30/09/2025
ESMA65-294529287-4737

Orientamenti

in materia di esternalizzazione a fornitori di servizi cloud

Indice

1 Ambito di applicazione

Destinatari

1. I presenti orientamenti si applicano alle autorità competenti e i) ai depositari di fondi di investimento alternativi (FIA) di cui all'articolo 21, paragrafo 3, lettera c), e all'articolo 21, paragrafo 3, terzo comma, della direttiva sui GEFIA, qualora non siano entità finanziarie alle quali si applica il DORA, e ii) ai depositari di OICVM di cui all'articolo 23, paragrafo 2, lettera c), della direttiva OICVM, se non sono entità finanziarie alle quali si applica il DORA.[1]

Oggetto

2. I presenti orientamenti si applicano in relazione alle seguenti disposizioni:

   a) Con riferimento ai depositari di FIA: articolo 21 della direttiva sui GEFIA; articolo 98 del regolamento delegato (UE) 2013/231 della Commissione;

   b) Con riferimento ai depositari di OICVM: articoli 22, 22 bis e 23, paragrafo 2, della direttiva OICVM; articolo 32 della direttiva 2010/43/UE della Commissione; Articolo 2, paragrafo 2, lettera j), articolo 3, paragrafo 1, articolo 13, paragrafo 2, articoli 15, 16 e 22 del regolamento delegato (UE) 2016/438 della Commissione.

Tempistica

3. I presenti orientamenti si applicano a decorrere dalla data della loro pubblicazione sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE e a tutti gli accordi di esternalizzazione tramite cloud conclusi, rinnovati o modificati a tale data o successivamente.

4. In applicazione del Regolamento (UE) 2022/2554 (DORA), i precedenti orientamenti dell'ESMA sull'esternalizzazione a fornitori di servizi cloud non si applicano più alle entità finanziarie soggette al DORA, come definite all'articolo 2 del medesimo regolamento.Per i depositari di FIA e per i depositari di OICVM di cui al paragrafo 1, i precedenti orientamenti dell'ESMA sull'esternalizzazione a fornitori di servizi cloud continueranno ad applicarsi fino alla data di pubblicazione dei presenti orientamenti sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE.

[1] Con riferimento agli accordi di esternalizzazione nel cloud, le entità finanziarie definite all'articolo 2, paragrafi 1 e 2 del Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (Regolamento DORA), sono soggette alle norme specifiche stabilite nel Regolamento DORA e nei regolamenti delegati e di esecuzione della Commissione.

2 Riferimenti normativi, abbreviazioni e definizioni

2.1 Riferimenti normativi

Regolamento ESMA	Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione ([2]).
GEFIA	Direttiva 2011/61/UE del Parlamento europeo e del Consiglio, dell'8 giugno 2011, sui gestori di fondi di investimento alternativi, che modifica le direttive 2003/41/CE e 2009/65/CE e i regolamenti (CE) n. 1060/2009 e (UE) n. 1095/2010 ([3]).
Regolamento delegato (UE) 2013/231 della Commissione	Regolamento delegato (UE) 2013/231 della Commissione, del 19 dicembre 2012, che integra la direttiva 2011/61/UE del Parlamento europeo e del Consiglio per quanto riguarda deroghe, condizioni generali di esercizio, depositari, leva finanziaria, trasparenza e sorveglianza ([4]).
Direttiva OICVM	Direttiva 2009/65/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di taluni organismi d'investimento collettivo in valori mobiliari (OICVM) ([5]).
Direttiva 2010/43/UE della Commissione	Direttiva 2010/43/UE della Commissione, del 1º luglio 2010, recante modalità di esecuzione della direttiva 2009/65/CE del Parlamento europeo e del Consiglio per quanto riguarda i requisiti organizzativi, i conflitti di interesse, le regole di condotta, la gestione del rischio e il contenuto dell'accordo tra il depositario e la società di gestione ([6]).
DORA	Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza

([2]) GU L 331 del 15.12.2010, pag. 84
([3]) GU L 174 dell'1.7.2011, pag. 1.
([4]) GU L 83 del 22.3.2013, pag. 1.
([5]) GU L 302 del 17.11.2009, pag. 32.
([6]) GU L 176 del 10.7.2010, pag. 42.

	operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011[7]
RGPD	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ([8]).

2.2 Abbreviazioni

ESMA	Autorità europea degli strumenti finanziari e dei mercati
Fornitore	Fornitore di servizi cloud
UE	Unione europea

2.3 Definizioni

Funzione	Qualsiasi processo, servizio o attività.
Funzione essenziale o importante	Qualunque funzione la cui difficoltà o mancata esecuzione comprometterebbero gravemente: a) il rispetto, da parte di un'impresa, degli obblighi che le incombono a norma della legislazione applicabile; b) la performance finanziaria di un'impresa; o c) la solidità o la continuità dei servizi e delle attività principali di un'impresa.
Servizi cloud	Servizi forniti utilizzando il cloud computing.
Cloud computing o cloud ([9])	Un paradigma che consente l'accesso in rete a un insieme scalabile ed elastico di risorse fisiche o virtuali condivisibili (ad esempio server, sistemi operativi, reti,

([7]) *GU L 333 del 27.12.2022, pag. 1.*
([8]) GU L 119 del 4.5.2016, pagg. 1-88.
([9]) Il cloud computing è spesso abbreviato in «cloud». Nel resto del documento viene utilizzato il termine «cloud» per facilità di riferimento.

	software, applicazioni e dispositivi di memorizzazione) con fornitura autonoma e amministrazione su richiesta.
Fornitore di servizi cloud	Una terza parte che fornisce servizi cloud nell'ambito di un accordo di esternalizzazione nel cloud.
Accordo di esternalizzazione nel cloud	Accordo di qualsiasi forma, compresi gli accordi di delega, tra: (i) un'impresa e un fornitore di servizi cloud (o fornitore) mediante il quale il fornitore stesso svolge una funzione che altrimenti sarebbe svolta dall'impresa stessa; o (ii) un'impresa e una terza parte, diversa da un fornitore di servizi cloud, che fa ricorso in misura significativa a un fornitore per svolgere una funzione che altrimenti sarebbe svolta dall'impresa stessa. In questo caso, il riferimento a un «fornitore di servizi cloud» nei presenti orientamenti dovrebbe essere inteso come riferimento a tale terza parte.
Subesternalizzazione	Una situazione in cui il fornitore di servizi cloud trasferisce ulteriormente la funzione esternalizzata (o parte di essa) a un altro fornitore di servizi nell'ambito di un accordo di esternalizzazione.
Modello di implementazione del cloud	Il modo in cui il cloud può essere organizzato sulla base del controllo e della condivisione di risorse fisiche o virtuali. I modelli di implementazione del cloud comprendono cloud di comunità ([10]), ibridi ([11]), privati ([12]) e pubblici ([13]).
Imprese	a) depositari di cui all'articolo 21, paragrafo 3, lettera c), e all'articolo 21, paragrafo 3, terzo comma, della direttiva

([10]) Un modello di implementazione del cloud in cui i servizi cloud sono riservati esclusivamente a uno specifico gruppo di clienti (e da questi condivisi), i quali hanno esigenze comuni e una relazione tra loro, e in cui le risorse sono controllate da almeno un membro di tale gruppo.
([11]) Un modello di implementazione del cloud che utilizza almeno due diversi modelli.
([12]) Un modello di implementazione del cloud in cui i servizi cloud sono utilizzati esclusivamente da un unico cliente di servizi cloud che ne controlla le risorse.
([13]) Un modello di implementazione del cloud in cui i servizi cloud sono potenzialmente disponibili a qualunque cliente di servizi cloud mentre le risorse sono controllate dal fornitore di servizi cloud.

sui GEFIA ("depositari di fondi di investimento alternativi (FIA)");

b) depositari di cui all'articolo 23, paragrafo 2, lettera c), della direttiva OICVM ("depositari di OICVM").

3 Scopo

5. I presenti orientamenti sono emanati ai sensi dell'articolo 16, paragrafo 1, del regolamento ESMA, con la finalità di istituire prassi di vigilanza coerenti, efficienti ed efficaci nell'ambito del Sistema europeo di vigilanza finanziaria (SEVIF) e di garantire un'applicazione comune, uniforme e coerente dei requisiti di cui alla sezione 1.1 «Oggetto» in cui le imprese esternalizzano i servizi ai fornitori. In particolare, gli orientamenti intendono aiutare le imprese e le autorità competenti a individuare, affrontare e monitorare i rischi e le sfide derivanti dagli accordi di esternalizzazione nel cloud, che vanno dalla presa di decisione di esternalizzare, selezione di un fornitore di servizi cloud, monitoraggio delle attività esternalizzate fino alla previsione di strategie di uscita.

4 Conformità e obblighi di comunicazione

4.1 Status degli orientamenti

6. Ai sensi dell'articolo 16, paragrafo 3, del regolamento ESMA, le autorità e le imprese competenti compiono ogni sforzo per conformarsi agli orientamenti.

7. Le autorità competenti alle quali si applicano i presenti orientamenti dovrebbero conformarvisi integrandoli nei propri quadri giuridici e/o di vigilanza nazionali, a seconda dei casi, anche laddove vi siano orientamenti specifici diretti principalmente alle imprese. In questo caso, le autorità competenti dovrebbero far sì che, esercitando la facoltà di vigilanza, le imprese si conformino agli orientamenti.

4.2 Obblighi di comunicazione

8. Entro due mesi dalla data di pubblicazione degli orientamenti sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE, le autorità competenti alle quali si applicano i presenti orientamenti devono notificare all'ESMA se i) sono conformi, ii) non sono conformi, ma intendono conformarsi, o iii) non sono conformi e non intendono conformarsi agli orientamenti.

9. In caso di non conformità, le autorità competenti devono inoltre notificare all'ESMA, entro due mesi dalla data di pubblicazione degli orientamenti sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE, i motivi per cui non rispettano tali orientamenti. Sul sito web

dell'ESMA è disponibile un modello di notifica che, una volta compilato, è trasmesso all'Autorità stessa.

10. Le imprese non sono tenute a comunicare la propria conformità ai presenti orientamenti.

5 Orientamenti in materia di esternalizzazione a fornitori di servizi cloud

Orientamento 1. Governance, sorveglianza e documentazione

11. Un'impresa dovrebbe disporre di una strategia di esternalizzazione del cloud definita e aggiornata che sia coerente con le pertinenti strategie e con le politiche e i processi interni dell'impresa, anche in relazione alle tecnologie dell'informazione e della comunicazione, alla sicurezza delle informazioni e alla gestione del rischio operativo.

12. Un'impresa dovrebbe:

    a) assegnare precise responsabilità per quanto concerne la documentazione, la gestione e il controllo degli accordi di esternalizzazione nel cloud all'interno della propria organizzazione;
    b) stanziare risorse sufficienti per garantire il rispetto dei presenti orientamenti e di tutte le disposizioni di legge applicabili ai propri accordi di esternalizzazione nel cloud;
    c) istituire una funzione di sorveglianza delle attività di esternalizzazione nel cloud o designare membri del personale di grado elevato che rispondano direttamente all'organo di gestione e incaricati della gestione e della supervisione dei rischi legati agli accordi di esternalizzazione nel cloud. Nel conformarsi ai presenti orientamenti, le imprese dovrebbero tenere conto della natura, delle dimensioni e della complessità della propria attività, anche in termini di rischio per il sistema finanziario, e dei rischi inerenti alle funzioni esternalizzate, nonché accertarsi che il proprio organo di gestione disponga delle competenze tecniche pertinenti per comprendere i rischi inerenti agli accordi di esternalizzazione nel cloud. Le imprese di piccole dimensioni e quelle meno complesse dovrebbero almeno garantire una chiara divisione dei compiti e delle responsabilità per la gestione e la sorveglianza degli accordi di esternalizzazione nel cloud.

13. Un'impresa dovrebbe monitorare lo svolgimento delle attività, le misure di sicurezza e il rispetto dei livelli di servizio concordati da parte dei propri fornitori di servizi cloud. Tale monitoraggio dovrebbe essere basato sul rischio, con particolare riguardo alle funzioni essenziali o importanti esternalizzate.

14. Un'impresa dovrebbe accertarsi periodicamente se i propri accordi di esternalizzazione nel cloud riguardano una funzione essenziale o importante ed effettuare una rivalutazione

ogniqualvolta il rischio, la natura o la portata di una funzione esternalizzata siano stati sottoposti a cambiamenti sostanziali.

15. Un'impresa dovrebbe tenere un registro aggiornato delle informazioni su tutti gli accordi di esternalizzazione nel cloud che la stessa ha stipulato, operando una distinzione tra esternalizzazione di funzioni essenziali o importanti e accordi di esternalizzazione di altro tipo. Nel distinguere tra l'esternalizzazione di funzioni essenziali o importanti e accordi di esternalizzazione di altro tipo, essa dovrebbe fornire una sintesi dei motivi per i quali la funzione esternalizzata è o non è considerata essenziale o importante. Tenendo conto del diritto nazionale, un'impresa dovrebbe inoltre conservare per un ragionevole periodo di tempo un registro degli accordi di esternalizzazione nel cloud conclusi.

16. Per gli accordi di esternalizzazione nel cloud riguardanti funzioni essenziali o importanti, il registro dovrebbe includere almeno le seguenti informazioni per ciascun accordo in questione:

    a) un numero di riferimento;
    b) la data di inizio e, se pertinente, la successiva data di rinnovo del contratto, la data di scadenza e/o i termini di preavviso per il fornitore di servizi cloud e per l'impresa;
    c) una breve descrizione della funzione esternalizzata, compresi i dati esternalizzati e se tali dati comprendono dati personali (ad esempio indicando «sì» o «no» in un campo a parte dove inserire queste informazioni);
    d) una categoria assegnata dall'impresa che rifletta la natura della funzione esternalizzata (ad esempio funzione di tecnologia dell'informazione, funzione di controllo), che dovrebbe facilitare l'identificazione dei diversi tipi di accordi di esternalizzazione nel cloud;
    e) se la funzione esternalizzata prevede attività operative aventi carattere d'urgenza;
    f) il nome e il marchio (ove pertinente) del fornitore di servizi cloud, il paese di registrazione, il numero di registrazione della società, l'identificativo della persona giuridica (se disponibile), l'indirizzo registrato, i contatti pertinenti e la denominazione dell'eventuale società madre;
    g) il diritto che disciplina l'accordo di esternalizzazione nel cloud e, se disponibile, la scelta della giurisdizione;
    h) il tipo di servizi cloud e di modelli di implementazione e la natura specifica dei dati da conservare, nonché i luoghi (regioni o paesi) in cui tali dati possono essere conservati;
    i) la data dell'ultima valutazione dell'essenzialità o dell'importanza della funzione esternalizzata e la data della prossima valutazione prevista;
    j) la data dell'ultima valutazione dei rischi/dell'audit del fornitore, unitamente a una breve sintesi dei principali risultati, e la data della prossima valutazione dei rischi/del prossimo audit;
    k) la persona fisica o l'organo decisionale, all'interno dell'impresa, che ha approvato l'accordo di esternalizzazione nel cloud;

l) ove applicabile, i nomi di tutti i subesternalizzatori ai quali è subesternalizzata una funzione essenziale o importante (o parti sostanziali della stessa), compresi i paesi dove sono registrati i subesternalizzatori, nei quali sarà prestato il servizio subesternalizzato, e le località (ossia regioni o paesi) presso le quali saranno conservati i dati;
m) il costo di bilancio annuale stimato dell'accordo di esternalizzazione nel cloud.

17. Per gli accordi di esternalizzazione nel cloud riguardanti funzioni non essenziali o non importanti, un'impresa dovrebbe definire le informazioni da includere nel registro in base alla natura, all'entità e alla complessità dei rischi inerenti alla funzione esternalizzata.

Orientamento 2. Analisi di pre-esternalizzazione e due diligence

18. Prima di concludere qualsiasi accordo di esternalizzazione nel cloud, un'impresa dovrebbe:

a) valutare se l'accordo di esternalizzazione nel cloud riguardi una funzione essenziale o importante;
b) individuare e valutare tutti i rischi relativi all'accordo di esternalizzazione nel cloud;
c) effettuare con due diligence alcune verifiche sul futuro fornitore di servizi cloud;
d) individuare e valutare eventuali conflitti di interesse che l'esternalizzazione potrebbe comportare.

19. L'analisi di pre-esternalizzazione e la due diligence riguardanti il potenziale fornitore di servizi cloud dovrebbero essere proporzionate alla natura, alle dimensioni e alla complessità della funzione che l'impresa intende esternalizzare e ai rischi inerenti a tale funzione. Dovrebbero comprendere almeno una valutazione dell'impatto potenziale dell'accordo di esternalizzazione nel cloud sui rischi operativi, giuridici, di conformità e reputazionali dell'impresa.

20. Nel caso in cui l'accordo di esternalizzazione nel cloud riguardi funzioni essenziali o importanti, l'impresa dovrebbe altresì:

a) valutare tutti i rischi rilevanti derivabili dall'accordo di esternalizzazione nel cloud, compresi i rischi relativi alle tecnologie dell'informazione e della comunicazione, alla sicurezza delle informazioni, alla continuità operativa, alla normativa e alla conformità; i rischi reputazionali, i rischi operativi e le eventuali limitazioni della sorveglianza per l'impresa, derivanti da quanto segue:
    i. il servizio cloud selezionato e i modelli di implementazione proposti;
    ii. la migrazione e/o i processi di implementazione;
    iii. il carattere sensibile della funzione e la riservatezza dei relativi dati di cui si prevede l'esternalizzazione e le misure di sicurezza che dovrebbero essere adottate;

iv. l'interoperabilità dei sistemi e delle applicazioni dell'impresa e del fornitore, in particolare la loro capacità di scambiare informazioni e di utilizzare reciprocamente le informazioni oggetto di scambio;

v. la portabilità dei dati dell'impresa, segnatamente la capacità di trasferire facilmente i dati dell'impresa da un fornitore di servizi cloud a un altro o di ritrasferirli all'impresa;

vi. la stabilità politica, la situazione della sicurezza e il sistema giuridico (comprese le disposizioni vigenti in materia di applicazione della legislazione, le disposizioni del diritto fallimentare applicabili in caso di dissesto del fornitore di servizi cloud, le leggi sulla protezione dei dati in vigore e se sono soddisfatte le condizioni per il trasferimento dei dati personali a un paese terzo ai sensi del RGPD) dei paesi (all'interno o all'esterno dell'UE) nei quali saranno espletate le funzioni esternalizzate e dove verranno conservati i dati esternalizzati; in caso di subesternalizzazione, i rischi aggiuntivi che possono presentarsi se il subesternalizzatore è ubicato in un paese terzo o in un paese diverso dal fornitore di servizi cloud e, nel caso di una catena di subesternalizzazione, eventuali rischi aggiuntivi, anche in relazione all'assenza di un contratto diretto tra l'impresa e il subesternalizzatore che svolge la funzione esternalizzata;

vii. possibile concentrazione all'interno dell'impresa (anche, laddove applicabile, a livello del rispettivo gruppo) causata da molteplici accordi di esternalizzazione nel cloud con lo stesso fornitore e da una possibile concentrazione all'interno del settore finanziario dell'UE, causata da più imprese che si avvalgono dello stesso fornitore di servizi cloud o di un piccolo gruppo di fornitori di servizi cloud. Nel valutare il rischio di concentrazione, l'impresa dovrebbe tenere conto di tutti i propri accordi di esternalizzazione nel cloud (e, ove applicabile, degli accordi di esternalizzazione nel cloud a livello del gruppo) con il fornitore in questione;

b) dovrebbe tenere conto dei benefici e dei costi attesi dell'accordo di esternalizzazione nel cloud, compresa la valutazione di eventuali rischi significativi che possono essere ridotti o gestiti meglio in relazione ai rischi significativi che possono presentarsi per effetto dell'accordo di esternalizzazione nel cloud.

21. In caso di esternalizzazione di funzioni essenziali o importanti, la due diligence dovrebbe includere una valutazione dell'idoneità del fornitore di servizi cloud. Nell'effettuare tale valutazione, un'impresa dovrebbe garantire che quest'ultimo possieda la reputazione commerciale, le competenze, le risorse (comprese quelle umane, informatiche e finanziarie), la struttura organizzativa e, se applicabile, la o le pertinenti autorizzazioni o registrazioni per svolgere la funzione essenziale o importante in modo affidabile e professionale e per adempiere ai propri obblighi per tutta la durata dell'accordo di

esternalizzazione nel cloud. Ulteriori fattori da prendere in considerazione nell'effettuare la due diligence su un fornitore di servizi cloud comprendono, tra l'altro:

a) la gestione della sicurezza delle informazioni, in particolare la protezione dei dati personali, riservati o comunque sensibili;
b) l'assistenza tecnica, compresi i piani e i contatti di assistenza nonché i processi di gestione degli incidenti;
c) la continuità operativa e i piani di ripristino in caso di disastro.

22. A seconda dei casi, e al fine di favorire la due diligence, un'impresa può anche utilizzare certificazioni basate su norme internazionali e relazioni di audit esterno o interno.

23. Se un'impresa viene a conoscenza di lacune significative e/o di modifiche sostanziali in relazione ai servizi forniti o alla situazione del fornitore di servizi cloud, l'analisi di pre-esternalizzazione e la due diligence dovrebbero essere riviste senza indugio o effettuate nuovamente se necessario.

24. Nel caso in cui un'impresa concluda un nuovo accordo o ne rinnovi uno esistente con un fornitore di servizi cloud che è già stato valutato, essa dovrà determinare, seguendo un approccio basato sul rischio, se è necessario ricorrere a una nuova due diligence.

Orientamento 3. Principali elementi contrattuali

25. I diritti e gli obblighi rispettivi di un'impresa e del suo fornitore di servizi cloud dovrebbero essere indicati in modo chiaro in un accordo scritto.

26. L'accordo scritto dovrebbe prevedere espressamente la possibilità per l'impresa di risolverlo, se necessario.

27. In caso di esternalizzazione di funzioni essenziali o importanti, l'accordo scritto dovrebbe comprendere almeno:

a) una descrizione chiara della funzione esternalizzata;
b) la data di inizio e la data di fine, ove applicabile, dell'accordo e i termini di preavviso per il fornitore di servizi cloud e per l'impresa;
c) la legislazione che disciplina l'accordo e, a seconda dei casi, la scelta della giurisdizione;
d) gli obblighi finanziari dell'impresa e del fornitore di servizi cloud;
e) se è consentita la subesternalizzazione e, in caso affermativo, a quali condizioni, tenuto conto dell'orientamento 7;
f) l'ubicazione o le ubicazioni (regioni o paesi) nelle quali sarà espletata la funzione esternalizzata e dove i dati saranno trattati e conservati, nonché le condizioni da

soddisfare, compreso l'obbligo d'informare l'impresa se il fornitore di servizi cloud propone di cambiare l'ubicazione o le ubicazioni;

g) disposizioni relative alla sicurezza delle informazioni e alla protezione dei dati personali, tenendo conto dell'orientamento 4;

h) il diritto dell'impresa di monitorare periodicamente le prestazioni del fornitore di servizi cloud nell'ambito dell'accordo di esternalizzazione nel cloud, tenendo conto dell'orientamento 6;

i) i livelli di servizio concordati, per i quali dovrebbero essere previsti precisi obiettivi di performance, sia quantitativi che qualitativi, in modo da consentire un monitoraggio tempestivo che permetta di adottare senza indebiti ritardi le opportune azioni correttive in caso di mancato raggiungimento dei livelli di servizio concordati;

j) gli obblighi di comunicazione del fornitore di servizi cloud nei confronti dell'impresa, compresi, ove opportuno, l'obbligo di presentare relazioni pertinenti per la funzione di sicurezza dell'impresa e le funzioni principali quali, ad esempio, le relazioni redatte dalla funzione di audit interno del fornitore di servizi cloud;

k) disposizioni relative alla gestione degli incidenti da parte del fornitore di servizi cloud, compreso l'obbligo per quest'ultimo di riferire all'impresa senza indebito ritardo gli incidenti che hanno inciso sul funzionamento del servizio esternalizzato dall'impresa;

l) una clausola che indichi se il fornitore di servizi cloud debba stipulare un'assicurazione obbligatoria contro determinati rischi e, ove applicabile, il livello di copertura assicurativa richiesto;

m) i requisiti per l'attuazione e la verifica da parte del fornitore di servizi cloud dei piani di continuità operativa e di ripristino in caso di disastro;

n) l'obbligo per il fornitore di servizi cloud di concedere all'impresa, alle sue autorità competenti e a qualsiasi altra persona designata dall'impresa o dalle autorità competenti il diritto di accedere («diritti di accesso») e di ispezionare («diritti di audit») le informazioni, i locali, i sistemi e i dispositivi pertinenti del fornitore di servizi cloud nella misura necessaria a monitorarne le prestazioni nel quadro dell'accordo di esternalizzazione nel cloud e la sua conformità ai requisiti normativi e contrattuali applicabili, tenendo conto dell'orientamento 6;

o) disposizioni volte a garantire che i dati che il fornitore di servizi cloud elabora o memorizza per conto dell'impresa possano essere consultati, recuperati e restituiti all'impresa in funzione delle necessità, tenendo conto dell'orientamento 5.

Orientamento 4. Sicurezza delle informazioni

28. Un'impresa dovrebbe stabilire requisiti di sicurezza delle informazioni nelle proprie politiche e procedure interne e nell'ambito dell'accordo scritto di esternalizzazione nel cloud e monitorare il rispetto di tali requisiti su base continuativa, anche per proteggere i dati riservati, personali o comunque sensibili. Tali requisiti dovrebbero essere proporzionati alla natura, alle dimensioni e alla complessità della funzione che l'impresa esternalizza al fornitore di servizi cloud e ai rischi inerenti a tale funzione.

29. A tal fine, in caso di esternalizzazione di funzioni essenziali o importanti, e fatti salvi i requisiti applicabili a norma del RGPD, un'impresa che applichi un approccio basato sul rischio dovrebbe quanto meno:

    a) *organizzazione della sicurezza delle informazioni:* garantire che vi sia una chiara ripartizione dei ruoli e delle responsabilità riguardo alla sicurezza delle informazioni tra l'impresa e il fornitore di servizi cloud, anche in relazione all'individuazione delle minacce, alla gestione degli incidenti e delle patch, e garantire che il fornitore di servizi cloud sia in grado di svolgere efficacemente i propri ruoli e le proprie responsabilità;
    b) *gestione dell'identità e dell'accesso*: garantire l'esistenza di solidi meccanismi di autenticazione (ad esempio l'autenticazione multifattoriale) e di controllo degli accessi al fine di impedire l'accesso non autorizzato ai dati dell'impresa e alle risorse cloud back-end;
    c) *crittografia e gestione delle chiavi:* garantire che siano utilizzate le tecnologie di crittografia del caso, ove necessario, per i dati in transito, i dati in memoria, i dati a riposo e i back up di dati, unitamente ad adeguate soluzioni di gestione delle chiavi per limitare il rischio di accesso non autorizzato alle chiavi di crittografia; in particolare, l'impresa dovrebbe prendere in considerazione la tecnologia e i processi più avanzati al momento di scegliere la propria soluzione di gestione delle chiavi;
    d) *sicurezza delle operazioni e della rete:* prendere in considerazione livelli adeguati di disponibilità della rete, separazione della rete [ad esempio, isolamento del tenant nell'ambiente condiviso del cloud, separazione operativa per quanto riguarda il web, la logica applicativa, il sistema operativo, la rete, il sistema di gestione di base di dati (DBMS) e i livelli di archiviazione] e ambienti di elaborazione (ad esempio test, test di accettazione degli utenti, sviluppo, produzione);
    e) *interfacce per programmi applicativi (API):* prendere in considerazione meccanismi per l'integrazione dei servizi cloud con i sistemi dell'impresa, per garantire la sicurezza delle API (ad esempio istituendo e mantenendo politiche e procedure in materia di sicurezza delle informazioni per le API in interfacce multisistema, giurisdizioni e funzioni operative per impedire la divulgazione, la modifica o la distruzione non autorizzate dei dati);

f) *continuità operativa e ripristino in caso di disastro:* garantire che siano posti in essere controlli efficaci della continuità operativa e del ripristino in caso di disastro (ad esempio stabilendo requisiti minimi di capacità, selezionando opzioni di hosting con una certa copertura geografica, con la possibilità di passare dall'una all'altra, oppure richiedendo e rivedendo la documentazione recante il percorso di trasporto dei dati dell'impresa tra i sistemi del fornitore di servizi cloud, nonché prendendo in considerazione la possibilità di replicare le immagini delle macchine presso una sede di archiviazione indipendente, sufficientemente distante dalla rete o posta offline);
g) *ubicazione dei dati*: adottare un approccio basato sul rischio per l'archiviazione e l'ubicazione o le ubicazioni del trattamento dei dati (regioni o paesi);
h) *conformità e monitoraggio*: verificare che il fornitore di servizi cloud osservi le norme riconosciute a livello internazionale in materia di sicurezza delle informazioni e abbia attuato adeguati controlli sulla sicurezza delle informazioni (ad esempio chiedendo al fornitore di dimostrare che effettua le pertinenti analisi della sicurezza delle informazioni ed effettuando valutazioni e prove periodiche per quanto concerne le misure che ha predisposto per garantire la sicurezza delle informazioni).

Orientamento 5. Strategie di uscita

30. In caso di esternalizzazione di funzioni essenziali o importanti, l'impresa dovrebbe garantire di essere in grado di recedere dall'accordo di esternalizzazione nel cloud senza indebite interruzioni delle proprie attività e dei propri servizi ai clienti e senza pregiudicare il rispetto degli obblighi che le incombono a norma della legislazione applicabile, nonché la riservatezza, l'integrità e la disponibilità dei propri dati. A tal fine, l'impresa dovrebbe:

a) elaborare piani di uscita che siano esaustivi, documentati e sufficientemente collaudati. Tali piani dovrebbero essere aggiornati secondo necessità, anche in caso di modifiche della funzione esternalizzata;
b) individuare soluzioni alternative ed elaborare piani di transizione affinché la funzione e i dati esternalizzati siano rimossi al fornitore di servizi cloud e, ove applicabile, da eventuali subesternalizzatori, e trasferirli al fornitore di servizi cloud sostitutivo indicato dall'impresa o reintegrarli in seno all'impresa stessa. Tali soluzioni dovrebbero essere definite tenendo conto dei problemi che possono sorgere dall'ubicazione dei dati, adottando le misure del caso per assicurare la continuità operativa durante la fase di transizione;
c) garantire che l'accordo scritto di esternalizzazione nel cloud preveda l'obbligo per il fornitore di servizi cloud di sostenere il trasferimento ordinato della funzione esternalizzata, e il relativo trattamento dei dati, dal fornitore stesso e da eventuali subesternalizzatori a un altro fornitore di servizi cloud indicato dall'impresa o direttamente all'impresa, nel caso in cui quest'ultima attivi la strategia di uscita. L'obbligo di sostenere il trasferimento ordinato della funzione esternalizzata e il

relativo trattamento dei dati dovrebbe comprendere, laddove pertinente, l'eliminazione sicura dei dati dai sistemi del fornitore di servizi cloud e di eventuali subesternalizzatori.

31. Nell'elaborare i piani di uscita e le soluzioni di cui alle precedenti lettere a) e b) («strategia di uscita»), l'impresa dovrebbe considerare quanto segue:

    a) definire gli obiettivi della strategia di uscita;
    b) definire gli eventi che potrebbero attivare la strategia di uscita. Tali misure dovrebbero comprendere almeno la cessazione dell'accordo di esternalizzazione nel cloud su iniziativa dell'impresa o del fornitore di servizi cloud e il dissesto o altra grave interruzione dell'attività operativa del fornitore di servizi cloud;
    c) effettuare un'analisi d'impatto aziendale proporzionata alla funzione esternalizzata, al fine di individuare le risorse umane e le altre risorse necessarie per l'eventuale attuazione della strategia di uscita;
    d) assegnare ruoli e responsabilità per la gestione della strategia di uscita;
    e) verificare l'adeguatezza della strategia di uscita utilizzando un approccio basato sul rischio (ad esempio, effettuando un'analisi dei potenziali costi, impatti, risorse e implicazioni in termini di tempo del trasferimento di un servizio esternalizzato a un fornitore alternativo);
    f) definire i criteri positivi della transizione.

32. Un'impresa dovrebbe includere indicatori degli eventi scatenanti della strategia di uscita nel monitoraggio e nella sorveglianza continui dei servizi resi dal fornitore di servizi cloud nell'ambito dell'accordo di esternalizzazione nel cloud.

Orientamento 6. Diritti di accesso e di audit

33. Un'impresa dovrebbe garantire che l'accordo scritto di esternalizzazione nel cloud non limiti l'esercizio effettivo, da parte dell'impresa e dell'autorità competente, dei diritti di accesso e di audit e delle possibilità di sorveglianza sul fornitore di servizi cloud.

34. Un'impresa dovrebbe garantire che l'esercizio dei diritti di accesso e di audit (ad esempio la frequenza dell'audit nonché i settori e i servizi da sottoporre ad audit) tenga conto del fatto che l'esternalizzazione sia correlata a una funzione essenziale o importante così come della natura e dell'estensione dei rischi e dell'impatto che l'accordo di esternalizzazione nel cloud comporta per l'impresa.

35. Nel caso in cui l'esercizio dei diritti di accesso o di audit o l'uso di determinate tecniche di audit comportino un rischio per l'ambiente del fornitore di servizi cloud e/o del cliente di un altro fornitore di servizi cloud (ad esempio, incidendo sui livelli di servizio, sulla riservatezza, sull'integrità e sulla disponibilità dei dati), il fornitore dovrebbe fornire all'impresa una chiara motivazione della ragione per cui ciò comporterebbe un rischio e dovrebbe concordare con l'impresa modalità alternative per ottenere un risultato simile

(ad esempio, l'inclusione di controlli specifici da testare in una specifica relazione/certificazione prodotta dal fornitore).

36. Ferma restando la loro responsabilità finale per quanto riguarda gli accordi di esternalizzazione nel cloud, al fine di utilizzare le risorse di audit in modo più efficiente e ridurre gli oneri organizzativi a carico del fornitore di servizi cloud e dei suoi clienti, le imprese potrebbero avvalersi di:

    a) certificazioni di terzi e relazioni di audit esterno o interno messe a disposizione dal fornitore di servizi cloud;
    b) serie di audit svolti congiuntamente con altri clienti dello stesso fornitore di servizi cloud o audit congiunti espletati da un revisore esterno designato da più clienti dello stesso fornitore di servizi cloud.

37. In caso di esternalizzazione di funzioni essenziali o importanti, un'impresa dovrebbe valutare se le certificazioni di terzi e le relazioni di audit esterno o interno di cui al paragrafo 37, lettera a), siano adeguate e sufficienti per ottemperare agli obblighi che le incombono a norma della legislazione applicabile, e dovrebbe mirare a non dipendere esclusivamente da tali certificazioni e relazioni nel corso del tempo.

38. In caso di esternalizzazione di funzioni essenziali o importanti, un'impresa dovrebbe avvalersi delle certificazioni di terzi e delle relazioni di audit esterno o interno di cui al paragrafo 37, lettera a), solo se:

    a) ha accertato che l'ambito delle certificazioni o delle relazioni di audit comprende i sistemi principali del fornitore di servizi cloud (ad esempio, processi, applicazioni, infrastruttura, centri dati), i controlli fondamentali individuati dall'impresa e la conformità agli obblighi di legge pertinenti;
    b) sottopone a valutazione accurata e periodica il contenuto delle certificazioni o relazioni di audit e verifica che non siano obsolete;
    c) assicura che i controlli e i sistemi principali del fornitore siano compresi anche nelle versioni successive della certificazione o della relazione di audit;
    d) è soddisfatta della parte incaricata della certificazione o dell'audit (ad esempio per quanto riguarda le qualifiche, le competenze, la ripetizione/verifica degli elementi concreti contenuti nel fascicolo di audit sottostante e la rotazione della società di certificazione o di audit);
    e) si è sincerata che le certificazioni siano rilasciate e che gli audit siano espletati conformemente a norme pertinenti e che comprendano anche una verifica dell'efficacia dei controlli essenziali in atto;
    f) ha il diritto contrattuale di chiedere l'ampliamento dell'ambito delle certificazioni o delle relazioni di audit per includervi taluni sistemi e controlli rilevanti del fornitore di servizi cloud; il numero e la frequenza di tali richieste di modifica dell'ambito dovrebbero essere ragionevoli e giustificati in un'ottica di gestione dei rischi;
    g) conserva il diritto contrattuale di effettuare audit individuali in loco a sua discrezione in relazione alla funzione esternalizzata.

39. L'impresa dovrebbe garantire che, prima di una visita in loco, anche da parte di un terzo designato dall'impresa (ad esempio un revisore), il fornitore di servizi cloud riceva un preavviso entro un periodo di tempo ragionevole, a meno che una notifica preventiva anticipata non sia possibile a causa di una situazione di emergenza o di crisi o comporti una situazione in cui l'audit non sarebbe più efficace. Tale preavviso dovrebbe includere il luogo, lo scopo della visita e il personale che vi parteciperà.

40. Considerando che i servizi cloud presentano un elevato livello di complessità tecnica e sollevano specifiche questioni giurisdizionali, il personale che effettua l'audit, ossia i revisori interni dell'impresa o i revisori che agiscono per suo conto, dovrebbero possedere le giuste competenze e conoscenze per valutare adeguatamente i servizi cloud in questione ed effettuare un audit efficace e pertinente. Ciò dovrebbe valere anche per il personale delle imprese che esamina le certificazioni o le relazioni di audit messe a disposizione dal fornitore di servizi cloud.

Orientamento 7. Subesternalizzazione

41. Se è consentita la subesternalizzazione di funzioni essenziali o importanti (o gran parte di esse), il contratto scritto di esternalizzazione nel cloud tra l'impresa e il fornitore di servizi cloud dovrebbe:

    a) specificare le parti o gli aspetti della funzione esternalizzata che sono esclusi dalla potenziale subesternalizzazione;
    b) indicare le condizioni da rispettare in caso di subesternalizzazione;
    c) specificare che il fornitore di servizi cloud è ritenuto responsabile ed è tenuto alla vigilanza dei servizi che ha subesternalizzato per garantire che tutti gli obblighi contrattuali tra il fornitore di servizi cloud e l'azienda siano continuamente rispettati;
    d) includere l'obbligo per il fornitore di servizi cloud di notificare all'impresa l'intenzione di subesternalizzare, o di apportarvi modifiche sostanziali, in particolare qualora ciò possa incidere sulla capacità del fornitore di servizi cloud di adempiere agli obblighi assunti nei confronti dell'impresa nell'ambito dell'accordo di esternalizzazione nel cloud. Il periodo di notifica stabilito nell'accordo scritto dovrebbe consentire all'impresa un periodo di tempo sufficiente almeno per effettuare una valutazione del rischio della subesternalizzazione proposta o delle relative modifiche sostanziali e per sollevare obiezioni o approvarle esplicitamente, come indicato alla lettera e);
    e) garantire che l'impresa abbia il diritto di opporsi alla subesternalizzazione prevista, o a modifiche sostanziali della stessa, o che sia necessaria un'approvazione esplicita prima che la subesternalizzazione proposta o le modifiche sostanziali abbiano efficacia;
    f) garantire che l'impresa abbia il diritto contrattuale di porre fine all'accordo di esternalizzazione nel cloud con il fornitore di servizi cloud nel caso in cui contesti la subesternalizzazione proposta o le modifiche sostanziali dello stesso e in caso di subesternalizzazione indebita (ad esempio se il fornitore di servizi cloud procede

con la subesternalizzazione senza informarne l'impresa o viola gravemente le condizioni di subesternalizzazione specificate nell'accordo di esternalizzazione).

42. L'impresa dovrebbe garantire che il fornitore di servizi cloud supervisioni adeguatamente il subesternalizzatore.

Orientamento 8. Notifica scritta alle autorità competenti

43. L'impresa dovrebbe notificare per iscritto alla propria autorità competente in tempo utile i previsti accordi di esternalizzazione nel cloud che riguardano una funzione essenziale o importante. L'impresa dovrebbe inoltre notificare tempestivamente e per iscritto alla propria autorità competente gli accordi di esternalizzazione nel cloud che riguardano una funzione precedentemente classificata come non essenziale o non importante e che in seguito è divenuta essenziale o importante.

44. La notifica scritta dell'impresa dovrebbe includere, tenendo conto del principio di proporzionalità, quanto meno le informazioni seguenti:

    a) la data di inizio del contratto di esternalizzazione nel cloud e, ove pertinente, la successiva data di rinnovo del contratto, la data di scadenza e/o i termini di preavviso per il fornitore di servizi cloud e per l'impresa;
    b) una breve descrizione della funzione esternalizzata;
    c) una breve sintesi delle ragioni per cui la funzione esternalizzata è considerata essenziale o importante;
    d) il nome e il marchio (eventualmente) del fornitore di servizi cloud, il paese di registrazione, il numero di registrazione della società, l'identificativo della persona giuridica (se disponibile), la sede legale, i contatti principali e il nome dell'eventuale società madre;
    e) la legge applicabile all'accordo di esternalizzazione nel cloud e, ove pertinente, la scelta della giurisdizione;
    f) i modelli di implementazione del cloud e la natura specifica dei dati che il fornitore di servizi cloud deve conservare, nonché le ubicazioni (regioni o paesi) dove tali dati saranno conservati;
    g) la data dell'ultima valutazione dell'essenzialità o dell'importanza della funzione esternalizzata;
    h) la data dell'ultima valutazione del rischio o dell'audit del fornitore di servizi cloud, unitamente a una breve sintesi dei principali risultati, e la data della valutazione dei rischi o audit successivi previsti;
    i) la persona fisica o l'organo decisionale, all'interno dell'impresa, che ha approvato l'accordo di esternalizzazione nel cloud;
    j) ove opportuno, i nomi di eventuali subesternalizzatori cui sono affidate parti sostanziali di una funzione essenziale o importante, compresi il paese o la regione dove i subesternalizzatori sono registrati, il luogo in cui sarà prestato il servizio subesternalizzato e saranno conservati i dati.

Orientamento 9. Supervisione degli accordi di esternalizzazione nel cloud

45. Le autorità competenti dovrebbero valutare, nell'ambito del loro processo di vigilanza, gli accordi delle imprese riguardanti l'esternalizzazione nel cloud. In particolare, tale valutazione dovrebbe concentrarsi sugli accordi relativi all'esternalizzazione di funzioni essenziali o importanti.

46. Le autorità competenti dovrebbero accertarsi di essere in grado di esercitare una vigilanza efficace, in particolare quando le imprese esternalizzano funzioni essenziali o importanti che sono svolte al di fuori dell'UE.

47. Le autorità competenti dovrebbero valutare, sulla base di un approccio basato sul rischio, se le imprese:

    a) dispongono della governance, delle risorse e dei processi operativi pertinenti per concludere, attuare e sorvegliare in modo adeguato ed efficace gli accordi di esternalizzazione nel cloud;
    b) individuare e gestire tutti i rischi pertinenti connessi all'esternalizzazione nel cloud.

48. Qualora siano individuati rischi di concentrazione, le autorità competenti dovrebbero monitorare l'evoluzione di tali rischi e valutarne il potenziale impatto sulle altre imprese soggette alla propria vigilanza e la stabilità del mercato finanziario.