

Istituzione di un Registro relativo ai contratti di outsourcing

E' previsto che l'istituzione finanziaria debba provvedere a informare, in modo adeguato e tempestivo, le Autorità competenti in merito all'eventuale esternalizzazione di attività critiche o importanti, fornendo opportune indicazioni al riguardo. La stessa deve, altresì, provvedere alle relative comunicazioni in caso di attività esternalizzata che possa diventare importante o critica, indicando

- (i) il numero di riferimento del relativo Registro;
- (ii) l'ultima data di rinnovo del contratto;
- (iii) la data di conclusione dell'accordo ovvero la data del successivo rinnovo.

È, infine, richiesto all'istituzione finanziaria di mettere a disposizione, su richiesta, tutte le informazioni necessarie al fine di consentire alle Autorità competenti l'esecuzione di un'efficace attività di supervisione, ivi inclusa la possibilità di prendere visione dei contratti di esternalizzazione.

Il Registro

Informazioni minime

- Numero di riferimento
- breve descrizione della funzione esternalizzata
- la data di inizio e la data di scadenza del contratto
- la categoria assegnata che riflette la natura della funzione
- il nome del fornitore di servizi
- il paese in cui il servizio è prestato
- in caso di fornitore di servizi cloud specificare i modelli di implementazione (natura dei dati e luoghi in cui saranno conservati);
- la data dell'ultima valutazione dell'essenzialità della funzione esternalizzata;
- un campo (si/no) per indicare se la funzione è ritenuta essenziale o importante.

FOI informazioni aggiuntive

- Una campo per indicare se il fornitore o subfornitore appartiene al gruppo;
- La data dell'ultima valutazione dei rischi e una sintesi dei risultati;
- L'organo decisionale che ha approvato l'accordo di outsourcing;
- La normativa che disciplina il contratto;
- Le date delle ultime verifiche audit e quelle in programma;
- Paese e luogo dove sarà prestato il servizio e in cui i dati saranno conservati;
- Il risultato (facile, difficile o impossibile) dell'analisi sulla possibilità di sostituzione o reinternalizzazione;
- Identificazione di fornitori alternativi;
- Indicare se l'esternalizzazione della funzione critica o importante è considerata tale nel tempo;
- La stima del costo finanziario annuo (budget cost).

La Funzione di Internal Audit

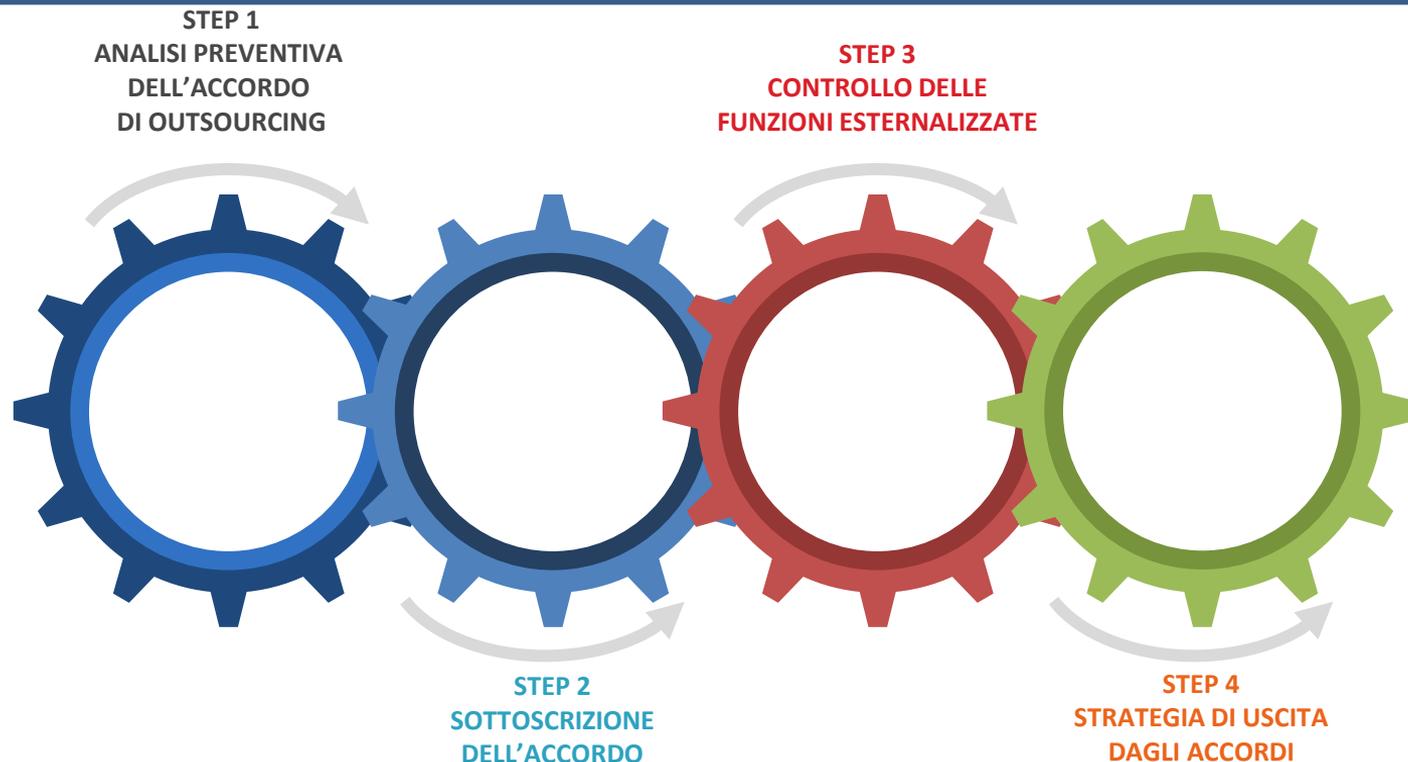
Il Piano di Audit deve includere la valutazione degli accordi di esternalizzazione di funzioni critiche o importanti, tra cui specifiche **analisi dell'adeguatezza delle misure di protezione dei dati**, dei controlli delle misure di gestione del rischio e di continuità operativa attuate dal fornitore di servizi.

Funzione di *Internal Audit* ha la responsabilità di accertare:

- il rispetto della Policy e delle Procedure interne;
- la corretta identificazione della funzione come FOI;
- che i rischi rimangano entro la propensione al rischio (*risk appetite*) definita;
- l'appropriato coinvolgimento degli organi aziendali;
- l'appropriato monitoraggio e gestione degli accordi di esternalizzazione.

FASE CONTRATTUALE: un sistema per il monitoraggio delle principali attività esternalizzate attraverso la definizione di un **insieme di regole per la misurazione del servizio e per il loro controllo (KPI e SLA)**, con la tempestiva evidenza di eventuali scostamenti, **al fine di permettere un costante monitoraggio delle esternalizzazioni e una costante verifica dei rischi e misurazione anche da parte della Funzione Internal Audit.**

Titolo IV – Processo di esternalizzazione



Step 1 - Attività di assessment preliminari (1/3)

Le Linee Guida sottolineano l'importanza di un accurato processo di valutazione da compiere nella fase preliminare all'esternalizzazione di funzioni/attività, con particolare riferimento a:

- (i) tipo di funzione che sarà oggetto di esternalizzazione (i.e. se funzione critica/importante o meno);
- (ii) possibilità di esternalizzare la funzione di volta in volta rilevante;
- (iii) rischi connessi alla figura del fornitore esterno (e.g. attività di due diligence, in relazione alla quale le Linee Guida forniscono ai destinatari specifici criteri e fattori da impiegare nel corso dell'analisi).

Con particolare riferimento alle attività di due diligence da svolgere sul potenziale provider, le Guidelines indirizzano i destinatari nel processo di valutazione nonché nell'individuazione degli elementi rilevanti da esaminare preliminarmente alla conclusione del contratto (e.g. relazioni professionali di lungo periodo con i fornitori che abbiano già lavorato per l'istituzione finanziaria), suggerendo, inoltre, adeguate e continue attività di monitoraggio delle performance del fornitore e - ove applicabile dei sub-fornitori - al fine di prevedere un regolare e periodico aggiornamento della valutazione dei rischi.

Step 1 – verifica presenza FOI - (2/3)

Gli enti e gli istituti di pagamento, prima della formalizzazione dell'accordo, valutano se esso riguarda una funzione essenziale o importante e se le condizioni di vigilanza per l'esternalizzazione siano soddisfatte. Le modalità di tale valutazione variano a seconda se un fornitore di servizi è situato in uno Stato membro o in un paese terzo:

- nel primo caso è sufficiente che sia soddisfatta una delle seguenti condizioni, ossia che il fornitore è registrato o autorizzato a svolgere attività bancaria o servizi di pagamento oppure è altrimenti autorizzato a svolgere tali attività o servizi di pagamento conformemente alla normativa applicabile in materia;
- nel secondo caso è invece necessario che siano soddisfatte tutte e tre le seguenti condizioni:
 - 1) il fornitore è registrato o autorizzato a svolgere tali attività o servizi di pagamento nel paese terzo ed è vigilato dall'autorità di quest'ultimo paese;
 - 2) esiste un accordo di cooperazione tra le autorità di vigilanza dell'ente e quelle del fornitore;
 - 3) l'accordo di cui al punto sub 2) dovrà assicurare che le autorità competenti siano quanto meno in grado di ottenere, su richiesta, le informazioni necessarie allo svolgimento dei propri compiti di vigilanza, avere accesso a dati e notizie rilevanti per l'esercizio dei poteri di supervisione, ricevere informazioni dall'autorità di vigilanza del paese terzo per indagare su presunte violazioni normative;

Step 1 – Analisi dei rischi (3/3)

Gli enti e gli istituti di pagamento, prima della formalizzazione dell'accordo, individuano e valutano l'impatto potenziale degli accordi di esternalizzazione in termini di rischio operativo, di concentrazione, reputazionale, legale e quello legato alla sub-esternalizzazione.

La valutazione dovrà includere scenari di possibili eventi di rischio, compresi quelli che comportano un rischio operativo di elevata gravità; effettuino una adeguata due diligence sul fornitore dei servizi.

Gli elementi da prendere in considerazione per lo svolgimento di tale attività sono, tra gli altri, la reputazione commerciale del provider, le sue capacità professionali, risorse umane, informatiche e finanziarie di cui dispone, la struttura organizzativa e proprietaria e il modello di business.

I contenuti delle linee guida EBA in materia di Outsourcing

Step 2 - Rafforzamento del contenuto minimo dei contratti

La seconda fase consiste nella formalizzazione dell'accordo di outsourcing, mediante la stipula di un contratto scritto.

Le Linee Guida sottolineano l'importanza di una puntuale e chiara definizione dei diritti e degli obblighi contrattuali tra le parti nell'ambito dell'esternalizzazione di funzioni o attività.

In tale ambito, le Guidelines forniscono un'elencazione puntuale delle previsioni che i contratti di outsourcing devono almeno contenere in caso di esternalizzazione di funzioni critiche o importanti (e.g. gli obblighi delle parti contrattuali; il livello di servizio atteso, sia da un punto di vista qualitativo sia quantitativo; il Paese in cui sarà svolta la funzione esternalizzata da parte del service provider; la possibilità di sub-esternalizzare funzioni critiche e le relative condizioni di subesternalizzazione; la presenza di un'eventuale copertura assicurativa a fronte di un inadempimento contrattuale; un chiaro riferimento alla Bank Recovery and Resolution Directive, con particolare riferimento alla descrizione delle concrete obbligazioni delle parti verso le Autorità competenti)

Step 2 – Contenuti minimi dell'accordo di esternalizzazione

- a. una descrizione chiara della funzione esternalizzata che deve essere svolta;
- b. la data di inizio e, ove applicabile, la data di fine dell'accordo e i termini di preavviso per il fornitore di servizi e per l'ente o l'istituto di pagamento;
- c. la normativa che disciplina il contratto;
- d. gli obblighi finanziari delle parti;
- e. una clausola che indichi se è consentita la subesternalizzazione di una funzione essenziale o importante o di parti sostanziali di essa e, in caso affermativo, le condizioni alle quali la subesternalizzazione è soggetta;
- f. i luoghi (regioni o paesi) in cui sarà svolta la funzione essenziale o importante e/o in cui saranno conservati e trattati i relativi dati, compreso l'eventuale luogo di conservazione, e le condizioni da soddisfare, compreso l'obbligo di informare l'ente o l'istituto di pagamento se il fornitore di servizi propone di cambiare tali luoghi;
- g. se del caso, le disposizioni riguardanti l'accessibilità, la disponibilità, l'integrità, la riservatezza e la sicurezza dei relativi dati;
- h. il diritto dell'ente o dell'istituto di pagamento di effettuare un monitoraggio costante della performance del fornitore di servizi;
- i. i livelli di servizio concordati, che dovrebbero includere precisi obiettivi di performance, quantitativi e qualitativi, per la funzione esternalizzata, in modo da consentire un monitoraggio tempestivo;

Step 2 – Contenuti minimi dell'accordo di esternalizzazione (segue)

- j. gli obblighi di reportistica del fornitore di servizi all'ente o all'istituto di pagamento, compresa la comunicazione da parte del fornitore di servizi di qualsiasi sviluppo che possa avere un impatto rilevante sulla sua capacità di svolgere efficacemente la funzione essenziale o importante;
- k. una clausola che indichi se il fornitore di servizi debba stipulare un'assicurazione obbligatoria contro determinati rischi e, ove applicabile, il livello di copertura assicurativa richiesto;
- l. i requisiti per l'attuazione e la verifica dei piani di emergenza dell'impresa (business contingency plans);
- m. disposizioni che assicurino l'accesso ai dati di cui l'ente o l'istituto di pagamento sono titolari in caso di insolvenza, risoluzione o cessazione dell'attività del fornitore di servizi;
- n. l'obbligo del fornitore di servizi di cooperare con le autorità competenti e le autorità di risoluzione dell'ente o dell'istituto di pagamento, e con altri soggetti da questi designati;
- o. per gli enti, un chiaro riferimento ai poteri dell'autorità nazionale di risoluzione e una descrizione degli «obblighi sostanziali» del contratto;
- p. il diritto illimitato degli enti, degli IP e delle autorità competenti di ispezionare e sottoporre a verifiche di audit il fornitore di servizi per quanto riguarda, in particolare, la funzione essenziale o importante esternalizzata;
- q. i diritti di cessazione.

Step 2 – Subesternalizzazione di funzioni essenziali o importanti

L'accordo di esternalizzazione dovrebbe specificare se è consentita o meno la subesternalizzazione di funzioni essenziali o importanti o di parti sostanziali delle stesse. Se è consentita, gli enti e gli istituti di pagamento dovrebbero stabilire se la parte della funzione da subesternalizzare è, in quanto tale, essenziale o importante (ovvero se costituisce una parte sostanziale della funzione essenziale o importante) e, in tal caso, annotarlo nel registro. Se la subesternalizzazione di funzioni essenziali o importanti è consentita, l'accordo scritto dovrebbe:

- a. specificare le tipologie di attività che sono escluse dalla subesternalizzazione;
- b. specificare le condizioni da rispettare in caso di subesternalizzazione;
- c. specificare che il fornitore di servizi è tenuto a controllare i servizi che ha subappaltato per assicurare che tutti gli obblighi contrattuali tra il fornitore di servizi e l'ente o l'istituto di pagamento siano rispettati nel continuo;
- d. richiedere al fornitore di servizi di ottenere dall'ente o dell'IP una preventiva autorizzazione specifica o generale, in forma scritta, prima di subesternalizzare i dati;
- e. contemplare l'obbligo del fornitore di servizi di informare l'ente o l'IP di qualsiasi subesternalizzazione pianificata, o di eventuali modifiche sostanziali della stessa, in particolare se ciò potrebbe influire sulla capacità del fornitore di servizi di ottemperare alle proprie responsabilità previste dall'accordo di esternalizzazione;
- f. assicurare, ove opportuno, che l'ente o l'istituto di pagamento abbia il diritto di opporsi alla subesternalizzazione pianificata o alle relative modifiche sostanziali, o che sia necessaria un'approvazione esplicita;
- g. assicurare che l'ente o l'IP abbia il diritto di porre termine all'accordo in caso di subesternalizzazione indebita.

I contenuti delle linee guida EBA in materia di Outsourcing

Esternalizzazione di funzioni/attività a service provider aventi sede in Paesi Terzi

L'Autorità europea, nell'ambito delle Linee Guida, dedica particolare attenzione alle casistiche di esternalizzazione di funzioni/attività a provider aventi sede in Paesi Terzi. Al riguardo, l'EBA fornisce puntuali indicazioni (criteri/elementi da tenere in considerazione) in merito alle attività di valutazione da porre in essere preliminarmente alla decisione di esternalizzare (e.g. in caso di esternalizzazione di funzioni di core business, esecuzione di una valutazione in merito alla presenza delle debite autorizzazioni in capo al potenziale provider, nonché relativamente alla presenza di un'intesa fra l'Autorità di Vigilanza connessa al destinatario esternalizzante e la competente Autorità di Vigilanza dell'outsourcer che assicuri, fra gli altri, la possibilità per la prima di accedere alle informazioni, ai dati e alle risorse necessarie ai fini dello svolgimento dei propri poteri di vigilanza anche nel Paese Terzo).

Si consente espressamente all'ente o all'istituto di pagamento di porre termine al contratto di outsourcing anche nei casi in cui:

- i) il provider violi disposizioni legislative, regolamentari e contrattuali;
- ii) vengano individuati impedimenti in grado di alterare l'esecuzione della funzione esternalizzata;
- iii) siano apportate modifiche rilevanti che incidono sull'accordo;
- iv) emergano carenze nella gestione e nella sicurezza dei dati o delle informazioni riservate.

Step 3 – Monitoraggio dell'attività del fornitore di servizi

La terza fase disciplina il monitoraggio dell'attività del fornitore di servizi su base continuativa secondo un approccio risk based, con particolare attenzione all'esternalizzazione di funzioni essenziali o importanti.

Gli enti e gli istituti di pagamento dovranno pertanto:

- i) aggiornare la propria valutazione dei rischi, dandone periodicamente notizia all'Organo di amministrazione;
- ii) assicurare che gli accordi di esternalizzazione soddisfino adeguati standard quantitativi e qualitativi;
- iii) adottare misure correttive qualora emergano carenze nell'esecuzione della funzione esternalizzata.

Step 4 - Meccanismi di salvaguardia e protezione

Le Linee Guida sanciscono specifici obblighi di collaborazione e sostegno in capo al provider nei confronti dell'istituzione esternalizzante, ad esempio in caso di trasferimento del servizio erogato dallo stesso provider ad altro competitor.

Inoltre, al fine di evitare danni da interruzione dei servizi esternalizzati, nell'ipotesi di fallimento del fornitore e/o di deterioramento delle funzioni critiche o importanti esternalizzate, le Linee Guida richiedono alle istituzioni la puntuale elaborazione di exit strategies (i.e. piani di transizione), nonché periodiche attività di testing inerenti alle stesse.

Step 4 – Exit Strategy

E' quindi previsto che gli enti e gli istituti di pagamento si dotino di una **strategia di uscita (exit strategy)** dall'accordo di outsourcing per tutte le esternalizzazioni di funzioni essenziali o importanti, nei casi di scadenza dell'accordo, di dissesto del provider, di deterioramento qualitativo dei servizi forniti o di insorgenza di rischi rilevanti per lo svolgimento adeguato e continuativo della funzione.

L'obiettivo è di **garantire l'uscita da ogni accordo di outsourcing, senza un'interruzione delle attività operative e senza pregiudicare la continuità e la qualità dei servizi resi alla clientela.** A tal fine, si richiede agli enti e agli istituti di pagamento di:

- i) **sviluppare e attuare piani di uscita (exit plans) completi, documentati e sufficientemente testati** (ad esempio, effettuando un'analisi dei costi potenziali, degli impatti previsti, delle implicazioni in termini di risorse e tempistiche per il trasferimento dei servizi esternalizzati a un altro provider); e
- ii) **individuare soluzioni alternative e sviluppare piani di transizione (transition plans) per permettere il trasferimento delle funzioni esternalizzate e dei dati da un provider all'altro o di re-internalizzare la funzione in modo ordinato.**

Titolo V - Orientamenti in materia di esternalizzazione indirizzati alle autorità competenti

Alle autorità di vigilanza si attribuisce il compito di verificare se gli enti e gli istituti di pagamento abbiano assicurato, nell'ambito dei rispettivi accordi di outsourcing, che i fornitori di servizi sono obbligati a concedere all'autorità competente e all'ente o all'istituto di pagamento in questione diritti di audit e di accesso ai locali in cui opera il provider.

L'azione di supervisione nei confronti degli outsourcers si sviluppa attraverso:

- i) l'analisi dei rischi di esternalizzazione degli enti, da effettuare nel contesto SREP e, relativamente agli istituti di pagamento, nell'ambito di altri processi di vigilanza (richieste ad hoc, ispezioni in loco, ecc.);
- ii) l'esame delle informazioni annotate nel registro; e
- iii) la richiesta di informazioni dettagliate sugli accordi di esternalizzazione, anche se la funzione in questione non è considerata essenziale o importante. Inoltre, seguendo un approccio basato sul rischio, le autorità competenti saranno chiamate a valutare se gli enti e gli istituti di pagamento: monitorano e gestiscono in modo adeguato gli accordi di esternalizzazione di funzioni essenziali o importanti; dispongano di risorse sufficienti per svolgere efficacemente i compiti di cui al punto precedente; individuano e gestiscono tutti i rischi cui sono o sarebbero esposti; identificano, valutano e gestiscono adeguatamente i conflitti di interesse che potrebbero insorgere tra l'ente e il fornitore di servizi.

Titolo V

Qualora siano riscontrate debolezze nei dispositivi di governance o gravi violazioni normative, le autorità competenti potranno adottare misure appropriate che possono prevedere la limitazione dell'esternalizzazione di funzioni o la restrizione del perimetro delle funzioni esternalizzate o l'obbligo di porre termine a uno o più contratti di outsourcing.

Principi generali

La banca, attraverso il ricorso all'esternalizzazione, non può:

- delegare le proprie responsabilità, né la responsabilità degli organi aziendali;
- alterare il rapporto e gli obblighi nei confronti dei suoi clienti;
- mettere a repentaglio la propria capacità di rispettare gli obblighi previsti dalla disciplina di vigilanza né mettersi in condizione di violare le riserve di attività previste dalla legge;
- pregiudicare la qualità del sistema dei controlli interni;
- ostacolare la vigilanza.

L'esternalizzazione di compiti operativi delle funzioni aziendali di controllo, all'interno o all'esterno del gruppo, è ammessa nel rispetto del principio di proporzionalità. Resta ferma la responsabilità degli organi aziendali e del responsabile della funzione esternalizzata per il corretto svolgimento dei compiti esternalizzati.

Comunicazioni alla Banca centrale europea o alla Banca d'Italia

Dopo l'approvazione da parte degli organi competenti e prima di dare corso all'esternalizzazione di funzioni essenziali o importanti, le banche comunicano alla Banca centrale europea o alla Banca d'Italia le informazioni di cui al paragrafo 54 degli Orientamenti dell'EBA in materia di esternalizzazione («Contenuto del Registro»).

È facoltà per le banche avviare un confronto preliminare con l'autorità di vigilanza sui progetti di esternalizzazione più rilevanti e/o innovativi, prima di conferire l'incarico. Restano in ogni caso fermi tutti i poteri, anche di intervento e sanzionatori, spettanti all'autorità di vigilanza.

Le banche informano la Banca centrale europea o la Banca d'Italia se una funzione esternalizzata è stata successivamente qualificata come funzione operativa essenziale o importante. L'informativa attesta il rispetto delle condizioni previste per l'esternalizzazione di funzioni essenziali o importanti. Le banche informano tempestivamente la Banca centrale europea o la Banca d'Italia di modifiche rilevanti e/o eventi gravi riguardanti i propri accordi di esternalizzazione che potrebbero avere un impatto significativo sulla continuità delle proprie attività operative.

Entro il 30 aprile di ogni anno le banche trasmettono alla Banca centrale europea o alla Banca d'Italia una relazione, redatta dalla funzione di revisione interna – o, se esternalizzata, dal referente aziendale – con le considerazioni dell'organo con funzione di controllo e approvata dall'organo con funzione di supervisione strategica, relativa ai controlli svolti sulle funzioni essenziali o importanti esternalizzate a fornitori di servizi al di fuori del gruppo, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate.

Esternalizzazione del trattamento del contante

Le banche che esternalizzano l'attività di trattamento del contante adottano specifiche cautele nella gestione dei rapporti con gli outsourcer sia all'atto della scelta del contraente, che deve fondarsi sull'accertamento della sua piena affidabilità, della correttezza della gestione e dell'adeguatezza delle strutture e dei processi organizzativi, sia nell'esercizio di efficaci controlli successivi, da svolgere nel continuo per verificare l'ordinato e corretto svolgimento dell'attività, nel pieno rispetto delle norme vigenti.

Le funzioni aziendali di controllo effettuano, ciascuna per i profili di competenza, una specifica valutazione delle procedure seguite per l'allacciamento e la gestione dei rapporti con i soggetti cui è esternalizzata l'attività di trattamento del contante nonché del complessivo assetto dei controlli sulle attività esternalizzate. Inoltre, tali funzioni assicurano il rispetto degli obblighi previsti dalla Decisione della BCE del 16 settembre 2010, n. 14 relativa al controllo dell'autenticità e idoneità delle banconote in euro e al loro ricircolo.

La banca che intende esternalizzare l'attività di trattamento del contante stipula con il fornitore di servizi un contratto concluso in forma scritta che, oltre a rispettare i requisiti previsti nel paragrafo precedente, prevede:

- l'obbligo di attenersi alle disposizioni comunitarie sopra richiamate, con particolare riguardo:
 - (i) all'utilizzo esclusivo di apparecchiature conformi a detta disciplina;
 - (ii) alle procedure di verifica delle apparecchiature;
 - (iii) alle attività di monitoraggio che possono essere condotte dalla Banca d'Italia;
- la possibilità per le banche di verificare la performance del servizio reso e di richiedere eventuali misure correttive;
- il diritto per la banca di recedere, senza penalità, nel caso in cui la controparte violi gli obblighi contrattuali e non vi ponga rimedio entro il periodo di tempo indicato nel contratto stesso.

Principi generali

L'esternalizzazione delle risorse e servizi ICT può assumere diverse forme a seconda del modello architetturale e delle strategie di outsourcing adottate dall'intermediario: outsourcing verticale (relativo a determinati processi operativi), outsourcing orizzontale di servizi trasversali come la gestione degli apparati hardware (facility management), lo sviluppo e la gestione del parco applicativo (application management), i collegamenti di rete, l'help desk tecnico e gli interventi di riparazione e manutenzione delle risorse ICT, fino al full outsourcing del complessivo sistema informativo aziendale. Viene inoltre in rilievo il cloud computing (servizi cloud), un modello che consente l'accesso in rete diffuso, conveniente, flessibile e su richiesta, a un gruppo condiviso di risorse informatiche (ad esempio reti, server, memorie, applicazioni e servizi), che vengono rese disponibili rapidamente, con un minimo di attività gestionale o di interazione con il fornitore del servizio.

Nell'utilizzo di un modello di cloud computing le banche definiscono i requisiti di sicurezza dei dati e dei sistemi nell'ambito dell'accordo di esternalizzazione e ne monitorano costantemente il rispetto; le banche inoltre adottano un approccio basato sul rischio con riferimento al luogo (paese e regione/località) dove sono conservati e trattati i dati e alla sicurezza delle informazioni.

Accordi con i fornitori e altri requisiti

Nell'accordo scritto tra la banca e i fornitori di sistemi e servizi ICT sono chiaramente definiti e formalizzati i seguenti aspetti:

- i. le misure di attenuazione dei rischi del fornitore dei servizi, che devono essere conformi con il quadro di riferimento per la gestione del rischio della banca, con particolare riguardo a quello ICT e di sicurezza;
- ii. misure idonee a garantire l'accountability e la ricostruibilità delle operazioni effettuate, almeno con riferimento alle operazioni critiche e agli accessi a dati personali o sensibili;
- iii. l'obbligo per il fornitore di servizi, una volta concluso il rapporto contrattuale e trascorso un periodo di tempo concordato, di eliminare – facendo uso di opportuni strumenti e soluzioni tecniche, debitamente documentati – qualsiasi copia o stralcio di dati personali o sensibili presente su propri sistemi o supporti in ragione dei servizi in precedenza esternalizzati dalla banca, in modo da escludere qualunque accesso successivo da parte del proprio personale o di terzi;
- iv. la ripartizione dei compiti e delle responsabilità attinenti all'attuazione della politica di Information Security della banca;
- v. il raccordo con i ruoli e le procedure dell'intermediario attinenti al processo di analisi dei rischi ICT e per il sistema di gestione dei dati.

Accordi con i fornitori e altri requisiti

L'informativa alla Banca centrale europea o alla Banca d'Italia (cfr. Capitolo 3, Sezione IV, par. 2), sottoscritta dal legale rappresentante della banca, attesta la conformità dell'operazione alle disposizioni di vigilanza applicabili e include le informazioni di seguito indicate:

- i. i risultati della valutazione dei rischi dell'accordo di esternalizzazione condotta dalla banca secondo quanto previsto dalla Sezione 12.2 degli Orientamenti dell'EBA in materia di esternalizzazione;
- ii. una descrizione delle strategie d'uscita (exit strategies), delle strategie di esternalizzazione della banca, del modello di riferimento per il sistema informativo come modificato dall'esternalizzazione e dei processi di funzionamento dei servizi esternalizzati, con particolare riguardo alle modalità con cui sono garantiti i requisiti di cui al presente Capitolo.

Nella relazione relativa ai controlli svolti sulle funzioni esternalizzate a fornitori di servizi al di fuori del gruppo la banca dà conto, tra l'altro, delle iniziative di esternalizzazione del sistema informativo che sono state oggetto di informativa preventiva, nonché dei principali servizi ICT forniti da terze parti che non assumono la qualifica di esternalizzazione.

Esternalizzazione, infrastrutture e controparti rilevanti

In caso di esternalizzazione di funzioni aziendali connesse allo svolgimento di processi critici, il piano di continuità operativa prevede le misure da attuare in caso di crisi con impatto rilevante sull'operatore o sul fornitore di servizi.

Nel contratto sono formalizzati:

- i livelli di servizio assicurati in caso di crisi e le soluzioni di continuità operativa poste in atto dal fornitore di servizi, adeguati al conseguimento degli obiettivi aziendali e coerenti con le prescrizioni della Banca d'Italia.
- le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori.

La Banca

acquisisce i piani di continuità operativa del fornitore di servizi o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità operativa realizzate all'interno.

Il fornitore di servizi

comunica tempestivamente all'operatore il verificarsi di incidenti al fine di consentire la pronta attivazione delle relative procedure di continuità operativa.

Esternalizzazione, infrastrutture e controparti rilevanti

Il piano di continuità operativa dell'operatore considera l'eventualità che le principali infrastrutture tecnologiche e finanziarie e le controparti rilevanti siano colpite da un evento catastrofico e stabilisce le misure per gestire i problemi conseguenti; la capacità di comunicare con i siti alternativi di tali soggetti è verificata periodicamente.

Per i servizi essenziali dell'operatore, va valutata la possibilità di prevedere il ricorso, in casi di emergenza, a fornitori alternativi. Nel caso in cui il fornitore abbia impegnato le stesse risorse per fornire analoghi servizi ad altre aziende, in particolare se situate nella stessa zona, sono stabilite cautele contrattuali per evitare il rischio che, in caso di esigenze concomitanti di altre organizzazioni, le prestazioni degenerino o il servizio si renda di fatto indisponibile

Controlli – Comunicazioni alla Banca d'Italia e alla BCE

Il piano di continuità operativa e il relativo processo di aggiornamento sono oggetto di regolare verifica da parte della funzione di revisione interna. L'internal audit prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, proponendo modifiche al piano di continuità operativa sulla base delle mancanze riscontrate. In tale ambito, particolare attenzione è posta all'analisi dei criteri di escalation.

In caso di incidenti, la funzione di audit verifica la congruità dei tempi rilevati per la dichiarazione dello stato di crisi. La funzione di revisione interna è anche coinvolta nel controllo dei piani di continuità operativa dei fornitori di servizi esternalizzati e degli altri fornitori critici; essa può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali, indipendenti e trasparenti quanto ai risultati dei controlli. L'internal audit esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali.

Gli operatori considerano l'opportunità di sottoporre il piano di continuità operativa alla revisione da parte di competenti terze parti indipendenti.

In caso di crisi, successivamente al ripristino dei processi critici, l'operatore fornisce alla Banca d'Italia e alla Banca centrale europea valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

Principi Generali

La principale finalità perseguita dalla MIFID II (e dalle relative norme di attuazione) è lo sviluppo di un mercato unico dei servizi finanziari in Europa, in cui:

- ❑ siano assicurate la trasparenza e la protezione degli investitori;
- ❑ i risparmiatori possano investire e le imprese di investimento abbiano la facoltà di prestare servizi di investimento a livello transfrontaliero (c.d. "passaporto unico") in modo più semplice e a condizioni identiche in tutti gli Stati dell'Unione;
- ❑ sia rafforzata la tutela degli investitori, prevedendo obblighi più stringenti al fine di garantire i clienti circa il fatto che i prodotti finanziari loro offerti siano adeguati alle loro esigenze e caratteristiche e che i beni nei quali investono siano adeguatamente protetti.

Principi Generali in tema di outsourcing: il Regolamento delegato (UE) 2017/565

Considerando 29 PROCEDURE

È necessario specificare in concreto i requisiti organizzativi e le procedure applicabili alle imprese di investimento che prestano detti servizi o esercitano dette attività. In particolare, è opportuno prevedere procedure rigorose in ambiti quali il controllo della conformità, la gestione del rischio, il trattamento dei reclami, le operazioni personali, l'esternalizzazione e l'individuazione, la gestione e la comunicazione dei conflitti di interesse.

Considerando 36 RISCHI

Ai fini dell'obbligo per le imprese di investimento di adottare, applicare e mantenere una politica di gestione del rischio idonea, i rischi relativi alle attività, ai processi e ai sistemi dell'impresa dovrebbero includere i rischi connessi con l'esternalizzazione di funzioni essenziali o importanti. Tali rischi dovrebbero includere quelli collegati alla relazione tra l'impresa e il fornitore del servizio e i rischi potenziali esistenti qualora le funzioni esternalizzate di più imprese di investimento o di altre entità regolamentate siano concentrate presso un numero limitato di fornitori di servizi.

Principi Generali in tema di outsourcing: il Regolamento delegato (UE) 2017/565

Considerando 43 ESTERNALIZZ. NE

Le autorità competenti non dovrebbero subordinare l'autorizzazione a prestare servizi di investimento o ad esercitare attività di investimento ad un divieto generale di esternalizzazione di una o più funzioni essenziali o importanti. Le imprese di investimento dovrebbero avere la possibilità di esternalizzare tali funzioni, purché gli accordi di esternalizzazione conclusi dall'impresa soddisfino talune **condizioni**.

Considerando 44 NOTIFICA ALL'AUTORITÀ

L'esternalizzazione di servizi o attività di investimento o di funzioni essenziali o importanti può costituire una modifica rilevante delle condizioni cui è subordinata l'autorizzazione dell'impresa di investimento (ai sensi dell'articolo 21, paragrafo 2, della direttiva MIFID II). Se gli accordi di esternalizzazione sono stabiliti dopo che l'impresa di investimento ha ottenuto l'autorizzazione (conformemente al titolo II, capo I, della direttiva Mifid II), tali accordi dovrebbero essere notificati all'autorità competente (nei casi previsti dall'articolo 21, paragrafo 2, della stessa direttiva).

La Direttiva 2014/65/UE (Mifid II)

Art. 16 – par. 2 – Requisiti organizzativi

Le imprese di investimento applicano politiche e procedure sufficienti a garantire che l'impresa, ivi compresi i suoi dirigenti, i suoi dipendenti e gli agenti collegati, adempiano agli obblighi che incombono loro in virtù della presente direttiva nonché alle opportune regole per le operazioni personali di tali persone.

Art. 16 – par. 5 – Requisiti organizzativi

Quando le imprese di investimento affidano ad un terzo l'esecuzione di funzioni operative essenziali ai fini della prestazione di un servizio continuo e soddisfacente ai clienti e dell'esercizio continuo e soddisfacente di attività di investimento, adottano misure ragionevoli per evitare un indebito aggravamento del rischio operativo.

L'affidamento a terzi di funzioni operative importanti non può mettere materialmente a repentaglio la qualità del controllo interno né impedire alle autorità di vigilanza di controllare che le imprese di investimento adempiano a tutti i loro obblighi.

Il Regolamento Congiunto Banca d'Italia/Consob

l'art. 19 del Regolamento Congiunto Banca d'Italia/Consob in materia di organizzazione e procedure degli intermediari che prestano servizi di investimento o di gestione collettiva del risparmio (Provvedimento del 29 ottobre 2007, aggiornato con atto Banca d'Italia/Consob del 19 gennaio 2015 – il “Regolamento Congiunto”) stabilisce che:

- ❑ “quando, nella prestazione dei servizi e delle attività di investimento, gli intermediari affidano ad un terzo l'esecuzione di funzioni operative essenziali o importanti o di servizi o attività di investimento, adottano misure ragionevoli per mitigare i connessi rischi”;
- ❑ “l'esternalizzazione non può ridurre l'efficacia del sistema dei controlli né impedire alle autorità di vigilanza di controllare che gli intermediari adempiano a tutti i loro obblighi”.

Regolamento Delegato (UE) 2017/565

Art. 2 – par. 3 – Definizione di Estermalizzazione

L'art. 2, paragrafo 3, definisce l'"esternalizzazione" come l'accordo in qualsiasi forma tra un'impresa di investimento e un fornitore di servizi in base al quale il fornitore di servizi realizza un processo, un servizio o un'attività che sarebbero altrimenti realizzati dalla stessa impresa di investimento. Tale definizione risulta allineata con quella attualmente prevista dal Regolamento Congiunto, secondo cui per "esternalizzazione" si intende "un accordo in qualsiasi forma tra un intermediario e un fornitore di servizi in base al quale il fornitore realizza un processo, un servizio o un'attività dello stesso intermediario" - cfr. l'art. 2, comma 1, lett. u).

Art. 30: "Gamma delle funzioni essenziali e importanti"

Al paragrafo 1 è previsto che una funzione operativa è considerata essenziale o importante (ai fini del suddetto art. 16, par. 5, comma 1 della direttiva MIFID II) se un'anomalia nella sua esecuzione o la sua mancata esecuzione comprometterebbero gravemente la capacità dell'impresa di investimento di continuare a garantire la conformità alle condizioni e agli obblighi della sua autorizzazione o agli altri obblighi imposti dalla Mifid II oppure ne comprometterebbero gravemente i risultati finanziari o la solidità o la continuità dei servizi e attività di investimento prestati o esercitati. *Tali previsioni risultano in linea con la normativa attualmente vigente di cui all'art. 20 del Regolamento Congiunto.*

Regolamento Delegato (UE) 2017/565

Art. 30: "Gamma delle funzioni essenziali e importanti"

Al paragrafo 2, è previsto inoltre che: Fatto salvo lo status di qualsiasi altra funzione, non sono considerate essenziali o importanti le seguenti funzioni:

- a) la prestazione all'impresa di investimento di servizi di consulenza e di altri servizi che non rientrino nelle sue attività di investimento, ivi compresi:
- la prestazione di consulenza legale all'impresa,
 - la formazione del suo personale,
 - i servizi di fatturazione,
 - la sicurezza dei locali e del personale dell'impresa;
- b) l'acquisto di servizi standardizzati, compresi quelli relativi alla fornitura di informazioni di mercato e di informazioni sui prezzi.

Anche tali previsioni risultano in linea con la normativa attualmente vigente di cui all'art. 20 del Regolamento Congiunto.

Regolamento Delegato (UE) 2017/565

Art. 31, Par. 1:
“Esternalizzazione di funzioni operative essenziali o importanti”
Responsabilità dell'impresa di investimento

Le imprese di investimento che esternalizzano funzioni operative essenziali o importanti restano pienamente responsabili del rispetto di tutti gli obblighi imposti loro dalla Mifid II e devono rispettare in particolare le seguenti condizioni:

- a) l'esternalizzazione non determini la delega della responsabilità da parte dell'alta dirigenza;
- b) non siano alterati il rapporto e gli obblighi dell'impresa di investimento nei confronti dei clienti (a norma della Mifid);
- c) non sia messo a repentaglio il rispetto delle condizioni che l'impresa di investimento deve soddisfare per poter ottenere l'autorizzazione ai sensi della Mifid II (cfr. l'articolo 5 in tema di requisiti per l'autorizzazione) e per conservarla;
- d) non sia soppressa né modificata nessuna delle altre condizioni alle quali è stata subordinata l'autorizzazione dell'impresa.

Tali previsioni risultano in linea con la normativa attualmente vigente di cui all'art. 21, comma 1, del Regolamento Congiunto in tema di condizioni per l'esternalizzazione di funzioni operative essenziali o importanti o di servizi o attività di investimento.

Regolamento Delegato (UE) 2017/565

Art. 31, Par. 2:
**“Esteralizzazione
di funzioni
operative
essenziali o
importanti”
Misure da
adottare**

Le imprese di investimento agiscono con la competenza, la cura e la diligenza dovute quando concludono, applicano o cessano un accordo con il quale esternalizzano ad un fornitore di servizi funzioni operative essenziali o importanti.

Le imprese di investimento devono adottare una serie di misure, necessarie per assicurare che siano soddisfatte talune condizioni, che ricadono sia sul fornitore sia sulla stessa impresa di investimento.

Regolamento Delegato (UE) 2017/565

Art. 31, Par. 2:
**“Esternalizzazione
di funzioni
operative
essenziali o
importanti”
Misure da
adottare:**

**Il Fornitore di
Servizi**

- a) possiede la competenza, la capacità, sufficienti risorse, un'adeguata struttura organizzativa a supporto dell'esecuzione delle funzioni esternalizzate e l'autorizzazione richiesta dalla legge per eseguirle in maniera affidabile e professionale;
- b) esegue i servizi esternalizzati in maniera efficace e in conformità con la normativa e i requisiti vigenti (stabilire metodi e procedure per valutare il livello delle prestazioni del fornitore di servizi e per riesaminare regolarmente i servizi da esso prestati);
- c) sorveglia adeguatamente l'esecuzione delle funzioni esternalizzate e gestisce in modo appropriato i rischi connessi con l'esternalizzazione;
- d) informa l'impresa d'investimento di qualsiasi sviluppo che possa incidere in modo rilevante sulla sua capacità di eseguire le funzioni esternalizzate in maniera efficace e in conformità con la normativa e i requisiti vigenti;
- e) collabora con l'autorità competente dell'impresa di investimento per quanto riguarda le funzioni esternalizzate;
- f) garantisce la protezione delle informaz riservate relative all'impresa di investim e ai suoi clienti;
- g) ha adottato, applicato e mantenuto un piano di emergenza per il ripristino dell'operatività dei sistemi in caso di disastro e la verifica periodica dei dispositivi di backup, quando ciò è necessario in considerazione della funzione, del servizio o dell'attività esternalizzati.

Regolamento Delegato (UE) 2017/565

**Art. 31, Par. 2:
“Esternalizzazione
di funzioni
operative
essenziali o
importanti”
Misure da
adottare:**

**L'Impresa di
Investimento**

- a) ha adottato misure idonee laddove risulti possibile che il fornitore di servizi non esegua le funzioni in maniera efficace e in conformità con la normativa e i requisiti vigenti;
- b) stabilisce i metodi e le procedure per valutare il livello delle prestazioni del fornitore di servizi e per riesaminare regolarmente i servizi da esso prestati;
- c) sorveglia in maniera efficace le funzioni o i servizi esternalizzati e gestisce i rischi associati all'esternalizzazione; a tal fine, mantiene la competenza e le risorse necessarie per sorvegliare le funzioni esternalizzate in maniera efficace e gestire tali rischi;
- d) è in grado, in caso di necessità, di cessare l'accordo di esternalizzazione con effetto immediato qualora ciò sia nell'interesse dei suoi clienti, senza pregiudicare la continuità e qualità della prestazione dei servizi ai clienti;
- e) ha effettivo accesso ai dati relativi alle funzioni esternalizzate e ai locali in cui opera il fornitore di servizi, laddove ciò sia necessario ai fini di condurre un'effettiva sorveglianza;
- f) ha adottato, applicato e mantenuto un piano di emergenza per il ripristino dell'operatività dei sistemi in caso di disastro e la verifica periodica dei dispositivi di backup, quando necessario;
- g) assicura il mantenimento della continuità e qualità delle funzioni o dei servizi esternalizzati anche in caso di cessazione dell'accordo di esternalizzazione, trasferendo le funzioni o i servizi esternalizzati a una terza parte o facendosi carico direttamente della loro esecuzione.

Regolamento Delegato (UE) 2017/565

Art. 31, Par. 2:
**“Esternalizzazione
di funzioni
operative
essenziali o
importanti”
Misure da
adottare:**

**Raffronto con
l'attuale disciplina**

Rispetto all'attuale disciplina (art. 21, comma 2, Regolamento Congiunto), che nella sostanza rimane analoga, si segnala l'inserimento di alcune integrazioni volte ad evidenziare:

- ❑ i profili di carattere organizzativo, atteso che viene specificata: o la necessità di valutare l'adeguatezza del fornitore anche in relazione alla struttura organizzativa dello stesso e alle risorse utilizzate per l'esecuzione delle attività esternalizzate; o l'importanza che l'impresa di investimento mantenga – oltre alla competenza – le risorse necessarie per sorvegliare le funzioni esternalizzate in maniera efficace e gestire tali rischi;
- ❑ la possibilità per l'impresa di investimento di cessare - in caso di necessità - l'accordo di esternalizzazione con effetto immediato qualora ciò sia nell'interesse dei suoi clienti;
- ❑ l'obbligo dell'impresa di investimento di assicurare il mantenimento della continuità e qualità delle funzioni o dei servizi esternalizzati anche in caso di cessazione dell'accordo di esternalizzazione, trasferendo le funzioni o i servizi esternalizzati a una terza parte o facendosi carico direttamente della loro esecuzione;
- ❑ la conformità dell'esecuzione dei servizi esternalizzati da parte del fornitore ed il regolare riesame dei servizi da esso prestati.

Regolamento Delegato (UE) 2017/565

Art. 31, Par. 2:
“Esternalizzazione di funzioni operative essenziali o importanti”
Misure da adottare:

Raffronto con l'attuale disciplina

Gli stessi principi sono in sostanza enunciati anche dalla disciplina relativa ai gestori di fondi di investimento alternativi.

In particolare, l'art. 20 della AIFMD e l'art. 77 del Regolamento UE 2013/231 prevedono:

- la possibilità di revoca con effetto immediato per proteggere gli interessi degli investitori;
- l'obbligo del Gefia (gestori di fondi di investimento alternativi) di riesaminare costantemente i servizi forniti dal delegato;
- la disponibilità da parte del delegato di risorse sufficienti per eseguire i propri compiti;
- la necessità per il Gefia di assicurare che il delegato eserciti le funzioni delegate in modo efficace e nel rispetto dei requisiti di legge e regolamentari applicabili, nonché di stabilire i metodi e le procedure per controllare su base continuativa i servizi forniti dal delegato;
- la necessità che il Gefia disponga costantemente delle conoscenze e delle risorse necessarie per sorvegliare le funzioni delegate;
- l'obbligo del Gefia di assicurare la continuità e la qualità delle funzioni delegate anche in caso di cessazione della delega a seguito del trasferimento delle funzioni delegate o del compito delegato di esercitare le funzioni ad un terzo o dell'esercizio diretto di tali funzioni.

Regolamento Delegato (UE) 2017/565

Art. 31, Par. 3:
**“Esteralizzazione
di funzioni
operative
essenziali o
importanti”**
Diritti e Obblighi

I diritti e gli obblighi rispettivi dell'impresa di investimento e del fornitore di servizi sono specificati e assegnati chiaramente in un **accordo scritto**. Tale principio è coerente con quanto stabilito nella normativa attualmente vigente di cui all'art. 21, comma 4, del Regolamento Congiunto.

Al riguardo, nella nuova disciplina è precisato espressamente che:

- l'impresa di investimento mantiene i suoi diritti di istruzione e cessazione, i suoi diritti di informazione e i suoi diritti di ispezionare e accedere ai registri e ai locali;
- l'accordo garantisce che l'esternalizzazione effettuata dal fornitore di servizi abbia luogo esclusivamente con il consenso scritto dell'impresa di investimento.

Regolamento Delegato (UE) 2017/565

Art. 31:
"Esternalizzazione
di funzioni
operative
essenziali o
importanti"

Par. 4 - Appartenenza allo stesso gruppo

Laddove l'impresa di investimento e il fornitore di servizi siano membri dello stesso gruppo, l'impresa di investimento può, ai fini dell'osservanza della presente normativa, tenere conto della misura in cui controlla il fornitore di servizi o ha la capacità di influenzarne l'operato.

Tale previsione risulta in linea con la normativa attualmente vigente di cui all'art. 21, comma 4, del Regolamento Congiunto.

Par. 5 - Informazioni all'autorità competente

Le imprese di investimento mettono a disposizione dell'autorità competente, su sua richiesta, tutte le informazioni necessarie per permetterle di controllare che le funzioni esternalizzate siano realizzate conformemente ai requisiti della Mifid II e relative misure di esecuzione.

Tale previsione risulta in linea in linea con la normativa attualmente vigente di cui all'art. 21, comma 5, del Regolamento Congiunto.

Regolamento Delegato (UE) 2017/565

Art. 32, Par. 1: “Fornitori di servizi situati in paesi terzi” Condizioni

In aggiunta agli obblighi di cui all'articolo 31, l'impresa di investimento, laddove esternalizzi ad un fornitore di servizi situato in un paese terzo funzioni relative al servizio di investimento di gestione del portafoglio fornito ai clienti, assicura che siano soddisfatte le seguenti condizioni:

- a) il fornitore di servizi è autorizzato o registrato nel suo paese di origine ai fini della prestazione di tale servizio ed è soggetto alla vigilanza efficace di un'autorità competente nel paese terzo;
- b) vige un adeguato accordo di cooperazione tra l'autorità competente dell'impresa di investimento e l'autorità di vigilanza del fornitore di servizi.

Tale principio risulta in linea con la normativa attualmente vigente di cui all'art. 22, comma 1, del Regolamento Congiunto (avente ad oggetto l'“Esternalizzazione del servizio di gestione di portafogli a soggetti extracomunitari”). Peraltro, a livello formale, quest'ultimo articolo fa riferimento alla necessità che fornitore di servizi sia soggetto a forme di vigilanza prudenziale (piuttosto che a una vigilanza efficace di un'autorità competente nel paese terzo).

Regolamento Delegato (UE) 2017/565

Art. 32, Par. 2:
“Fornitori di servizi situati in paesi terzi”
Accordo di cooperazione: garanzie

L'accordo di cooperazione tra le autorità garantisce che l'autorità competente dell'impresa di investimento sia in grado, come minimo, di:

- a) ottenere, su richiesta, le informazioni necessarie a svolgere i suoi compiti di vigilanza a norma della Mifid II e del regolamento (UE) n. 600/2014 (sui mercati degli strumenti finanziari - c.d. MIFIR);
- b) ottenere l'accesso ai documenti utili per lo svolgimento dei suoi compiti di vigilanza conservati nel paese terzo;
- c) ricevere quanto prima dall'autorità di vigilanza del paese terzo le informazioni che le permettono di svolgere indagini su apparenti violazioni dei requisiti stabiliti dalla Mifid II e relative misure di esecuzione e dal regolamento MIFIR;
- d) collaborare ai fini dell'esecuzione, in conformità al diritto nazionale e internazionale applicabile all'autorità di vigilanza del paese terzo e alle autorità competenti nell'Unione, in caso di violazione dei requisiti stabiliti dalla Mifid II e relative misure di esecuzione e dal diritto nazionale pertinente.

Regolamento Delegato (UE) 2017/565

**Art. 32, Par. 3:
“Fornitori di
servizi situati in
paesi terzi”
Accordo di
cooperazione:
elenco**

Le autorità competenti pubblicano sul loro sito internet un elenco delle autorità di vigilanza dei paesi terzi con le quali hanno concluso l'accordo di cooperazione summenzionato (di cui al paragrafo 1, lettera b).

Tale previsione è coerente con quanto stabilito dalla normativa attualmente vigente (di cui all'art. 22, comma 3, del Regolamento Congiunto).

Le autorità competenti aggiornano gli accordi di cooperazione stipulati prima della data di applicazione del Regolamento delegato in esame (il n. 2017/565) entro sei mesi a partire da tale data.

Decreto Legislativo 3 agosto 2017, n. 129

Il Decreto in parola, relativo ai mercati degli strumenti finanziari, fornisce alcune definizioni utili:

- ❑ **"dispositivo di pubblicazione autorizzato" o "APA":** un soggetto autorizzato ai sensi della direttiva 2014/65/UE a pubblicare i report delle operazioni concluse per conto di imprese di investimento ai sensi degli articoli 20 e 21 del regolamento (UE) n. 600/2014;
- ❑ **"fornitore di un sistema consolidato di pubblicazione" o "CTP":** un soggetto autorizzato ai sensi della direttiva 2014/65/UE a fornire il servizio di raccolta presso mercati regolamentati, sistemi multilaterali di negoziazione, sistemi organizzati di negoziazione e APA dei report delle operazioni concluse per gli strumenti finanziari di cui agli articoli 6, 7, 10, 12, 13, 20 e 21 del regolamento (UE) n 600/2014 e di consolidamento delle suddette informazioni in un flusso elettronico di dati aggiornati in continuo, in grado di fornire informazioni sui prezzi e sul volume per ciascuno strumento finanziario;
- ❑ **"meccanismo di segnalazione autorizzato" o "ARM":** un soggetto autorizzato ai sensi della direttiva 2014/65/UE a segnalare le informazioni di dettaglio sulle operazioni concluse alle autorità competenti o all'AESFEM per conto delle imprese di investimento;
- ❑ **"servizi di comunicazione dati":** la gestione di un dispositivo di pubblicazione autorizzato (APA) o di un sistema consolidato di pubblicazione (CTP) o di un meccanismo di segnalazione autorizzato (ARM);
- ❑ **"fornitore di servizi di comunicazione dati":** un APA, un CTP o un ARM.

Regolamento Delegato (UE) 2017/571

Il Regolamento delegato (UE) 2017/571 del 2 giugno 2016 integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione sull'autorizzazione, i requisiti organizzativi e la pubblicazione delle operazioni per i fornitori di servizi di comunicazione dati.

Sono disciplinati i **requisiti** che gli organi di gestione dei fornitori di servizi dovranno possedere: onorabilità, onestà, integrità e indipendenza, nonché conoscenze, competenze ed esperienze adeguate Sono soggetti ad autorizzazione preventiva ai sensi della MIFID II della Consob, in base a quanto previsto dal TUF come modificato dal d. lgs. 129/2017 (per i gestori di mercato: cfr. gli artt. 44 e ss. della MIFID II e i nuovi artt. 64 e ss. del TUF; i per fornitori dei servizi di comunicazione dati: cfr. gli artt. 59 e ss. della MIFID II e i nuovi artt. 79 e ss. del TUF).

Regolamento Delegato (UE) 2017/571

Art. 6: “Requisiti organizzativi per l'esternalizzazione”

Il fornitore di servizi di comunicazione dati:

- se dispone che un terzo esegua attività per suo conto, si accerta che il terzo prestatore di servizi possieda la competenza e la capacità per eseguirle in maniera affidabile e professionale;
- indica le attività destinate all'esternalizzazione specificando l'entità delle risorse umane e tecniche necessarie per eseguirle;
- se esternalizza attività provvede a che l'esternalizzazione non limiti la sua capacità o il suo potere di esercitare le funzioni dell'alta dirigenza o dell'organo di gestione;
- provvede a che il terzo prestatore di servizi collabori con l'autorità competente del fornitore di servizi di comunicazione dati relativamente alle attività esternalizzate;

Regolamento Delegato (UE) 2017/571

Art. 6: “Requisiti organizzativi per l'esternalizzazione”

Il fornitore di servizi di comunicazione dati resta responsabile delle attività esternalizzate e adotta i provvedimenti organizzativi necessari per:

- a) valutare se il terzo prestatore di servizi esegua le attività esternalizzate in maniera efficace e in conformità con i requisiti normativi e regolamentari applicabili e provveda a colmare adeguatamente le carenze riscontrate;
- b) individuare i rischi che si pongono in relazione alle attività esternalizzate e effettuare un adeguato controllo periodico;
- c) sottoporre le attività esternalizzate a procedure adeguate di controllo, anche in termini di effettiva vigilanza sulle attività e sui rischi associati nell'ambito dello stesso fornitore di servizi di comunicazione dati;
- d) assicurare un'adeguata continuità operativa delle attività esternalizzate (valuta la qualità e, se necessario, ne richiede miglioramenti).

Regolamento Delegato (UE) 2017/571

Art. 6: “Requisiti organizzativi per l'esternalizzazione”

Il fornitore di servizi di comunicazione se esternalizza funzioni essenziali comunica all'autorità competente del proprio Stato membro d'origine una serie di dati, ossia:

- a) l'identità del terzo prestatore di servizi;
- b) i provvedimenti organizzativi e le politiche adottati in materia di esternalizzazione e i rischi che questa comporta;
- c) i rapporti interni o esterni sulle attività esternalizzate (posto che una funzione è considerata essenziale se un'anomalia nella sua esecuzione o la sua mancata esecuzione comprometterebbero gravemente la capacità del fornitore di servizi di comunicazione dati di continuare a garantire la conformità alle condizioni e agli obblighi dell'autorizzazione o agli altri obblighi imposti dalla Mifid II).

Regolamento Delegato (UE) 2017/584

Il Regolamento delegato (UE) 2017/584 del 14 luglio 2016 integra la Direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per specificare i requisiti organizzativi delle sedi di negoziazione.

Art. 6, par. 1: “Esternalizzazione e appalti” - Sedi di negoziazione

Le sedi di negoziazione che esternalizzano in tutto o in parte le loro funzioni operative in relazione ai sistemi che consentono o autorizzano la negoziazione algoritmica si assicurano che:

- a) l'accordo di esternalizzazione si riferisca esclusivamente alle funzioni operative e non modifichi le responsabilità dell'alta dirigenza e dell'organo di gestione;
- b) il rapporto e gli obblighi della sede di negoziazione nei confronti dei suoi membri, delle autorità competenti o di terzi, quali i clienti di servizi di fornitura dati, non siano alterati;
- c) soddisfino i requisiti che sono tenute a rispettare per essere autorizzate a norma del titolo III della Mifid II

Requisiti Operativi delle Sedi di negoziazione (art. 65-sexies del TUF)

Disponibilità di sistemi, procedure e meccanismi efficaci atti ad assicurare che i sistemi di negoziazione:

- a) siano resilienti e abbiano capacità sufficiente a gestire i picchi di volume di ordini e messaggi;
- b) siano in grado di garantire negoziazioni ordinate in condizioni di mercato critiche;
- c) siano pienamente testati per garantire il rispetto delle condizioni di cui alle lettere a) e b);
- d) siano soggetti a efficaci disposizioni in materia di continuità operativa per garantire la continuità dei servizi in caso di malfunzionamento.

Disponibilità di sistemi, procedure e meccanismi efficaci:

- a) per garantire che i sistemi algoritmici di negoziazione utilizzati dai membri o partecipanti o clienti non possano creare o contribuire a creare condizioni di negoziazione anormali sulla sede di negoziazione e per gestire qualsiasi condizione di negoziazione anormale causata dagli stessi;
- b) per identificare, attraverso la segnalazione di membri o partecipanti o clienti, gli ordini generati mediante negoziazione algoritmica, i diversi algoritmi utilizzati per la creazione degli ordini e le corrispondenti persone che avviano tali ordini;
- c) per rifiutare gli ordini che eccedono soglie predeterminate di prezzo e volume o sono chiaramente errati

Requisiti Operativi delle Sedi di negoziazione (art. 65-sexies del TUF) - segue

Disponibilità di sistemi, procedure e meccanismi efficaci:

- d) per sospendere o limitare temporaneamente le negoziazioni qualora si registri un'oscillazione significativa nel prezzo di uno strumento finanziario nel mercato gestito o in un mercato correlato in un breve lasso di tempo;
- e) in casi eccezionali, per cancellare, modificare o correggere qualsiasi operazione;
- f) per controllare gli ordini inseriti, incluse le cancellazioni e le operazioni eseguite dai loro membri o partecipanti o clienti, per identificare le violazioni delle regole del sistema, le condizioni di negoziazione anormali o gli atti che possono indicare comportamenti vietati dal regolamento (UE) n. 596/2014 o le disfunzioni del sistema in relazione a uno strumento finanziario

Regolamento Delegato (UE) 2017/584

Art. 6, par. 2:
“Esternalizzazione e appalti” Le funzioni operative

Le funzioni operative comprendono tutte le attività dirette connesse alla performance e alla sorveglianza dei sistemi di negoziazione che supportano i seguenti elementi:

- a) connettività a monte (upstream), capacità di immissione degli ordini, capacità di regolazione e capacità di ripartire l'entrata degli ordini dei clienti tra diversi gateway;
- b) motore di negoziazione per l'abbinamento degli ordini;
- c) connettività a valle (downstream), modifica (edit) degli ordini e delle operazioni e qualsiasi altro tipo di flussi di dati di mercato;
- d) infrastruttura per monitorare la performance degli elementi di cui alle lettere a), b) e c).

Art. 6, par. 2:
“Esternalizzazione e appalti” Misure e condizioni (1/3)

Le sedi di negoziazione documentano il processo di selezione del fornitore di servizi al quale esternalizzare le funzioni operative.

Le sedi di negoziazione devono adottare le misure necessarie per garantire, prima di concludere l'accordo di esternalizzazione e per tutta la sua durata, che siano soddisfatte talune condizioni, che ricadono sia sul fornitore sia sulla stessa sede di negoziazione.

Regolamento Delegato (UE) 2017/584

Art. 6, par. 2: “Esternalizzazione e appalti” Misure e condizioni: il fornitore di servizi (2/3)

- a) disponga delle competenze necessarie per esercitare le funzioni esternalizzate in maniera professionale e affidabile e di tutte le autorizzazioni richieste dalla legge per tali fini;
- b) sorvegli adeguatamente l'esecuzione delle funzioni esternalizzate e gestisca in modo appropriato i rischi connessi con l'accordo di esternalizzazione;
- c) fornisca servizi esternalizzati conformemente alle specifiche dell'accordo di esternalizzazione, che sono basate su metodi predeterminati per la valutazione del livello delle prestazioni del fornitore di servizi, compresi criteri metrici finalizzati a quantificare il servizio fornito e le specifiche dei requisiti che devono essere soddisfatti;
- d) rispetti i requisiti per proteggere le informazioni riservate;
- e) adotti, applichi e mantenga un piano di emergenza per il ripristino dell'operatività dei sistemi in caso di disastro e la verifica periodica dei dispositivi di backup, quando ciò è necessario in considerazione della funzione operativa che è stata esternalizzata;
- f) informi la sede di negoziazione di qualsiasi sviluppo che possa incidere in modo rilevante sulla sua capacità di eseguire le funzioni esternalizzate in maniera efficace e in conformità con i suoi obblighi giuridici;
- g) specifichi nell'accordo i suoi obblighi qualora non sia in grado di fornire i propri servizi, compresa la fornitura del servizio da parte di un'impresa sostitutiva;
- h) collabori con le autorità competenti per quanto riguarda le funzioni esternalizzate.

Regolamento Delegato (UE) 2017/584

Art. 6, par. 2: "Esternalizzazione e appalti" Misure e condizioni: la sede di negoiazione (3/3)

- a) sia in grado di porre termine all'accordo di esternalizzazione, ove necessario, senza che ciò vada a detrimento della continuità e della qualità del servizio alla clientela;
- b) abbia la competenza richiesta per controllare efficacemente le funzioni esternalizzate e per gestire i rischi connessi all'accordo di esternalizzazione;
- c) abbia la capacità di adottare rapidamente misure se il fornitore di servizi non esegue le funzioni in maniera efficace e in conformità con la normativa e i requisiti vigenti;
- d) abbia un accesso effettivo ai dati relativi alle attività esternalizzate e ai locali del fornitore di servizi e i revisori dei conti della sede di negoziazione e le autorità competenti abbiano accesso effettivo ai dati relativi alle attività esternalizzate;
- e) stabilisca i requisiti che devono essere soddisfatti dai fornitori di servizi per proteggere le informazioni riservate relative alla sede di negoziazione e ai suoi membri, e alle informazioni e al software proprietari della sede;
- f) adotti, applichi e mantenga un piano di emergenza per il ripristino dell'operatività dei sistemi in caso di disastro e la verifica periodica dei dispositivi di backup, quando ciò è necessario in considerazione della funzione operativa che è stata esternalizzata;
- g) abbia accesso alle informazioni in relazione alle disposizioni in materia di continuità operativa.

Regolamento Delegato (UE) 2017/584

Art. 6, par. 4: “Esternalizzazione e appalti” Contenuto dell'accordo di esternalizzazione

L'accordo di esternalizzazione è stipulato in forma scritta e contiene:

- a) l'assegnazione dei diritti e degli obblighi al fornitore di servizi e alla sede di negoziazione;
- b) una chiara descrizione dei seguenti elementi:
 - (i) le funzioni operative che sono esternalizzate;
 - (ii) l'accesso della sede di negoziazione ai libri e ai registri del fornitore di servizi;
 - (iii) la procedura per identificare i potenziali conflitti di interesse e porvi rimedio;
 - (iv) la responsabilità assunta da ciascuna parte;
 - (v) la procedura per modificare e porre fine all'accordo;
- c) i mezzi per garantire che sia la sede di negoziazione che il fornitore di servizi agevolino in tutti i modi necessari l'esercizio da parte delle autorità competenti dei loro poteri di vigilanza.

Regolamento Delegato (UE) 2017/584

Art. 6, par. 5 e 6: “Esternalizzazione e appalti” Comunicazione all’Autorità

Le sedi di negoziazione comunicano alle autorità competenti la loro intenzione di esternalizzare funzioni operative nei seguenti casi:

- a) se il fornitore di servizi presta lo stesso servizio ad altre sedi di negoziazione;
- b) se vengono esternalizzate funzioni operative essenziali necessarie per la continuazione dell'attività, nel qual caso le sedi di negoziazione chiedono un'autorizzazione preliminare all'autorità competente (rientrano tra le funzioni operative essenziali tutte le funzioni necessarie per conformarsi agli obblighi di cui all'articolo 47, paragrafo 1, lettere b), c) ed e), della Mifid II).

Le sedi di negoziazione informano le autorità competenti degli accordi di esternalizzazione non soggetti all'obbligo di autorizzazione preliminare immediatamente dopo la firma dell'accordo.

La disciplina dell'esternalizzazione ai sensi della Mifid II

Regolamento Delegato (UE) 2017/593

La Direttiva delegata UE n. 2017/593 del 7 aprile 2016 integra la direttiva MIFID II per quanto riguarda la salvaguardia degli strumenti finanziari e dei fondi dei clienti, gli obblighi di governance dei prodotti e le regole applicabili per la fornitura o ricezione di onorari, commissioni o benefici monetari o non monetari.

**Art. 2, comma 5:
“Salvaguardia
degli strumenti
finanziari e dei
fondi dei clienti”**

Gli Stati membri devono prescrivere che le imprese di investimento rendano tempestivamente disponibili le informazioni relative agli strumenti finanziari e ai fondi ad una serie di soggetti ivi specificati (quali le autorità competenti, i curatori fallimentari designati e i responsabili per la risoluzione di enti in dissesto) specificando che devono essere messe a disposizione anche informazioni dettagliate sui terzi che svolgono eventuali attività correlate (esternalizzate) e sulle eventuali attività esternalizzate.

Decreto Legislativo 3 agosto 2017, n. 129 (attuazione della Mifid II)

L'art. 2 dello schema di Decreto contiene le modifiche che si rendono necessarie per l'attuazione della MIFID II e per l'adeguamento del TUF al regolamento MIFIR, operando un riordino delle disposizioni in materia di intermediari. In particolare, tra i vari interventi apportati al TUF, viene modificato l'art. 6 del TUF e vengono introdotti gli articoli 6-bis e 6-ter, tutti volti a disciplinare i «poteri» delle Autorità di Vigilanza, ossia:

- poteri regolamentari;
- poteri informativi e di indagine;
- poteri ispettivi.

D.lgs. di attuazione della Mifid II – Poteri Regolamentari

All'art. 6, comma 1, del TUF viene introdotta la lettera c-bis), con la conseguenza che sarà compito della Banca d'Italia, sentita la Consob, disciplinare con regolamento anche gli obblighi dei soggetti abilitati relativi alla prestazione dei servizi e delle attività di investimento e alla gestione collettiva del risparmio, in materia di:

...

8) esternalizzazione di funzioni operative essenziali o importanti o di servizi o di attività.

D.lgs. di attuazione della Mifid II – Poteri Informativi e di Indagine

Viene introdotto nel TUF l'art. 6-bis, il quale dispone, tra l'altro, che:

- ❑ la Banca d'Italia può chiedere la comunicazione di dati e notizie e la trasmissione di atti e documenti (con le modalità e nei termini dalla stessa stabiliti) anche a coloro ai quali i soggetti abilitati abbiano esternalizzato funzioni aziendali essenziali o importanti e al loro personale (in linea con quanto previsto dall'art. dall'art. 69, comma 2, lettere a), b), d), g) e r) della Direttiva MIFID II);
- ❑ la Consob può:
 - a) chiedere a chiunque la comunicazione di dati e notizie e la trasmissione di atti e documenti con le modalità e nei termini dalla stessa stabiliti, che possano essere pertinenti ai fini dell'esercizio della propria funzione di vigilanza;
 - b) procedere ad audizione personale nei confronti di chiunque possa essere in possesso di informazioni pertinenti.

D.lgs. di attuazione della Mifid II – Poteri Ispettivi

Viene introdotto nel TUF l'art. 6-ter, che stabilisce, tra l'altro, che la Banca d'Italia e la Consob possono, nell'ambito delle rispettive competenze e nel rispetto delle disposizioni normative europee, effettuare ispezioni e richiedere l'esibizione dei documenti e il compimento degli atti ritenuti necessari nei confronti dei soggetti abilitati e di coloro ai quali i soggetti abilitati abbiano esternalizzato funzioni aziendali essenziali o importanti e al loro personale.

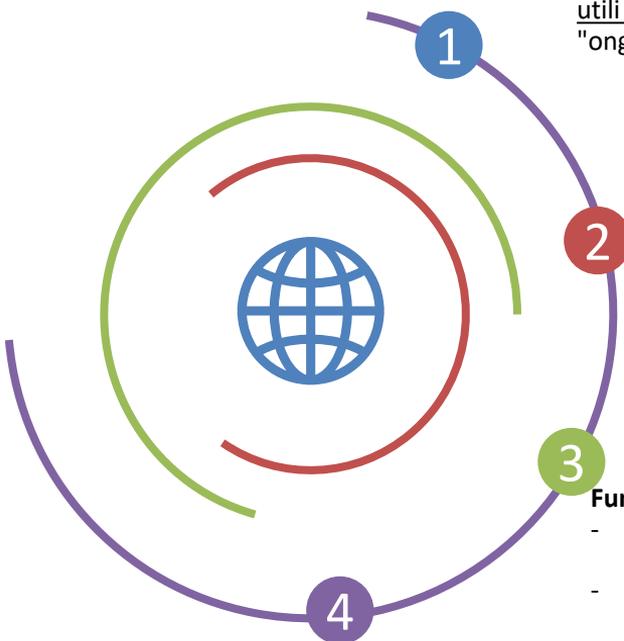
La Consob può avvalersi della Guardia di Finanza che esegue gli accertamenti richiesti agendo con i poteri di indagine ad essa attribuiti ai fini dell'accertamento dell'IVA e delle imposte sui redditi.

D.lgs. di attuazione della Mifid II – Sanzioni amministrative pecuniarie

L'art. 5 dello schema di decreto in esame modifica l'art. 190 del TUF (da rubricare "Sanzioni amministrative pecuniarie in tema di disciplina degli intermediari", anziché "Altre sanzioni amministrative pecuniarie in tema di disciplina degli intermediari e dei mercati") ed include anche i soggetti ai quali sono state esternalizzate funzioni operative essenziali o importanti tra i destinatari delle sanzioni amministrative pecuniarie stabilite dal comma 1.

L'importo di dette sanzioni pecuniarie varia da € trentamila ad € cinque milioni ovvero fino al 10% del fatturato, quando tale importo è superiore a € cinque milioni e il fatturato è determinabile ai sensi dell'articolo 195, per l'inosservanza delle norme ivi indicate (tra cui gli artt. 6, 6-bis e 6-ter del TUF).

Approccio verso l'Esternalizzazione



Sistema IT

Identificazione e valutazione delle possibili soluzioni IT che facilitino il processo di raccolta delle informazioni utili al popolamento del registro delle esternalizzazioni ed ottimizzino il relativo processo di aggiornamento "ongoing".

Governance

Analisi critica della governance, allo scopo di identificare e formalizzare:

- il posizionamento del presidio di outsourcing con individuazione di possibili configurazioni organizzative
- i ruoli e le responsabilità della Capogruppo, delle Legal Entity, delle funzioni di controllo e dei diversi attori coinvolti nel processo, con indicazione dei flussi informativi rilevanti e delle necessità di reporting
- il processo di outsourcing nelle sue diverse fasi, analizzando le modalità operative in essere al fine di delineare un piano di azione per assicurare la conformità alle nuove disposizioni nei termini previsti
- la normativa interna conformemente alle nuove disposizioni EBA.

Legale

Supporto, in fase e durante i due anni di transition period, alle attività di revisione ed adeguamento dei contratti di outsourcing sulla base dei nuovi requisiti.

Funzioni di Controllo

- Definizione di un framework di gestione dei rischi derivanti dagli accordi di outsourcing, con particolare riferimento alle funzioni di controllo impattate
- Verifica della conformità delle attuali metodologie di valutazione dei rischi alle nuove disposizioni EBA in materia di outsourcing
- Supporto nell'individuazione delle appropriate metodologie di misurazione dei rischi e nell'attuazione dei risk assessment.

Processo per le esternalizzazioni: analisi pre-outsourcing

Supervisory Conditions

- Il service provider è autorizzato da, o registrato presso, un'autorità competente a svolgere l'attività bancaria o a fornire servizi di pagamento
- Il service provider è autorizzato a svolgere tali attività in accordo con il quadro normativo nazionale di riferimento
- Esiste un adeguato accordo di cooperazione tra le Autorità di vigilanza responsabili della supervisione delle banche e quelle di supervisione del service provider (in caso quest'ultimo sia situato in un paese terzo)

Valutazione dei rischi

- Valutare tutti i rischi ed i relativi impatti derivanti dagli accordi di outsourcing quali, ad esempio, rischio operativo, rischio di concentrazione, rischio reputazionale, rischio legale, rischio di step-in,
- La valutazione dei rischi deve includere specifici scenari, regolarmente aggiornati e adeguatamente riportati al management

Due Diligence

- Verificare che il service provider abbia le appropriate e sufficienti competenze, capacità, risorse e struttura organizzativa per svolgere la funzione critica o importante in maniera affidabile e professionale.

Contratti

- Tutti gli accordi devono essere formalizzati in apposti contratti. Tra gli altri, sono indicati i seguenti contenuti minimi per l'esternalizzazione di CIF:
 - eventuali clausole relative alla possibilità di sub-esternalizzare funzioni critiche o importanti
 - diritti di accesso, informazione e audit
 - obblighi informativi da parte del service provider nei confronti dell'istituto
 - livelli di servizio (SLA) e target di performance (KPI)

Processo per le esternalizzazioni: monitoraggio

Supervisione Funzioni
esternalizzate

- Monitoraggio dell'outsourcer su base continuativa secondo un approccio risk based, con particolare attenzione alle funzioni critiche o importanti
- La valutazione dei rischi deve essere periodicamente aggiornata e riportata al management
- Performance e qualità dell'outsourcer devono essere quantificate e stabilite attraverso KPI, KCI, auto certificazioni e verifiche indipendenti.

Exit Strategy

- Definizione delle exit strategy per tutti gli accordi di outsourcing di funzioni critiche o importanti. Tali strategie devono tenere conto di tutti i potenziali rischi e prevedere la possibilità di risoluzione dell'accordo di outsourcing nel caso di fallimento del service provider e/o deterioramento rilevante del servizio prestato

Obblighi di informative
vs il Regulator

- L'istituto deve fornire, ove richiesto dalle Autorità competenti, il registro di tutti gli accordi di outsourcing esistenti secondo un formato dati comune
- L'istituto deve tempestivamente informare le autorità competenti relativamente agli accordi di outsourcing di funzioni critiche o importanti pianificati.

Considerazioni conclusive

Stante quanto illustrato in precedenza, le indicazioni fornite dall'EBA nell'ambito delle Linee Guida avranno un impatto significativo per i destinatari delle stesse, imponendo una revisione/ rafforzamento del framework attualmente adottato dai destinatari.

In particolare, le istituzioni bancarie dovranno innanzitutto intervenire sulla Politica aziendale in materia di esternalizzazione di funzioni/attività aziendali e sui relativi processi sottostanti, allineando le previsioni esistenti ai principi espressi dalle Guidelines, provvedendo altresì all'implementazione del Registro relativo ai contratti di outsourcing, che comporterà la necessità di definirne e formalizzarne i contenuti, al fine di strutturare uno strumento in linea con i desiderata espressi dall'EBA.

In tale ambito, in considerazione delle nuove previsioni relative alla definizione di strategie di uscita connesse ad ogni contratto di esternalizzazione di funzioni critiche o importanti, sarà inoltre necessario eseguire accurate valutazioni sul fornitore e relativi competitor, al fine di individuare i principali rischi connessi.

Sarà inoltre necessario recepire e formalizzare, sia nei contratti di futura stipula sia nei contratti già in essere (a partire dalla prima data di rinnovo), gli elementi/requisiti minimi richiesti dall'Autorità.

E' importante sottolineare come le previsioni in oggetto abbiano un impatto rilevante su quelle istituzioni finanziarie non già destinatarie di accurate e puntuali disposizioni regolamentari connesse all'ambito delle esternalizzazioni, che saranno pertanto chiamate a rafforzare sensibilmente il proprio framework interno in materia.

Carlo **ARLOTTA**
Partner
Mob. +39 340 73.11.380
carlo.arlotta@consiliabm.com

Gianluca **POTENZA**
Senior Manager
Mob. +39 334 11.62.711
gianluca.potenza@consiliabm.com

Margherita **SINGARELLI**
Senior Consultant
Mob. +39 334 31.77.310
margherita.singarelli@consiliabm.com



Vincenzo **DE RISI**
Partner
Mob. +39 349 67.15.524
vincenzo.derisi@consiliabm.com

Valentina **PIRO**
Senior Manager
Mob. +39 366 62.75.860
valentina.piro@consiliabm.com

Maria Cristina **SANTORO**
Consultant
Mob. +39 334 34.33.295
mariacristina.santoro@consiliabm.com

 **CBM**

CONSILIA
Business Management

Corso Europa, 13
20122 Milano
www.consiliabm.com



+39 02 87389370



segreteria@consiliabm.com
Info@consiliabm.com