EIOPA-BoS-20-002

Orientamenti in materia di esternalizzazione a fornitori di servizi cloud

Indice

Introduzione

1. Conformemente all'articolo 16 del regolamento (UE) n. 1094/2010[1], l'EIOPA emana orientamenti per fornire alle imprese di assicurazione e di riassicurazione una guida sulle modalità di applicazione delle disposizioni in materia di esternalizzazione di cui alla direttiva 2009/138/CE[2] ("direttiva solvibilità II") e al regolamento delegato (UE) 2015/35[3] della Commissione ("regolamento delegato") in caso di esternalizzazione a fornitori di servizi cloud.
2. I presenti orientamenti si basano sull'articolo 13, paragrafo 28, sull'articolo 38 e sull'articolo 49 della direttiva solvibilità II nonché sull'articolo 274 del regolamento delegato. Essi si basano, inoltre, sulle guide fornite dagli orientamenti dell'EIOPA sul sistema di governance (EIOPA-BoS-14/253).
3. Gli orientamenti sono rivolti alle autorità competenti, alle quali forniscono una guida su come le imprese di assicurazione e di riassicurazione (collettivamente "imprese") dovrebbero applicare i requisiti in materia di esternalizzazione previsti negli atti giuridici di cui sopra nel contesto dell'esternalizzazione a fornitori di servizi cloud.
4. Gli orientamenti si applicano sia alle singole imprese sia, *mutatis mutandis*, ai gruppi[4].

   Le entità soggette ad altri requisiti settoriali, che fanno parte di un gruppo, sono escluse dal campo di applicazione dei presenti orientamenti a livello individuale in quanto devono rispettare i requisiti settoriali specifici nonché i pertinenti orientamenti forniti dall'Autorità europea degli strumenti finanziari e dei mercati e dall'Autorità bancaria europea.
5. In caso di esternalizzazione infragruppo e subesternalizzazione a fornitori di servizi cloud, i presenti orientamenti dovrebbero essere applicati unitamente alle disposizioni degli orientamenti EIOPA sul sistema di governance in materia di esternalizzazione infragruppo.
6. Nel rispettare questi orientamenti o nel vigilare sul rispetto degli stessi, le imprese e le autorità competenti dovrebbero tenere conto del principio di proporzionalità[5] e della crucialità o dell'importanza del servizio esternalizzato a fornitori di servizi cloud. Il principio di proporzionalità dovrebbe garantire che gli accordi di governance, compresi quelli relativi all'esternalizzazione a fornitori di servizi cloud, siano proporzionati alla natura, alla portata e alla complessità dei rischi sottostanti.
7. I presenti orientamenti dovrebbero essere letti unitamente agli orientamenti dell'EIOPA sul sistema di governance e agli obblighi normativi di cui al paragrafo 1, che rimangono impregiudicati.

Definizioni

8. Se non definiti nei presenti orientamenti, i termini assumono il significato definito negli atti giuridici citati nell'introduzione.

---

[1] Regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/79/CE della Commissione (GU L 331 del 15.12.2010, pag. 48).

[2] Direttiva 2009/138/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 335 del 17.12.2009, pag. 1).

[3] Regolamento delegato 2015/35 della Commissione, del 10 ottobre 2014, che integra la direttiva 2009/138/CE del Parlamento europeo e del Consiglio in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 12 del 17.1.2015, pag. 1).

[4] Articolo 212, paragrafo 1, della direttiva solvibilità II.

[5] Articolo 29, paragrafo 3, della direttiva solvibilità II.

9. Inoltre, ai fini dei presenti orientamenti, valgono le definizioni elencate di seguito.

Fornitore di servizi	un terzo che svolge in tutto o in parte un processo, un servizio o un'attività nell'ambito di un accordo di esternalizzazione.
Fornitore di servizi cloud	un fornitore di servizi, come sopra definito, responsabile della fornitura di servizi cloud nell'ambito di un accordo di esternalizzazione.
Servizi cloud	servizi forniti tramite cloud computing, ossia un modello che consente l'accesso in rete diffuso, pratico e su richiesta a un gruppo condiviso di risorse elettroniche configurabili (ad esempio, reti, server, memorie, applicazioni e servizi), che possono essere forniti e messi a disposizione rapidamente con un minimo di impegno gestionale o di interazione con il fornitore del servizio.
Cloud pubblico	infrastruttura cloud disponibile per l'utilizzo da parte della generalità degli utenti..
Cloud privato	infrastruttura cloud disponibile per l'utilizzo esclusivo da parte di una sola impresa.
Cloud di comunità	infrastruttura cloud disponibile per l'utilizzo esclusivo da parte di una specifica comunità di imprese, ad esempio diverse imprese appartenenti a un unico gruppo.
Cloud ibrido	infrastruttura cloud costituita da due o più infrastrutture cloud distinte.

Data di applicazione

10. I presenti orientamenti si applicano a partire dal 1ºgennaio 2021 a tutti gli accordi di esternalizzazione nel cloud stipulati o modificati in tale data o successivamente.

11. Le imprese dovrebbero rivedere e modificare di conseguenza gli esistenti accordi di esternalizzazione nel cloud relativi a funzioni o attività operative essenziali o importanti, al fine di garantire la conformità ai presenti orientamenti entro il 31 dicembre 2022.

12. Qualora il riesame degli accordi di esternalizzazione nel cloud di funzioni essenziali o importanti non sia concluso entro il 31 dicembre 2022, l'impresa dovrebbe informare di tale circostanza la propria autorità di vigilanza[6], segnalando altresì le misure previste per completare il riesame o l'eventuale strategia di uscita. Se del caso, l'autorità di vigilanza può concordare con l'impresa un termine più lungo per il completamento di tale riesame.

13. L'aggiornamento (ove necessario) delle politiche e dei processi interni dell'impresa dovrebbe essere effettuato entro il 1º gennaio 2021, mentre gli obblighi in materia di documentazione per gli accordi di esternalizzazione nel cloud relativi a funzioni o attività operative essenziali o importanti dovrebbero essere adempiuti entro il 31 dicembre 2022.

[6] Articolo 13, paragrafo 10, della direttiva solvibilità II.

Orientamento 1 – Servizi cloud ed esternalizzazioni

14. L'impresa dovrebbe stabilire se un accordo con un fornitore di servizi cloud rientra nella definizione di esternalizzazione ai sensi della direttiva solvibilità II. Nell'ambito di tale valutazione occorre considerare:

a. se la funzione o l'attività operativa esternalizzata (o parte di essa) è svolta in modo ricorrente o continuativo; e

b. se tale funzione o attività operativa (o parte di essa) rientrerebbe in genere nell'ambito delle funzioni o attività operative che l'impresa svolgerebbe o potrebbe svolgere nel corso delle sue normali attività operative, anche nel caso in cui l'impresa non abbia svolto tale funzione o attività operativa in passato.

15. Se un accordo con un fornitore di servizi riguarda molteplici funzioni o attività operative, l'impresa dovrebbe esaminare tutti gli aspetti dell'accordo nella sua valutazione.

16. Nei casi in cui l'impresa esternalizza funzioni o attività operative a fornitori di servizi che non sono fornitori di servizi cloud ma fanno, in modo significativo, ricorso a infrastrutture cloud per fornire i propri servizi (ad esempio, se il fornitore di servizi cloud fa parte di una catena di subesternalizzazione), l'accordo per tale esternalizzazione rientra nell'ambito di applicazione dei presenti orientamenti.

Orientamento 2 – Principi generali di governance per l'esternalizzazione nel cloud

17. Fatto salvo l'articolo 274, paragrafo 3, del regolamento delegato, l'organo amministrativo, direttivo o di vigilanza dell'impresa ("OADV") dovrebbe garantire che qualsiasi decisione di esternalizzare funzioni o attività operative essenziali o importanti a fornitori di servizi cloud si basi su un'approfondita valutazione dei rischi, compresi tutti i rischi pertinenti derivanti dall'accordo quali le tecnologie dell'informazione e della comunicazione ("information and communication technology, ICT"), la continuità operativa, gli aspetti giuridici e di conformità alle norme, la concentrazione, altri rischi operativi e i rischi associati alla migrazione dei dati e/o alla fase di implementazione, se del caso.

18. In caso di esternalizzazione a fornitori di servizi cloud di funzioni o attività operative essenziali o importanti, l'impresa, ove opportuno, dovrebbe riportare le modifiche del proprio profilo di rischio derivanti dai suoi accordi di esternalizzazione nel cloud nella propria valutazione del rischio e della solvibilità ("ORSA").

19. L'uso di servizi cloud dovrebbe essere coerente con le strategie dell'impresa (ad esempio, strategia ICT, strategia sulla sicurezza delle informazioni, strategia di gestione del rischio operativo) e con le politiche e i processi interni, che vanno aggiornati, se necessario.

Orientamento 3 – Aggiornamento della politica scritta di esternalizzazione

20. In caso di esternalizzazione a fornitori di servizi cloud, l'impresa dovrebbe aggiornare la politica scritta di esternalizzazione (ad esempio, rivedendola, aggiungendo un'appendice separata o elaborando nuove politiche dedicate) e le altre politiche interne pertinenti (ad esempio, la sicurezza delle informazioni), tenendo conto delle specificità dell'esternalizzazione cloud almeno nelle seguenti aree:

a. i ruoli e le responsabilità delle funzioni dell'impresa interessata, in particolare l'OADV, e delle funzioni responsabili delle ICT, della sicurezza delle

informazioni, della conformità alle norme, della gestione dei rischi e dell'audit interno;

b. i processi e le procedure di comunicazione necessari per l'approvazione, l'attuazione, il monitoraggio, la gestione e il rinnovo, se del caso, degli accordi di esternalizzazione nel cloud relativi a funzioni o attività operative essenziali o importanti;

c. la sorveglianza dei servizi cloud proporzionata alla natura, alla portata e alla complessità dei rischi inerenti ai servizi forniti, tra cui i) la valutazione del rischio degli accordi di esternalizzazione nel cloud e i controlli di *due diligence* sui fornitori di servizi cloud, compresa la frequenza della valutazione del rischio; ii) il monitoraggio e i controlli di gestione (ad esempio, verifica dell'accordo sul livello dei servizi); iii) standard e controlli di sicurezza;

d. per quanto riguarda l'esternalizzazione nel cloud di funzioni o attività operative essenziali o importanti, si dovrebbe fare riferimento agli obblighi contrattuali descritti nell'orientamento 10;

e. i requisiti inerenti alla documentazione e la notificazione scritta all'autorità di vigilanza relativamente alle esternalizzazioni cloud di funzioni o attività operative essenziali o importanti;

f. per quel che riguarda ciascun accordo di esternalizzazione cloud che include funzioni o attività operative essenziali o importanti, l'obbligo di una "strategia di uscita" documentata e, se del caso, sufficientemente collaudata, proporzionata alla natura, alla portata e alla complessità dei rischi inerenti ai servizi forniti. La strategia di uscita può contemplare una serie di procedure di risoluzione contrattuale, tra cui sospendere, reintegrare o trasferire i servizi previsti nell'accordo di esternalizzazione nel cloud.

Orientamento 4 – Notifica scritta all'autorità di vigilanza

21. Gli obblighi di notificazione scritta di cui all'articolo 49, paragrafo 3, della direttiva solvibilità II, e ulteriormente dettagliati negli orientamenti EIOPA sul sistema di governance, si applicano a tutte le esternalizzazioni a fornitori di servizi cloud di funzioni e attività operative essenziali o importanti. Nel caso in cui una funzione o un'attività operativa esternalizzata precedentemente classificata come non essenziale o non importante diventi essenziale o importante, l'impresa dovrebbe informarne l'autorità di vigilanza.

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

a. una breve descrizione della funzione o dell'attività operativa esternalizzata;

b. la data di inizio e, se applicable, 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. la legislazione che disciplina il contratto di esternalizzazione cloud;

d. il nome del fornitore di servizi cloud, il numero di registrazione dell'impresa, l'identificativo della persona giuridica (se disponibile), l'indirizzo della sede legale e altri recapiti del caso, nonché il nome dell'eventuale impresa madre; e in caso di gruppi, se il fornitore di servizi cloud fa parte o meno del gruppo;

e. i modelli di servizi cloud e di implementazione del cloud, ossia pubblico/privato/ibrido/di comunità, nonché la natura specifica dei dati da conservare e i luoghi (paesi o regioni) in cui tali dati saranno conservati;

f. una breve sintesi delle ragioni per cui la funzione o l'attività operativa esternalizzata è considerata essenziale o importante;

g. la data dell'ultima valutazione dell'essenzialitào dell'importanza della funzione o dell'attività esternalizzata.

Orientamento 5 – Requisiti documentali

23. Nell'ambito del proprio sistema di governance e di gestione dei rischi, l'impresa dovrebbe tenere traccia dei suoi accordi di esternalizzazione nel cloud, ad esempio in forma di un registro dedicato tenuto aggiornato nel tempo. L'impresa dovrebbe inoltre tenere traccia degli accordi di esternalizzazione cloud già risolti per un adeguato periodo di conservazione soggetto alla normativa nazionale.

24. In caso di esternalizzazione di funzioni o attività operative essenziali o importanti, l'impresa dovrebbe registrare tutte le informazioni seguenti:

a. le informazioni da notificare all'autorità di vigilanza di cui all'orientamento 4;

b. nel caso di gruppi, le imprese di assicurazione o riassicurazione e le altre imprese rientranti nell'ambito del consolidamento prudenziale che si avvalgono dei servizi cloud;

c. la data dell'ultima valutazione dei rischi e una breve sintesi dei principali risultati;

d. la persona fisica o l'organo decisionale (ad esempio l'OADV), all'interno dell'impresa, che ha approvato l'accordo di esternalizzazione cloud;

e. le date degli ultimi audit ed eventualmente di quelli in programma;

f. i nomi di eventuali subcontraenti cui sono affidate parti sostanziali di una funzione o un'attività operativa essenziale o importante, compresi i paesi nei quali i subcontraenti sono registrati, il luogo in cui sarà prestato il servizio e, a seconda dei casi, i luoghi (paesi o regioni) in cui i dati saranno conservati;

g. il risultato di una valutazione della sostituibilità del fornitore di servizi cloud (se è facile, difficile o impossibile sostituirlo);

h. un campo che indichi se la funzione o l'attività operativa essenziale o importante esternalizzata supporta attività operative che sono critiche in termini di tempo;

i. una stima dei costi finanziari annui (budget cost);

j. se l'impresa che esternalizza dispone di una strategia di uscita in caso di recesso di una delle parti o di interruzione dei servizi da parte del fornitore di servizi cloud.

25. In caso di esternalizzazione di funzioni o attività operative non essenziali o non importanti, l'impresa dovrebbe definire le informazioni di cui tenere traccia in base alla natura, alla portata e alla complessità dei rischi inerenti ai servizi forniti dal fornitore di servizi cloud.

26. L'impresa dovrebbe mettere a disposizione dell'autorità di vigilanza, su richiesta, tutte le informazioni necessarie per consentirle di esercitare la vigilanza sull'impresa, compresa una copia dell'accordo di esternalizzazione.

Orientamento 6 – Analisi pre-esternalizzazione

27. Prima di concludere qualsiasi accordo con fornitori di servizi cloud, l'impresa dovrebbe:

a. valutare se l'accordo di esternalizzazione cloud riguarda una funzione o un'attività operativa essenziale o importante, conformemente all'orientamento 7;

b. individuare e valutare tutti i rischi pertinenti dell'accordo di esternalizzazione cloud, conformemente all'orientamento 8;

c. effettuare un'adeguata dovuta diligenza sul potenziale fornitore di servizi cloud, conformemente all'orientamento 9;

d. individuare e valutare i conflitti di interesse che l'esternalizzazione può causare, in linea con i requisiti di cui all'articolo 274, paragrafo 3, lettera b), del regolamento delegato.

Orientamento 7 – Valutazione delle funzioni e delle attività operative essenziali o importanti

28. Prima di concludere qualsiasi accordo di esternalizzazione con fornitori di servizi cloud, l'impresa dovrebbe valutare se l'accordo di esternalizzazione nel cloud riguarda una funzione o un'attività operativa essenziale o importante. Nell'effettuare tale valutazione, ove opportuno, l'impresa dovrebbe considerare se l'accordo ha il potenziale per diventare essenziale o importante in futuro. L'impresa dovrebbe inoltre valutare nuovamente l'essenzialità o l'importanza della funzione o dell'attività operativa precedentemente esternalizzata a fornitori di servizi cloud, qualora la natura, la portata e la complessità dei rischi inerenti all'accordo cambino sostanzialmente.

29. Nella valutazione, l'impresa dovrebbe tenere conto, unitamente all'esito della valutazione dei rischi, quanto meno dei fattori seguenti:

a. il potenziale impatto di un'eventuale interruzione sostanziale della funzione o dell'attività esternalizzata o della mancata prestazione del servizio, da parte del fornitore di servizi cloud, ai livelli di servizio concordati, sui seguenti aspetti dell'impresa:
    i. la continua conformità agli obblighi normativi;
    ii. la resilienza e la solidità finanziarie e di solvibilità a breve e lungo termine;
    iii. la propria continuità e resilienza operativa;
    iv. i rischi operativi, compresi i rischi di condotta, i rischi ICTe i rischi legali;
    v. i rischi reputazionali;

b. il potenziale impatto dell'accordo di esternalizzazione nel cloud sulla capacità dell'impresa di:
    i. individuare, monitorare e gestire tutti i rischi pertinenti;
    ii. rispettare tutte le disposizioni di legge e tutti gli obblighi normativi;
    iii. condurre opportune verifiche inerenti alla funzione o all'attività operativa esternalizzata;

c. l'esposizione complessiva dell'impresa (e del gruppo, se del caso) nei confronti dello stesso fornitore di servizi cloud e il potenziale impatto cumulativo degli accordi di esternalizzazione nella medesima area operativa;

d. le dimensioni e la complessità di qualsiasi area operativa dell'impresa interessata dall'accordo di esternalizzazione cloud;

e. la capacità, se necessario o auspicabile, di trasferire l'accordo di esternalizzazione cloud proposto a un altro fornitore di servizi cloud o di reintegrare i servizi ("sostituibilità");

f. la protezione dei dati personali e non personali e il potenziale impatto sull'impresa, sugli assicurati o su altri soggetti rilevanti, di una violazione della riservatezza o della mancata garanzia della disponibilità e dell'integrità dei dati sulla base, *inter alia*, del regolamento (UE) 2016/679[7]. L'impresa dovrebbe in particolare prendere in considerazione i dati che costituiscono segreti aziendali e/o sono sensibili (ad esempio, i dati sanitari degli assicurati).

Orientamento 8 – Valutazione dei rischi dell'esternalizzazione cloud

30. In linea generale, l'impresa dovrebbe adottare un approccio proporzionato alla natura, alla portata e alla complessità dei rischi inerenti ai servizi esternalizzati a fornitori di servizi cloud. Ciò include la valutazione del potenziale impatto di qualsiasi esternalizzazione nel cloud, in particolare sui relativi rischi operativi e reputazionali.

31. In caso di esternalizzazione di funzioni o attività operative essenziali o importanti a fornitori di servizi cloud, un'impresa dovrebbe:

a. tenere conto dei benefici e dei costi attesi dell'accordo proposto 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 sorgere per effetto dell'accordo proposto di esternalizzazione del cloud;

b. valutare, ove applicabile e opportuno, i rischi, compresi i rischi legali, informatici, di conformità e reputazionali nonché le limitazioni della sorveglianza derivanti da:

    i. il servizio cloud selezionato e i modelli di implementazione proposti (pubblico/privato/ibrido/comunità);

    ii. la migrazione e/o l'implementazione;

    iii. le attività e i relativi dati e sistemi per i quali si sta valutando l'esternalizzazione (o che sono stati esternalizzati), la loro sensibilità e le misure di sicurezza necessarie;

    iv. la stabilità politica e la situazione della sicurezza dei paesi (all'interno o al di fuori dell'UE) in cui i servizi esternalizzati sono o possono essere forniti e in cui i dati sono o possono essere conservati. La valutazione dei rischi dovrebbe considerare:

        1. la legislazione vigente, compresa quella sulla protezione dei dati;

        2. i dispositivi in atto per l'applicazione della legislazione;

        3. le disposizioni del diritto fallimentare applicabili in caso di dissesto di un fornitore di servizi e le eventuali restrizioni che potrebbero insorgere per quanto riguarda il recupero urgente dei dati dell'impresa;

    v. la subesternalizzazione, compresi i rischi aggiuntivi che possono sorgere se il subcontraente ha sede in un paese terzo o in un paese diverso da quello del fornitore di servizi cloud e il rischio che lunghe

[7] 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 (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

e compliesse catene di subesternalizzazione riducano la capacità dell'impresa di sorvegliare le proprie funzioni o attività operative essenziali o importanti e la capacità delle autorità di vigilanza di soprintendere efficacemente su di esse;

vi. il rischio complessivo di concentrazione dell'impresa con lo stesso fornitore di servizi cloud, compresa l'esternalizzazione a un fornitore di servizi cloud non facilmente sostituibile o la stipula di molteplici accordi di esternalizzazione con lo stesso fornitore di servizi cloud. Nel valutare il rischio di concentrazione, l'impresa (e/o il Gruppo, se del caso) dovrebbe tenere conto di tutti i suoi accordi di esternalizzazione nel cloud con un singolo fornitore di servizi cloud.

32. La valutazione del rischio dovrebbe essere eseguita prima di stipulare un accordo di esternalizzazione cloud. Se l'impresa viene a conoscenza di carenze significative e/o di modifiche consistenti ai servizi forniti o alla situazione del fornitore di servizi cloud, la valutazione del rischio dovrebbe essere prontamente rivista o effettuata *ex novo*. In caso di rinnovo di un accordo di esternalizzazione cloud relativamente al suo contenuto e all'ambito di applicazione (ad esempio, ampliamento dell'ambito di applicazione o inclusione nello stesso di funzioni operative essenziali o importanti precedentemente non incluse), la valutazione del rischio deve essere eseguita nuovamente.

Orientamento 9 – *Due diligence* in merito al fornitore di servizi cloud

33. L'impresa dovrebbe garantire, nel suo processo di selezione e valutazione, che il fornitore di servizi cloud sia idoneo secondo i criteri definiti dalla sua politica scritta di esternalizzazione.

34. La *due diligence* in merito al fornitore di servizi cloud deve essere eseguita prima di esternalizzare qualsiasi funzione o attività operativa. Nel caso in cui l'impresa concluda un secondo accordo con un fornitore di servizi cloud che è già stato valutato, la stessa dovrebbe determinare, seguendo un approccio basato sul rischio, se è necessaria una seconda *due diligence*. Se l'impresa viene a conoscenza di carenze significative e/o di modifiche consistenti ai servizi forniti o alla situazione del fornitore di servizi cloud, l'attività di *due diligence* dovrebbe essere prontamente rivista o effettuata nuovamente.

35. In caso di esternalizzazioni cloud di funzioni operative essenziali o importanti, l'attivitá di *due diligence* dovrebbe includere una valutazione dell'idoneità del fornitore di servizi cloud (ad esempio, competenze, infrastruttura, situazione economica, stato aziendale e normativo). Ove opportuno, per dimostrare che l'attività di *due diligence* sia stata realizzata, l'impresa può utilizzare certificazioni basate su norme internazionali, relazioni di revisione di terze parti riconosciute o relazioni di revisione interna.

Orientamento 10 – Obblighi contrattuali

36. I diritti e gli obblighi rispettivi dell'impresa e del fornitore di servizi cloud dovrebbero essere assegnati chiaramente e indicati in un accordo scritto.

37. Fatti salvi i requisiti di cui all'articolo 274 del regolamento delegato, in caso di esternalizzazione di funzioni o attività operative essenziali o importanti a un fornitore di servizi cloud, l'accordo scritto tra l'impresa e il fornitore di servizi cloud dovrebbe stabilire:

a. una chiara descrizione della funzione esternalizzata da fornire (servizi cloud, compresa la tipologia dei servizi di supporto);

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 competenza giurisdizionale e la normativa che disciplina l'accordo;

d. gli obblighi finanziari delle parti;

e. una clausola che indichi se è consentita la sub-esternalizzazione di una funzione o attività operativa essenziale o importante (o di parti sostanziali di essa) e, in tal caso, le condizioni cui è soggetta la sub-esternalizzazione significativa (cfr. l'orientamento 13);

f. i luoghi (regioni o paesi) in cui i dati pertinenti saranno conservati e trattati (ubicazione dei centri dati) e le condizioni da soddisfare, compreso l'obbligo di informare l'impresa se il fornitore di servizi propone di cambiare l'ubicazione o le ubicazioni;

g. disposizioni relative all'accessibilità, alla disponibilità, all'integrità, alla riservatezza, alla privacy e alla sicurezza dei dati pertinenti, tenendo conto delle specifiche dell'orientamento 12;

h. il diritto dell'impresa di monitorare periodicamente le prestazioni del fornitore di servizi cloud;

i. i livelli di servizio concordati, che dovrebbero includere precisi obiettivi di performance, quantitativi e qualitativi, in modo da consentire un monitoraggio tempestivo che consenta di adottare, senza indebiti ritardi, le opportune azioni correttive in caso di mancato raggiungimento dei livelli di servizio concordati;

j. gli obblighi di reportistica del fornitore di servizi cloud all'impresa, compresi, se del caso, l'obbligo di presentare relazioni pertinenti per la funzione di sicurezza dell'impresa e le funzioni chiave, come ad esempio le relazioni sulla funzione di audit interno del fornitore di servizi cloud;

k. 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;

l. i requisiti per l'attuazione e la verifica dei piani di emergenza dell'impresa (business contingency plans);

m. il requisito per il fornitore di servizi cloud di concedere all'impresa, alle sue autorità di vigilanza e a qualsiasi altra persona designata dall'impresa o dalle autorità di vigilanza:

    i. pieno accesso a tutti i locali aziendali pertinenti (uffici centrali e centri operativi), incluso l'intero insieme di dispositivi, sistemi, reti, informazioni e dati utilizzati per lo svolgimento della funzione esternalizzata, tra cui le relative informazioni finanziarie, il personale e i revisori esterni del fornitore di servizi ("diritti di accesso");

    ii. diritti illimitati di ispezione e di audit relativi all'accordo di esternalizzazione nel cloud ("diritti di audit"), per consentire il monitoraggio dell'accordo di esternalizzazione e assicurare il rispetto di tutti gli obblighi normativi e contrattuali applicabili.

n. disposizioni che assicurino che i dati in possesso dell'impresa possano essere recuperati prontamente dalla stessa in caso di insolvenza, risoluzione o cessazione dell'attività del prestatore di servizi cloud;

Orientamento 11 – Diritti di accesso e di audit

38. L'accordo di esternalizzazione cloud non dovrebbe limitare l'effettivo esercizio, da parte dell'impresa, dei diritti di accesso e di audit nonché delle opzioni di controllo sui servizi cloud al fine di adempiere i propri obblighi normativi.

39. L'impresa dovrebbe esercitare i propri diritti di accesso e di audit nonché determinare la frequenza degli audit e le aree e i servizi da sottoporre a ispezione secondo un approccio basato sul rischio, conformemente alla sezione 8 degli orientamenti dell'EIOPA sul sistema di governance.

40. Nel determinare la frequenza e la portata del suo esercizio dei diritti di accesso o di audit, l'impresa dovrebbe considerare se l'esternalizzazione nel cloud è correlata a una funzione o attività operativa essenziale o importante, la natura e l'entità del rischio e l'impatto sull'impresa derivante dagli accordi di esternalizzazione cloud.

41. Se l'esercizio dei suoi diritti di accesso o di audit o l'uso di determinate tecniche di audit crea un rischio per l'ambiente del fornitore di servizi cloud e/o per un altro cliente del fornitore di servizi cloud (ad esempio, l'impatto sui livelli di servizio, la disponibilità dei dati, gli aspetti di riservatezza), l'impresa e il fornitore di servizi cloud dovrebbero concordare modalità alternative per fornire un livello di garanzia e di servizio analogo all'impresa (ad esempio, l'inclusione di controlli specifici da testare in una relazione/certificazione specifica prodotta dal fornitore di servizi cloud).

42. Fatta salva la loro responsabilità ultima per quanto riguarda le attività svolte dai loro fornitori di servizi 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 possono utilizzare:

a. certificazioni di soggetti terzi e relazioni di terzi o dell'audit interno messe a disposizione dal fornitore di servizi;

b. verifiche congiunte di audit (ovvero eseguiti congiuntamente ad altri clienti dello stesso fornitore di servizi cloud), oppure verifiche congiunte di audit eseguite da soggetti terzi da questi nominati.

43. In caso di esternalizzazione nel cloud di funzioni o attività operative essenziali o importanti, le imprese dovrebbero utilizzare il metodo di cui al paragrafo 42, lettera a), solo se:

a. assicurano che l'ambito della certificazione o della relazione di audit comprenda i sistemi (ad esempio, processi, applicazioni, infrastruttura, centri dati) e i controlli individuati dall'impresa e valutano la conformità agli obblighi normativi pertinenti;

b. sottopongono a valutazione accurata e periodica il contenuto di nuove certificazioni o relazioni di audit e verificano che non siano obsolete;

c. assicurano che i controlli e i sistemi essenziali siano compresi anche nelle versioni successive della certificazione o della relazione di audit;

d. considerano idoneo il soggetto che esegue la certificazione o l'audit (per quanto riguarda, ad esempio, la rotazione delle società di certificazione o di audit, le qualifiche, le competenze, la riesecuzione/verifica relativa alle risultanze contenute nel fascicolo di audit);

e. assicurano che le certificazioni siano rilasciate e che gli audit siano espletati sulla base di norme professionali ampiamente riconosciute e che comprendano anche una verifica dell'efficacia operativa dei controlli essenziali in essere;

f. hanno il diritto contrattuale di chiedere l'ampliamento dell'ambito delle certificazioni o delle relazioni di audit per includervi sistemi e controlli rilevanti; 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. mantengono il diritto contrattuale di eseguire a loro discrezione singole verifiche di audit in loco con riferimento all'esternalizzazione cloud di funzioni o attività operative essenziali o importanti; tale diritto dovrebbe essere esercitato in caso di esigenze specifiche, quando non è possibile farlo attraverso altre modalità di interazioni con il fornitore di servizi di cloud.

44. Per l'esternalizzazione a fornitori di servizi cloud di funzioni essenziali o importanti, l'impresa dovrebbe valutare se le certificazioni e le relazioni di terzi di cui al paragrafo 42, lettera a) sono adeguate e sufficienti per ottemperare agliobblighi normativi e, adottando un approccio basato sul rischio, non dovrebbe basarsi esclusivamente su tali relazioni e certificati nel tempo.

45. Prima di un accesso in loco programmato, la parte che esercita il proprio diritto di accesso (impresa, revisore o terzo che agisce per conto dell'impresa o delle imprese) dovrebbe darne preavviso entro un periodo di tempo ragionevole, a meno che non sia possibile a causa di una situazione di emergenza o di crisi. Tale preavviso dovrebbe includere il luogo e lo scopo della visita nonché il personale che vi parteciperà.

46. In considerazione dell'elevata complessità tecnica delle soluzioni cloud, l'impresa dovrebbe verificare che il personale che esegue l'audit – ossia i propri revisori interni o il gruppo di revisori che opera per suo conto, o i revisori nominati dal fornitore di servizi cloud – o, se del caso, il personale che rivede la certificazione di terza parte o le relazioni di audit del fornitore di servizi, abbiano acquisito le capacità e conoscenze adeguate per eseguire audit e/o valutazioni.

Orientamento 12 – Sicurezza dei dati e dei sistemi

47. L'impresa dovrebbe garantire che i fornitori di servizi cloud rispettino le normative europee e nazionali nonché gli opportuni standard di sicurezza delle tecnologie dell'informazione e della comunicazione (ICT).

48. In caso di esternalizzazione di funzioni o attività operative essenziali o importanti a fornitori di servizi cloud, l'impresa dovrebbe inoltre definire requisiti specifici di sicurezza delle informazioni nell'accordo di esternalizzazione e monitorare periodicamente il rispetto di tali requisiti.

49. Ai fini del paragrafo 48, in caso di esternalizzazione di funzioni o attività operative essenziali o importanti a fornitori di servizi cloud, l'impresa, applicando un approccio basato sul rischio e tenendo conto delle proprie responsabilità e di quelle del fornitore di servizi cloud, dovrebbe:

a. concordare ruoli e responsabilità chiari tra il fornitore di servizi cloud e l'impresa in relazione alle funzioni o alle attività operative interessate dall'esternalizzazione nel cloud, che dovrebbero essere chiaramente assegnati;

b. definire e decidere un adeguato livello di protezione dei dati riservati, della continuità delle attività esternalizzate nonché dell'integrità e della tracciabilità dei dati e dei sistemi nel contesto della prevista esternalizzazione cloud;

c. prendere in considerazione, laddove necessario, misure specifiche per i dati in movimento, i dati memorizzati e i dati a riposo, ad esempio l'utilizzo di tecniche crittografiche unite a un'adeguata gestione strategica;

d. considerare i meccanismi di integrazione dei servizi cloud con i sistemi delle imprese, ad esempio le interfacce per programmi applicativi e un solido processo di gestione degli utenti e degli accessi;

e. garantire contrattualmente che la disponibilità del traffico di rete e la capacità prevista soddisfino rigorosi requisiti di continuità, ove applicabile e fattibile;

f. definire e decidere opportuni requisiti di continuità che garantiscano livelli adeguati a ciascun livello della catena tecnologica, ove applicabile;

g. disporre di un processo di gestione degli incidenti solido e ben documentato che includa le rispettive responsabilità, ad esempio mediante la definizione di un modello di cooperazione in caso di incidenti effettivi o sospetti;

h. adottare un approccio basato sul rischio per quanto riguarda la conservazione e il trattamento dei dati e le relative ubicazioni (ad esempio, paese o regione) e le considerazioni relative alla sicurezza delle informazioni;

i. monitorare il rispetto dei requisiti relativi all'efficacia e all'efficienza dei meccanismi di controllo implementati dal fornitore di servizi cloud che attenuerebbero i rischi connessi ai servizi forniti.

Orientamento 13 – Subesternalizzazione di funzioni e attività operative essenziali o importanti

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

a. specificare le tipologie di attività che sono escluse dalla potenziale subesternalizzazione;

b. indicare le condizioni da rispettare in caso di subesternalizzazione (ad esempio, che anche il subesternalizzatore rispetterà integralmente gli obblighi del fornitore di servizi cloud). Tali obblighi comprendono i diritti di accesso e di audit e la sicurezza di dati e sistemi;

c. indicare che il fornitore di servizi cloud mantiene la piena responsabilità e la supervisione sui servizi subesternalizzati;

d. contemplare l'obbligo per il fornitore di servizi cloud di informare l'impresa di qualsiasi modifica significativa pianificata con riferimento ai subcontraenti o dei servizi subesternalizzati che possano compromettere la capacità del fornitore di servizi di ottemperare ai propri obblighi quali previsti dall'accordo di esternalizzazione cloud. Il periodo di notifica di tali modifiche dovrebbe consentire all'impresa per lo meno di effettuare una valutazione del rischio relativa agli effetti delle modifiche proposte, prima che tali modifiche attuate;

e. assicurare, nei casi in cui un fornitore di servizi cloud preveda modifiche a un subesternalizzatore o a servizi subesternalizzati che avrebbero un effetto negativo sulla valutazione del rischio dei servizi concordati, che l'impresa abbia il diritto di opporsi a tali modifiche e/o il diritto di rescindere il contratto e recedere dallo stesso.

Orientamento 14 – Monitoraggio e supervisione degli accordi di esternalizzazione nel cloud

51. L'impresa dovrebbe monitorare periodicamente lo svolgimento delle attività, le misure di sicurezza e il rispetto del livello di servizio concordato dai propri fornitori

di servizi cloud seguendo un approccio basato sul rischio. L'attenzione principale dovrebbe essere rivolta all'esternalizzazione nel cloud di funzioni operative essenziali e importanti.

52. A tal fine, l'impresa dovrebbe istituire meccanismi di monitoraggio e sorveglianza che tengano conto, ove fattibile e opportuno, della presenza di una subesternalizzazione di funzioni operative essenziali o importanti o di parte di esse.

53. L'OADV dovrebbe essere periodicamente aggiornato sui rischi individuati nell'esternalizzazione cloud di funzioni o attività operative essenziali o importanti.

54. Al fine di garantire un monitoraggio e una sorveglianza adeguati dei propri accordi di esternalizzazione nel cloud, le imprese dovrebbero impiegare risorse sufficienti con competenze e conoscenze adeguate per monitorare i servizi esternalizzati nel cloud. Il personale dell'impresa responsabile di tali attività dovrebbe possedere, se ritenuto necessario, sia conoscenze in materia di ITC sia conoscenze nel campo aziendale.

Orientamento 15 – Diritti di recesso e strategie di uscita

55. In caso di esternalizzazione cloud di funzioni o attività operative essenziali o importanti, all'interno dell'accordo di esternalizzazione cloud l'impresa dovrebbe prevedere una clausola chiaramente definita relativa alla strategia di uscita, che le garantisca la possibilità di risolvere l'accordo, se necessario. La risoluzione dell'accordo dovrebbe essere resa possibile senza pregiudicare la continuità e la qualità della sua prestazione di servizi agli assicurati. A tale scopo, l'impresa dovrebbe:

a. sviluppare piani di uscita che siano esaustivi, basati su servizi, documentati e sufficientemente testati (ad esempio, effettuando un'analisi dei potenziali costi, impatti, risorse e tempistiche delle varie potenziali opzioni di uscita);

b. individuare soluzioni alternative ed elaborare piani di transizione appropriati e fattibili per consentire all'impresa di rimuovere e trasferire le attività e i dati esistenti dal fornitore di servizi cloud a fornitori di servizi alternativi o di reintegrarli all'interno dell'impresa. Tali soluzioni dovrebbero essere definite tenendo conto dei problemi che possono sorgere a causa dell'ubicazione dei dati, adottando le misure necessarie per garantire la continuità operativa durante la fase di transizione;

c. garantire che il fornitore di servizi cloud fornisca all'impresa l'adeguato supporto nel trasferimento dei dati, dei sistemi o delle applicazioni esternalizzati a un altro fornitore di servizi o direttamente all'impresa;

d. concordare con il fornitore di servizi cloud che, una volta ritrasferiti all'impresa, i suoi dati saranno cancellati integralmente e in modo sicuro dal fornitore di servizi cloud in tutte le regioni.

56. Nell'elaborazione delle strategie di uscita, l'impresa dovrebbe considerare quanto segue:

a. definire gli obiettivi della strategia di uscita;

b. definire gli eventi scatenanti (ad esempio, indicatori chiave di rischio che segnalano un livello di servizio inaccettabile) che potrebbero attivare la strategia di uscita;

c. effettuare un'analisi d'impatto aziendale proporzionata alle attività esternalizzate, al fine di individuare le risorse umane e le altre risorse necessarie per l'eventuale attuazione del piano di uscita e calcolare le relative tempistiche;

d. attribuire ruoli e responsabilità per la gestione dei piani di uscita e delle attività di transizione;

e. definire i criteri di successo della transizione.

Orientamento 16 – Supervisione degli accordi di esternalizzazione nel cloud da parte delle autorità di vigilanza

57. Le autorità di vigilanza dovrebbero effettuare, nell'ambito del loro processo di riesame, l'analisi degli impatti derivanti dagli accordi delle imprese relativi all'esternalizzazione cloud. Tale analisi dovrebbe concentrarsi, in particolare, sugli accordi relativi all'esternalizzazione di funzioni o attività operative essenziali o importanti.

58. Le autorità di vigilanza dovrebbero considerare i rischi seguenti nella vigilanza degli accordi di esternalizzazione nel cloud delle imprese:

a. rischi ICT;

b. altri rischi operativi (compresi il rischio legale e di conformità, il rischio legato all'esternalizzazione ("*outsourcing and third party risk*") e il rischio relativo alla gestione di terzi);

c. rischio reputazionale;

d. rischio di concentrazione, anche a livello nazionale/settoriale.

59. Nella loro valutazione, le autorità di vigilanza dovrebbero includere i seguenti aspetti in un approccio basato sul rischio:

a. l'adeguatezza e l'efficacia della governance dell'impresa e dei processi operativi relativi all'approvazione, all'attuazione, al monitoraggio, alla gestione e al rinnovo degli accordi di esternalizzazione nel cloud;

b. se l'impresa dispone di risorse sufficienti con competenze e conoscenze adeguate per monitorare i servizi esternalizzati nel cloud;

c. se l'impresa individua e gestisce tutti i rischi evidenziati dai presenti orientamenti.

60. Nel caso di gruppi di imprese, l'autorità di vigilanza del gruppo dovrebbe assicurare che gli impatti dell'esternalizzazione nel cloud di funzioni o attività operative essenziali o importanti si riflettano nella valutazione del rischio di vigilanza del gruppo, tenendo conto dei requisiti elencati ai paragrafi 58 e 59 e delle singole caratteristiche operative e di governance del gruppo.

61. Se l'esternalizzazione nel cloud di funzioni o attività operative essenziali o importanti coinvolge più di un'impresa in diversi Stati membri ed è gestita a livello centrale dall'impresa madre o da una controllata del gruppo (ad esempio, un'impresa o una società di servizi del gruppo come il fornitore di TIC del gruppo), l'autorità di vigilanza del gruppo e/o le autorità di vigilanza competenti delle imprese coinvolte nell'esternalizzazione nel cloud dovrebbero discutere, ove opportuno, degli impatti di tale esternalizzazione sul profilo di rischio del gruppo in seno al collegio delle autorità di vigilanza.

62. Qualora siano individuati problemi che inducano a concludere che un'impresa non è più dotata di solidi dispositivi di governance o non rispetta gli obblighi normativi, le autorità di vigilanza dovrebbero adottare misure appropriate, che possono prevedere, ad esempio, l'obbligo per l'impresa di migliorare il dispositivo di governance, la limitazione o la restrizione della portata delle funzioni esternalizzate o l'obbligo di recesso da uno o più accordi di esternalizzazione. In particolare,

tenendo conto della necessità di assicurare la continuità del funzionamento dell'impresa, potrebbe essere richiesta la risoluzione dei contratti se la vigilanza e l'applicazione degli obblighi normativi non possono essere garantiti con altri mezzi.

Norme sulla conformità e sulla segnalazione

63. Il presente documento contiene orientamenti emanati in applicazione dell'articolo 16 del regolamento (UE) n. 1094/2010. A norma dell'articolo 16, paragrafo 3, di detto regolamento, le autorità e gli istituti finanziari competenti sono tenuti a compiere ogni sforzo per essere conformi agli orientamenti e alle raccomandazioni.

64. Le autorità competenti che sono conformi o intendono conformarsi ai presenti orientamenti dovrebbero integrarli opportunamente nel proprio quadro normativo o di vigilanza.

65. Le autorità competenti devono confermare all'EIOPA se sono conformi o intendono conformarsi ai presenti orientamenti, indicando i motivi, laddove non siano conformi, entro due mesi dalla pubblicazione delle versioni tradotte.

66. In assenza di una risposta entro tale termine, le autorità competenti saranno considerate non conformi in materia di segnalazione e verranno segnalate come tali.

Disposizione finale sulle revisioni

67. I presenti orientamenti saranno oggetto di riesame da parte dell'EIOPA.