# La gestione del rischio di terze parti ICT nella vigenza di DORA, tra profili di *governance* e tutele contrattuali



*A cura di Avv. Marco Romanelli*

## 1. Premessa

La crescente dipendenza degli intermediari bancari e finanziari da fornitori esterni di servizi tecnologici– dal *cloud computing* alle piattaforme di *core banking*, dai servizi di elaborazione dei pagamenti alle infrastrutture di rete – ha progressivamente spostato larga parte del rischio operativo al di fuori del perimetro aziendale, per lo più allocato su provider con i quali gli finanziari intrattengono rapporti esclusivamente contrattuali.

In tale contesto, il principio riaffermato dal Regolamento DORA, applicabile dal 17 gennaio 2025, secondo cui l'ente finanziario che si avvale di servizi ICT di terzi "*rimane sempre pienamente responsabile*" del rispetto

degli obblighi regolamentari[1], onera l'ente vigilato di individuare, adottare e monitorare i presidi organizzativi, procedurali e contrattuali più idonei a prevenire disservizi, interruzioni dell'operatività e perdite economiche.

Il rapporto congiunto pubblicato dalle Autorità europee di vigilanza ("**ESAs**") in data 3 giugno 2026 sugli incidenti gravi occorsi nel 2025 censisce n. 3.383 incidenti gravi notificati nell'Unione, oltre il 60% dei quali nel settore creditizio; in particolare, il 29% di tali incidenti origina da un malfunzionamento imputabile a un fornitore terzo e circa un terzo ha avuto impatto transfrontaliero[2]. Le ESAs hanno rilevato, tra l'altro, un "*effetto moltiplicatore*" nei gruppi bancari le cui componenti condividono la medesima infrastruttura di *core banking* o di *processing* dei pagamenti, cosicché un singolo disservizio del fornitore è in grado di generare decine di incidenti gravi.

Oltre al fattore dipendenza da infrastrutture e servizi di terzi, il quadro delle minacce è in rapida evoluzione: con lo *Statement* del 31 luglio 2026 le ESAs hanno richiamato l'attenzione sui rischi informatici amplificati dai modelli di intelligenza artificiale di frontiera, capaci di individuare e sfruttare in tempi ridotti le vulnerabilità delle infrastrutture condivise e i singoli punti critici lungo la catena di fornitura[3].

Nel confronto tra operatori di mercato, Autorità di Vigilanza e fornitori che ha accompagnato la prima fase applicativa del DORA, emergono due direttrici di intervento, tra loro strettamente connesse:

(i) il rafforzamento della *governance* dei rischi informatici, anche mediante l'inserimento negli organi di amministrazione degli enti vigilati di esponenti con competenze specifiche;

(ii) la revisione delle tutele contrattuali nei rapporti con le terze parti, con particolare riferimento alla gestione dei casi di subappalto, *audit* ed *exit*.

# 2. Il rafforzamento della *governance* dei rischi informatici

## 2.1. La responsabilità finale dell'organo di gestione

La gestione del rischio informatico compete al vertice dell'organizzazione aziendale: l'art. 5, paragrafo 2, del Regolamento DORA stabilisce che l'organo di gestione "*definisce e approva l'attuazione di tutte le disposizioni concernenti il quadro per la gestione dei rischi informatici*", "*vigila su tale attuazione e ne è responsabile*",

---

(1) Cfr. art. 28, paragrafo 1, lett. a), del Regolamento DORA: "*le entità finanziarie che hanno stipulato accordi contrattuali per l'utilizzo di servizi TIC per lo svolgimento delle proprie operazioni commerciali rimangono sempre pienamente responsabili del rispetto e dell'adempimento di tutti gli obblighi previsti dal presente regolamento e dalla normativa applicabile in materia di servizi finanziari*".

(2) Cfr. ESAs, *2025 Report on major ICT-related incidents*, JC 2026 16 del 3 giugno 2026, redatto ai sensi dell'art. 22, paragrafo 2, del DORA. Il rapporto precisa che in circa l'8% dei casi l'incidente ha interessato più di dieci Stati membri e che, secondo le ESAs, la dipendenza da fornitori terzi, "*even those non designated as critical*", costituisce un'area di attenzione di vigilanza. L'analisi è limitata agli incidenti per i quali la relazione finale era stata trasmessa entro il 5 febbraio 2026.

(3) Cfr. ESAs, *Toward a consistent and risk-based approach for ICT risks from frontier AI models*, JC 2026 25 del 31 luglio 2026, adottato anche alla luce dell'*Action Plan on Cybersecurity and Artificial Intelligence* della Commissione europea del 7 luglio 2026 e del *warning* del Comitato europeo per il rischio sistemico (ESRB/2026/3) del 25 giugno 2026.

assumendo "*la responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria*"[4]. Sempre all'organo di gestione spetta, tra l'altro, approvare e riesaminare periodicamente la politica relativa all'uso dei servizi ICT prestati da fornitori terzi, nonché istituire canali informativi che consentano di essere aggiornato sugli accordi conclusi con tali fornitori, sulle relative modifiche rilevanti e sul loro potenziale impatto sulle funzioni essenziali o importanti.

Agli enti finanziari diversi dalle microimprese è richiesto, inoltre, di istituire una figura dedicata al monitoraggio degli accordi conclusi con i fornitori terzi, oppure designare un dirigente di rango elevato quale responsabile della sorveglianza sulla relativa esposizione al rischio informatico.

Si tratta di previsioni tutt'altro che programmatiche: il Decreto DORA ha infatti esteso la responsabilità sanzionatoria anche ai singoli esponenti aziendali, prevedendo sanzioni da Euro 5.000 fino a Euro 5 milioni a carico dei soggetti che svolgono funzioni di amministrazione, direzione o controllo, quando l'inosservanza sia conseguenza della violazione di doveri propri o dell'organo di appartenenza e la condotta abbia inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali, nonché, nei casi più gravi, la sanzione accessoria dell'interdizione da sei mesi a tre anni dallo svolgimento di funzioni di amministrazione, direzione e controllo[5].

## 2.2. Le competenze in materia ICT negli organi di amministrazione

In coerenza con il quadro normativo in materia di responsabilità degli organi sociali poco sopra rappresentato, l'art. 5, paragrafo 4, del DORA impone ai membri dell'organo di gestione di mantenere "*attivamente aggiornate conoscenze e competenze adeguate per comprendere e valutare i rischi informatici e il loro impatto sulle operazioni dell'entità finanziaria*", anche avvalendosi di una specifica formazione su base regolare[6].

Tale disposizione si inserisce nel quadro normativo nazionale in materia di requisiti di idoneità degli esponenti aziendali e di composizione degli organi sociali, con particolare riferimento alle competenze necessarie per assicurare un'efficace supervisione dei rischi connessi all'impiego delle tecnologie dell'informazione e della comunicazione. Sembra potersi ritenere che la competenza tecnologica debba essere complessivamente condivisa dall'organo di amministrazione nel suo insieme, così da consentire un esercizio consapevole delle relative funzioni di supervisione strategica, anche con riguardo alla valutazione delle scelte di esternalizzazione e dei rischi da esse derivanti.

La concreta osservanza dei richiamati presidi di governance richiede a ciascun ente finanziario di verificare e, se del caso, integrare:

(i) competenze specialistiche nell'organo di amministrazione, attraverso la nomina di almeno un componente dotato di specifica esperienza in materia di ICT, *cybersicurezza* e trasformazione digitale,

---

(4) Cfr. art. 5, paragrafo 2, lett. a), h) e i), del Regolamento DORA.

(5) Cfr. art. 144-*ter*, commi 2-*bis*, 2-*ter* e 3-*bis*, TUB, introdotti dall'art. 10 del d.lgs. 10 marzo 2025, n. 23. Per le violazioni della disciplina sulle terze parti il massimale della sanzione a carico della persona fisica è pari a 3,5 milioni di euro. Ove il vantaggio ottenuto dall'autore della violazione sia superiore ai massimali, la sanzione è elevata fino al doppio dell'ammontare del vantaggio, purché determinabile (comma 2-quater).

(6) Cfr. art. 5, paragrafo 4, del Regolamento DORA, che prosegue precisando che la formazione deve essere "*commisurata ai rischi informatici gestiti*".

da valorizzare nell'ambito dei processi di autovalutazione e di definizione della composizione quali-quantitativa ottimale dell'organo;

(ii) programmi strutturati di formazione e aggiornamento, mediante iniziative di *induction* e formazione continua sui rischi ICT, adeguatamente documentate e calibrate sulle caratteristiche operative e sul profilo di rischio dell'ente;

(iii) l'attribuzione a un comitato interno all'organo di amministrazione – tipicamente il comitato rischi – di un mandato in materia di resilienza operativa digitale e di rischi derivanti dai rapporti con soggetti terzi, supportato da flussi informativi periodici sugli accordi di esternalizzazione relativi a funzioni essenziali o importanti.

In linea con tale impostazione, anche le Autorità europee di vigilanza (ESAs) hanno richiamato l'attenzione sulla necessità che il *risk appetite framework* tenga conto delle esposizioni ai rischi ICT derivanti dal ricorso a fornitori terzi[7].

## 2.3. Il sistema dei controlli interni

Sul piano della gestione dei rischi informatici connessi ai fornitori terzi, assume un ruolo centrale l'art. 28, par. 2 del DORA, che impone agli enti di adottare una complessiva strategia per i rischi derivanti dai fornitori terzi, inclusiva di una policy relativa all'utilizzo dei servizi ICT a supporto delle funzioni essenziali o importante prestati da fornitori terzi; approvata dall'organo di gestione, la strategia disciplina, su base individuale e, ove pertinente, consolidata, l'intero ciclo di vita dei rapporti contrattuali, dalla selezione del fornitore fino alla cessazione del rapporto.

In attuazione dei principi dettati da DORA, il Regolamento delegato (UE) 2024/1773 del 13 marzo 2024 ha imposto agli enti finanziari di definire, nella policy relativa all'utilizzo di servizi ICT prestati da fornitori terzi a supporto di funzioni essenziali o importanti, le responsabilità relative all'approvazione, alla gestione, al controllo e alla documentazione degli accordi, assicurando che l'ente disponga delle competenze necessarie per sorvegliarli efficacemente. A tal fine, l'art. 3 del citato Regolamento richiede di individuare all'interno della policy il ruolo o il dirigente responsabile del monitoraggio degli accordi, disciplinandone i rapporti con le funzioni di controllo e i flussi informativi verso l'organo di gestione, anche con riguardo alla tipologia e alla frequenza delle informazioni da trasmettere[8].

Non è quindi necessaria la creazione di una struttura *ad hoc*: nel rispetto del principio di proporzionalità, l'ente può attribuire tale responsabilità a un'unità organizzativa già esistente, ad esempio quella che gestisce

---

(7) Cfr. *Statement* JC 2026 25 emanato dalle ESAs in data 31 luglio 2026, ove al par. 7 stabilisce che "*competent authorities should also ensure that financial entities' management body is fully committed to mitigate frontier AI models-driven cyber risks with clear governance and accountability frameworks in place, timely response plans adequately prepared, and sufficient internal investments dedicated to strengthening cyber resilience. The Risk Appetite Framework should be reviewed to update and/or incorporate metrics, tolerance thresholds, and control measures consistent with the evolving risk profile stemming both from the internal use of such models and from indirect exposure to them*".

(8) Cfr. art. 3, paragrafi 3 e 5, del Regolamento n. 1773. Il considerando (7) chiarisce che, "per garantire un'adeguata segnalazione all'organo di gestione", la politica dovrebbe "specificare e individuare chiaramente le responsabilità interne per l'approvazione, la gestione, il controllo e la documentazione degli accordi contrattuali". Ai sensi dell'art. 3, paragrafo 4, la politica deve altresì imporre di valutare se il fornitore disponga di risorse sufficienti a garantire il rispetto, da parte dell'ente, di tutti i requisiti legali e regolamentari relativi ai servizi prestati.

i fornitori o i rischi, oppure a un singolo dirigente. Ciò che rileva è che siano garantiti un adeguato raccordo con le funzioni di controllo e un flusso informativo verso l'organo di gestione, cui resta imputata la responsabilità ultima prevista dal DORA. La politica deve inoltre assicurare che i servizi ICT a supporto di funzioni essenziali o importanti siano sottoposti a riesame indipendente e inclusi nel piano di audit[9], estendendo così le verifiche della revisione interna anche alle attività esternalizzate.

Per inquadrare questi presidi nell'assetto dei controlli dell'ente, occorre considerare l'art. 6, par. 4, del DORA, che impone agli enti diversi dalle microimprese di affidare la gestione e la sorveglianza dei rischi informatici a una funzione di controllo dotata di adeguata indipendenza e di assicurare la separazione tra gestione dei rischi ICT, controllo e revisione interna, in modo non dissimile dal noto modello di tripartizione delle funzioni di controllo. Per le banche italiane, tale impostazione si innesta su un assetto già in parte consolidato: le disposizioni di vigilanza della Banca d'Italia prevedevano, infatti, l'attribuzione del presidio dei rischi ICT e di sicurezza a una funzione di controllo di secondo livello. Questa disciplina è stata successivamente, in larga parte, sostituita dal rinvio al DORA e ai relativi atti delegati[10].

A ciò si aggiunge un profilo specifico relativo alle competenze dei revisori: ai sensi dell'art. 28, par. 6, del Regolamento DORA, quando gli accordi presentano un'elevata complessità tecnica, l'ente deve verificare che i revisori dispongano delle conoscenze e delle competenze necessarie per svolgere efficacemente le verifiche[11].

## 3. Il rafforzamento delle tutele contrattuali nei rapporti con le terze parti

L'efficace gestione del rischio di terze parti delineato da DORA esige un rafforzamento tanto della governance dell'intermediario quanto dei meccanismi contrattuali che legano l'ente al provider, al fine di rendere effettivamente coercibili gli obblighi assunti pattiziamente dal provider medesimo, con particolare riguardo alla trasmissione delle informazioni rilevanti, allo svolgimento delle ispezioni e alla migrazione in caso di exit.

Sul punto, il legislatore europeo ha delineato un articolato insieme di prescrizioni sul contenuto degli accordi, distribuite su più livelli normativi: il Regolamento DORA, che all'art. 30 individua le clausole minime che ogni

(9) Cfr. art. 3, paragrafo 7, del Regolamento n. 1773, da leggersi unitamente all'art. 5, paragrafo 2, lett. f), del DORA, che attribuisce all'organo di gestione il compito di approvare e riesaminare periodicamente i piani di *audit* interno in materia di TIC, e all'art. 6, paragrafo 6, del Regolamento DORA, ai sensi del quale il quadro per la gestione dei rischi informatici è sottoposto periodicamente a verifiche di audit interno, con frequenza e oggetto "*commisurati ai rischi connessi alle TIC*". La politica dovrebbe inoltre garantire il diritto dell'ente, dei terzi da esso designati e delle autorità competenti di effettuare ispezioni e di accedere alle informazioni.

(10) Cfr. art. 6, paragrafo 4, del Regolamento DORA. Il considerando (38) chiarisce che l'introduzione di meccanismi di *governance* più complessi – tra cui l'istituzione di funzioni per la supervisione degli accordi con i fornitori terzi e l'organizzazione della gestione dei rischi informatici secondo il modello delle tre linee di difesa – è riservata alle entità finanziarie che non sono microimprese, in quanto "*meglio attrezzate*" a tal fine.

(11) Cfr. art. 28, paragrafo 6, secondo comma, del Regolamento DORA: "*laddove gli accordi contrattuali conclusi con fornitori terzi di servizi TIC per l'utilizzo di servizi TIC comportino un'elevata complessità tecnica, l'entità finanziaria verifica che i revisori, indipendentemente dal fatto che siano revisori interni o esterni o siano un gruppo di revisori, possiedano competenze e conoscenze adeguate per svolgere efficacemente gli audit e le valutazioni del caso*".

contratto per l'utilizzo di servizi ICT deve contenere e, all'art. 28, impone la previsione di specifiche cause di risoluzione e di strategie di uscita; il Regolamento delegato (UE) 2025/532 del 24 marzo 2025, che detta le condizioni alle quali il fornitore può avvalersi di subappaltatori per i servizi a supporto di funzioni essenziali o importanti e il relativo contenuto contrattuale; il già menzionato Regolamento delegato (UE) 2024/1773, che stabilisce che la policy interna disciplini i diritti di accesso, ispezione e audit nei contratti e l'uscita dagli accordi mediante piani documentati e periodicamente testati.

## 3.1. Il contenuto contrattuale minimo delineato dall'art. 30 del DORA

L'art. 30 del Regolamento DORA disegna un contenuto contrattuale minimo degli accordi per l'utilizzo di servizi ICT, articolato su due livelli. Il primo trova applicazione a tutti gli accordi aventi a oggetto servizi ICT; il secondo si aggiunge al primo laddove il servizio sia a supporto di funzioni essenziali o importanti.

Quanto al primo livello, il contratto deve recare, tra l'altro, la descrizione completa delle funzioni e dei servizi che il fornitore deve svolgere, con l'indicazione dell'eventuale autorizzazione al subappalto e delle relative condizioni; le località di prestazione dei servizi e di trattamento dei dati, con obbligo di preavviso in caso di modifica; le garanzie di accesso, ripristino e restituzione dei dati anche in caso di insolvenza del fornitore; l'obbligo di assistenza in caso di incidente "*senza costi aggiuntivi o a un costo stabilito ex ante*"; l'obbligo di cooperare senza riserve con le autorità competenti e di risoluzione.

Quanto al secondo livello, vengono in rilievo livelli di servizio con precisi obiettivi quantitativi e qualitativi, obblighi di notifica degli sviluppi rilevanti, piani di emergenza testati, la partecipazione ai test di penetrazione basati sulle minacce (*TLPT*), diritti incondizionati di accesso, ispezione e audit e strategie di uscita con un periodo di transizione obbligatorio.

A tali elementi si aggiungono le cause di risoluzione che l'art. 28, par. 7, del Regolamento DORA impone di prevedere in ogni accordo, tra le quali spicca l'ipotesi in cui l'autorità competente "*non sia più in grado di vigilare efficacemente sull'entità finanziaria*" per effetto delle condizioni contrattuali[(12)].

Nella prassi negoziale, il principale ostacolo è rappresentato dall'asimmetria di forza contrattuale rispetto ai grandi fornitori *cloud* e di piattaforma, i quali sono soliti proporre condizioni generali accompagnate da appositi "*addendum* DORA" predisposti unilateralmente. La verifica di conformità non può che essere condotta clausola per clausola: un *addendum* che richiami genericamente il DORA, ma subordini l'esercizio dell'audit a lunghi preavvisi, a limiti di frequenza non concordati o a costi indeterminati, difficilmente potrebbe ritenersi idoneo a soddisfare il requisito di diritti il cui effettivo esercizio "*non sia impedito o limitato*".

## 3.2. Le forme e le modalità del subappalto

Nell'attuale quadro normativo, delineato dal Regolamento delegato (UE) 2025/532 del 24 marzo 2025, l'eventuale subappalto di servizi ICT a supporto di funzioni essenziali o importanti deve essere oggetto di approfondita verifica da parte dell'ente finanziario prima della conclusione del contratto principale di

(12) Cfr. art. 28, paragrafo 7, lett. d), del Regolamento DORA. Le ulteriori ipotesi riguardano la rilevante violazione di leggi, regolamenti o condizioni contrattuali da parte del fornitore, le circostanze emerse dal monitoraggio suscettibili di alterare l'esercizio delle funzioni e i punti deboli del fornitore nella gestione complessiva dei rischi informatici.

appalto. Nell'ambito di tali verifiche preliminari, l'ente deve valutare in particolare la capacità del fornitore di selezionare e valutare i potenziali subappaltatori e di individuarli tutti, l'estensione all'ente e alle autorità degli stessi diritti di accesso e ispezione concessi dal fornitore, nonché la valutazione, da parte dell'ente, dell'impatto di un eventuale inadempimento del subappaltatore, dei rischi connessi alla sua localizzazione e degli ostacoli all'esercizio dei diritti di audit.

Ove il subappalto sia ammesso, l'art. 4 del Regolamento n. 532 individua il contenuto minimo del contratto, che deve tra l'altro specificare che (i) il fornitore resta responsabile delle prestazioni rese dai subappaltatori e deve monitorarle; (ii) il contratto a valle riproduce gli obblighi relativi ai piani di emergenza e agli standard di sicurezza; (iii) il subappaltatore riconosce all'ente e alle autorità gli stessi diritti di accesso, ispezione e audit; il fornitore garantisce la continuità del servizio lungo l'intera catena.

Di notevole rilievo è la previsione che obbliga il fornitore a informare l'ente di qualsiasi modifica sostanziale che intende apportare ai propri accordi di subappalto in tempo utile per consentirne la valutazione; il contratto deve fissare un ragionevole termine di preavviso entro il quale l'ente approva le modifiche o vi si oppone; la modifica può essere attuata solo dopo l'approvazione o lo spirare del termine senza opposizione[13]. Nel caso in cui il fornitore abbia modificato il contratto di subappalto nonostante l'opposizione dell'ente o prima della scadenza del preavviso, ovvero abbia subappaltato un servizio non espressamente ammesso al subappalto, l'ente ha il diritto di recedere dal rapporto con il fornitore.

Affinché tali prescrizioni si traducano in clausole effettivamente tutelanti per l'intermediario, è essenziale che il contratto definisca con precisione cosa costituisca "*modifica sostanziale*", preveda un congruo termine di preavviso e individui il contenuto minimo dell'informativa dovuta dal fornitore.

## 3.3. I diritti di audit, accesso e ispezione

Per i servizi a supporto di funzioni essenziali o importanti, l'art. 30, paragrafo 3, lett. e), del Regolamento DORA richiede "*diritti incondizionati di accesso, ispezione e audit*" in capo all'ente, a un terzo da esso designato e all'autorità competente, il cui effettivo esercizio non sia impedito o limitato da altri accordi contrattuali o politiche di attuazione, nonché l'obbligo del fornitore di cooperare senza riserve nel corso delle ispezioni.

E' possibile concordare livelli di garanzia alternativi qualora siano interessati i diritti di altri clienti del fornitore – ipotesi tipica degli ambienti *cloud* condivisi – e, per le microimprese, delegare i diritti di *audit* a un terzo indipendente nominato dal fornitore. L'art. 28, paragrafo 6, del Regolamento DORA impone poi all'ente di predeterminare, secondo un approccio basato sul rischio, la frequenza e le aree delle verifiche.

Quanto agli strumenti di *audit*, il Regolamento delegato 1773 individua l'*audit* interno o condotto da un terzo designato, gli *audit* e i test congiunti con altre entità finanziarie clienti del medesimo fornitore (c.d. *pooled audit*), le certificazioni di terze parti e le relazioni di *audit* messe a disposizione dal fornitore[14]. Il *pooled audit*

(13) Cfr. art. 5 del Regolamento 532. Ai sensi del paragrafo 4, ove ritenga che le modifiche superino la propria tolleranza al rischio, l'ente, prima della scadenza del termine di preavviso, ne informa il fornitore, si oppone alle modifiche e chiede di apportarvi variazioni prima della loro attuazione.

(14) Cfr. art. 8, paragrafo 2, del Regolamento 1773 cit., che ricomprende negli audit congiunti anche i test di penetrazione guidati dalla minaccia organizzati congiuntamente con altre entità finanziarie che utilizzano i servizi del medesimo fornitore.

potrebbe rappresentare una risposta efficiente all'asimmetria negoziale, consentendo di ripartire i costi e di contenere l'impatto operativo sul fornitore. Le certificazioni e le relazioni del fornitore, per contro, non possono assurgere a unico presidio, essendo il suo utilizzo subordinato a stringenti condizioni – tra le quali l'adeguatezza del piano di audit del fornitore, la copertura dei sistemi e controlli essenziali, il diritto contrattuale di chiederne l'estensione del perimetro e di svolgere comunque audit individuali e congiunti – e con il divieto per l'ente di affidarsi esclusivamente a esse[(15)].

Ne discende che la clausola di *audit* dovrebbe, quanto meno: (a) estendere i diritti di *audit* all'intera catena di subappalto; (b) prevedere preavvisi contenuti e la possibilità di verifiche senza preavviso in caso di incidente grave o di richiesta dell'autorità; (c) predeterminare il regime dei costi, evitando che corrispettivi genericamente previsti operino quale limite di fatto all'esercizio degli *audit*.

Da ultimo, le ESAs hanno suggerito di ricomprendere nel perimetro delle verifiche anche la sicurezza della catena di fornitura del *software* e la protezione del codice sorgente, profili sui quali l'*audit* tradizionale si rivela spesso carente[(16)].

## 3.4. La gestione dell'*exit*

La strategia di uscita rappresenta il vero banco di prova della resilienza: un contratto robusto è di scarsa utilità se l'ente non è in grado di uscirne senza interrompere i propri servizi.

L'art. 28, paragrafo 8, del Regolamento DORA richiede che l'ente possa porre termine agli accordi "*senza: a) perturbare le proprie attività commerciali; b) limitare il rispetto dei requisiti normativi; c) pregiudicare la continuità e la qualità dei servizi forniti ai clienti*", e che i piani di uscita siano esaustivi, documentati, testati e periodicamente riesaminati.

Per ciascun accordo deve esistere un piano di uscita documentato, costruito su tre scenari minimi (interruzioni impreviste e persistenti, inadeguata o mancata erogazione dei servizi, risoluzione inattesa) e detto piano deve essere "*realistico, fattibile, basato su scenari plausibili*", con un calendario di attuazione "*compatibile con le condizioni di uscita e di risoluzione stabilite negli accordi contrattuali*". È proprio quest'ultimo requisito a saldare il piano interno con le clausole contrattuali: se il periodo di transizione pattuito è più breve del tempo stimato per la migrazione, il piano è inefficace.

Sul piano contrattuale, l'art. 30, paragrafo 3, lett. f), del Regolamento DORA impone un periodo di transizione obbligatorio, durante il quale il fornitore continua a prestare il servizio al fine di ridurre il rischio di perturbazioni e che consenta la migrazione verso un altro fornitore oppure verso l'internalizzazione.

Alla luce delle citate previsioni, una clausola di prosecuzione del servizio per un certo numero di mesi successivi alla cessazione dell'accordo contrattuale potrebbe rivelarsi insufficiente ad assicurare una

(15) Cfr. art. 8, paragrafo 3, del Regolamento 1773 cit., che elenca otto condizioni cumulative, tra le quali la verifica che le certificazioni siano rilasciate e gli audit eseguiti "sulla base di norme professionali pertinenti ampiamente riconosciute" e includano un test dell'efficacia operativa dei controlli essenziali.

(16) Cfr. *Statement* JC 2026 25, cit., Allegato, ove si richiama la necessità di estendere gli standard di sicurezza all'intera catena di fornitura, includendo "*not only services providers and partners but also soft- and hardware providers and open-source communities*".

transizione ordinata a un nuovo fornitore. Invero, una clausola di *exit* efficace dovrebbe disciplinare quanto meno:

(i) la durata del periodo di transizione, attivabile con dichiarazione unilaterale dell'ente indipendentemente dalla causa di cessazione del rapporto contrattuale, alle medesime condizioni e livelli di servizio;

(ii) gli obblighi di assistenza alla migrazione del fornitore uscente, ivi inclusa la cooperazione con il fornitore subentrante;

(iii) la restituzione integrale di dati e configurazioni in formati aperti e documentati, e la successiva cancellazione certificata;

(iv) la predeterminazione dei costi dell'exit;

(v) il coordinamento con le cause di risoluzione e con il diritto di recesso.

In questa direzione, un contributo può giungere dal Regolamento (UE) 2023/2854 ("**Data Act**"), che ha introdotto obblighi di agevolazione del passaggio tra fornitori di servizi di trattamento dei dati, e dalle clausole contrattuali standard non vincolanti per i contratti di *cloud computing* pubblicate dalla Commissione europea il 20 novembre 2025, che comprendono appositi set dedicati al passaggio e all'uscita, alla risoluzione, alla sicurezza e alla continuità operativa[17]. Pur non essendo state concepite in funzione del DORA, esse paiono costituire un utile parametro di riferimento, prevedendo lo stesso Regolamento DORA di prendere in considerazione il ricorso a clausole contrattuali standard elaborate dalle autorità pubbliche[18].

## 4. Considerazioni conclusive

L'esperienza dei primi due anni di applicazione del Regolamento DORA dimostra che *governance* e tutele contrattuali sono due anelli di un'unica catena. La politica sui fornitori approvata dall'organo di gestione fissa le condizioni della relazione; il contratto le rende opponibili al fornitore; il registro delle informazioni e il sistema dei controlli interni ne verificano la tenuta nel tempo. Una debolezza in uno di tali presidi finisce, inevitabilmente, per riflettersi sugli altri: un organo di amministrazione privo delle competenze necessarie a valutare il rischio ICT difficilmente sarà in grado di esercitare in modo consapevole il diritto di opposizione a una modifica del subappalto; un diritto di audit mai esercitato perde gran parte della propria utilità; un piano di uscita mai testato rischia di rivelarsi fallace nel momento in cui se ne renda necessaria l'attivazione.

L'accelerazione delle minacce abilitate dall'intelligenza artificiale, rendendo più ristretti i tempi entro i quali una lacuna contrattuale od organizzativa può tradursi in un incidente, impone agli intermediari di rafforzare

---

[17] Cfr. Regolamento (UE) 2023/2854 del 13 dicembre 2023, applicabile dal 12 settembre 2025, Capo VI, e la Raccomandazione della Commissione del 20 novembre 2025 recante termini contrattuali tipo non vincolanti in materia di accesso e utilizzo dei dati e clausole contrattuali standard non vincolanti per i contratti di *cloud computing*, adottata ai sensi dell'art. 41 del Data Act. Che tali clausole possano agevolare anche la conformità al DORA è stato osservato, incidentalmente, dall'EIOPA in risposta alla Q&A DORA117-3153.

[18] Cfr. art. 30, paragrafo 4, del Regolamento DORA: "*all'atto della negoziazione degli accordi contrattuali, le entità finanziarie e i fornitori terzi di servizi TIC prendono in considerazione il ricorso a clausole contrattuali standard elaborate dalle autorità pubbliche per servizi specifici*".

senza indugio la resilienza digitale attraverso l'adozione, *in primis*, di misure di governance efficaci e di tutele contrattuali adeguate.

Rimane aperto l'interrogativo su come la Banca d'Italia e la BCE, nell'ambito delle rispettive prerogative di vigilanza, declineranno in concreto i principi di proporzionalità e di responsabilità finale dell'ente nei rapporti con i fornitori di maggiori dimensioni, rispetto ai quali la forza negoziale degli intermediari, specie di quelli meno significativi, risulta strutturalmente limitata. In tale contesto, il ricorso a strumenti di tipo collettivo, quali gli *audit* congiunti e le clausole contrattuali standard elaborate dalle autorità pubbliche, potrebbe rappresentare un utile fattore di riequilibrio.

***

# Contatti


### Marco Romanelli



**Partner**
☎ +39 06 8083138
✉ mromanelli@studiocarbonetti.it

### Alberto Mozzi



**Counsel**
☎ +39 02 72019078
✉ amozzi@studiocarbonetti.it