Gli obblighi relativi agli accordi contrattuali stipulati tra fornitori terzi di servizi ICT e soggetti regolati

I Introduzione

Con il Regolamento (UE) 2022/2554, in materia di resilienza operativa digitale (il *Digital Operational Reslience Act*, più noto come DORA), pubblicato nella Gazzetta ufficiale dell'Unione europea del 27 dicembre 2022, il legislatore UE, in risposta alla digitalizzazione dei modelli di *business* e operativi degli operatori del settore finanziario, ha inteso rafforzare e armonizzare a livello europeo la disciplina relativa alla gestione dei rischi connessi all'uso di servizi ICT, prevedendo regole uniformi per tutti i soggetti regolati che operano nel settore finanziario, dalle banche, alle assicurazioni, alle società di gestione del risparmio, fino ai nuovi attori come le piattaforme di *crowdfunding* e i *crypto-asset service provider*.

Sebbene DORA troverà applicazione solo a partire dal 17 gennaio 2025, si ritiene necessario che gli operatori del settore inizino sin d'ora a tenere conto delle regole previste dal nuovo Regolamento, in particolare nell'ambito della negoziazione dei contratti con i c.d. *third party provider* del settore ICT.

Questo rappresenta infatti uno degli aspetti forse meno noti ma di probabile maggiore impatto di DORA per due ordini di ragioni:

- in primo luogo, l'ampiezza della definizione di "servizi ICT" di cui all'articolo 3, n. 21), del Regolamento, che comprende i servizi digitali e di dati forniti attraverso sistemi di ICT a uno o più utenti interni o esterni su base continuativa, inclusi l'*hardware* come servizio e i servizi *hardware*, comprendenti la fornitura di assistenza tecnica mediante aggiornamenti di *software* e *firmware* da parte del fornitore dell'*hardware*;

- in secondo luogo, l'assenza di alcun regime transitorio o di *grandfathering* per i contratti esistenti, per effetto della quale questi - salvo che il legislatore europeo, con l'avvicinarsi della data di applicazione di DORA, decida di introdurre una proroga o delle disposizioni transitorie - dovranno essere rinegoziati qualora in sede di stipula non si sia potuto tenere conto del regime previsto da DORA.

II Gli obblighi contrattuali tra soggetti regolati e *third party provider*: spunti di riflessione nella (ri)negoziazione dei contratti

Prima di analizzare gli obblighi posti dalla nuova disciplina ed evidenziare alcuni elementi da considerare nella(ri)negoziazione dei contratti, occorre richiamare l'attenzione sul fatto che la nuova disciplina posta da DORA riguardante i rapporti con i fornitori terzi, compresi gli obblighi di contenuto minimo dei contratti, troverà applicazione in relazione a tutti i "*contractual arrangement*" instaurati tra operatori del settore finanziario e fornitori terzi riguardanti l'uso di servizi ICT, e non solo ai contratti di esternalizzazione.

Il superamento del concetto di *outsourcing* in DORA si riflette anche nelle regole riguardanti il rapporto tra il fornitore terzo e i suoi *sub-fornitori*: mentre infatti nella disciplina di settore le previsioni rilevanti sono quelle in materia di *sub-outsourcing*, in DORA tale concetto è sostituito da quello di *sub-contracting*.

Già da queste prime considerazioni, risulta evidente che ne deriveranno temi non secondari di coordinamento, dato che DORA affianca e non sostituisce la normativa in materia di esternalizzazione, come peraltro chiaramente affermato dal legislatore europeo nel Considerando 29 di DORA.

I principi fondamentali che guideranno i soggetti regolati nella gestione contrattuale dei rischi informatici derivanti da terzi sono stabiliti nel Capo V di DORA e delineano, di fatto, un intero processo di gestione delle terze parti finalizzato a monitorare efficacemente tutti i rischi informatici che insorgano a tale livello.

In tale processo, dopo le fasi di *assessment* dei rischi di fornitura e di valutazione preliminare del rischio di concentrazione, DORA, all'articolo 30, individua dettagliatamente il contenuto minimo dei contratti con i terzi. A tale contenuto minimo, in caso di contratti con fornitori a supporto di funzioni essenziali o importanti, andranno poi aggiunti ulteriori elementi che prevedano *inter alia* la fissazione di termini di preavviso e obblighi di segnalazione nei confronti dell'entità finanziaria, l'obbligo di partecipare e cooperare pienamente ai *Threat-Led Penetration Testing* cui questa è tenuta, il diritto di monitorare costantemente le prestazioni del fornitore terzo e le strategie di uscita, in particolare la definizione di un adeguato periodo di transizione obbligatorio.

Alla luce degli elementi di novità introdotti da DORA rispetto alla precedente normativa di settore, in questa sede si segnalano tre aspetti che riteniamo di particolare interesse ai fini della (ri)negoziazione dei contratti.

Il primo attiene ai livelli di servizio. DORA, all'articolo 30, par. 2, lett. e), prevede infatti che tutti i contratti con i fornitori terzi, compresi quindi quelli non a supporto di funzioni importanti, prevedano non solo la descrizione dei livelli di servizio, ma anche l'indicazione dei relativi processi periodici di revisione e aggiornamento. L'obbligo di concordare in sede contrattuale anche tale aspetto degli SLA dovrà quindi essere negoziato con particolare attenzione posto che i contratti di servizi ICT sono per definizione di durata ma soggetti a rapida obsolescenza, considerata la velocità dell'innovazione tecnologica.

Il secondo elemento attiene al contenuto minimo della clausola relativa ai diritti di *audit* del soggetto regolato nei confronti del fornitore di servizi ICT, che deve essere obbligatoriamente prevista per i contratti relativi all'uso di servizi ICT a supporto di funzioni essenziali o importanti. L'articolo 30, par. 3, lett. e) di DORA prevede infatti sul punto che il diritto di monitorare costantemente le prestazioni del fornitore terzo di servizi ITC comporta anche l'obbligo, per il soggetto regolato, di riconoscere al fornitore di servizi alcuni diritti connessi alle modalità di svolgimenti dell'*audit*. In particolare, si prevede il riconoscimento, in capo ai *service provider*, del diritto di concordare livelli di garanzia alternativi, qualora l'*audit* possa avere effetti pregiudizievoli per i diritti degli altri clienti del *provider*, e del diritto di ricevere dettagli sull'ambito di applicazione, sulle procedure da seguire e sulla frequenza di ispezioni e *audit*. Tali previsioni, unitamente all'introduzione di un regime di *oversight* per i *service provider* critici, sono indicative dell'attenzione che il legislatore europeo inizia a prestare anche alla sana e prudente gestione dei fornitori di servizi ICT per il ruolo cruciale svolto da questi ultimi ai fini della stabilità del sistema finanziario.

Il terzo elemento è l'introduzione dell'obbligo per il fornitore di servizi ICT previsto dall'articolo 30, par. 2, lett. f), di DORA di prestare assistenza al soggetto regolato senza costi aggiuntivi o a un costo stabilito *ex ante*, qualora si verifichi un incidente connesso al servizio ICT prestato, indipendentemente dal fatto che tale incidente sia dovuto a colpa del fornitore di servizi ICT o del soggetto regolato. In relazione a tale aspetto contrattuale, il punto negoziale più complesso sarà quindi quello della predeterminazione del costo dell'assistenza, vista la difficoltà di prevedere *ex ante* tutti i possibili casi di incidente ICT e i rimedi necessari per ciascuno di essi e potendosi ad esempio ipotizzare assetti incentrati sul calcolo dei "giorni uomo" richiesta per la gestione dell'incidente.