DB non solo diritto bancario

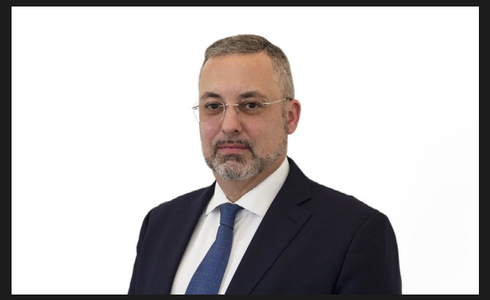
leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

DORA: gli adempimenti organizzativi, gestionali e documentali

Settembre 2024

Alessandro del Ninno, Partner, Fivers



Alessandro del Ninno, Partner, Fivers

Alessandro del Ninno

Alessandro del Ninno è titolare delle Cattedre di Informatica Giuridica e di Intelligenza Artificiale, Machine Learning e Diritto presso la LUISS Guido Carli di Roma. Avvocato del Foro di Roma e Socio dello Studio legale e tributario Fivelex. È altresì: Appointed member del Pool of Experts europei di supporto e consulenza al Comitato europeo per la protezione dei dati personali; Presidente del Comitato Scientifico dell'Associazione Nazionale per la protezione dei dati personali; Membro e Vicepresidente del Comitato Scientifico dell'Istituto Italiano Privacy.

Sommario: 1. Introduzione: una nuova cultura di impresa nella gestione del rischio informatico quale presupposto della corretta attuazione del Regolamento DORA; **2.** I nuovi compiti e le responsabilità operative dell'organo di gestione delle entità finanziarie: adempimenti organizzativi, gestionali e documentali; **2.1** Segue. Gli adempimenti organizzativi, gestionali e documentali a carico dell'organo di gestione per garantire standard elevati di accessibilità, disponibilità, autenticità, integrità e riservatezza dei dati personali e non personali. I rapporti tra DORA e GDPR.; **2.2** Segue. Definire chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC. Istituire efficaci canali di comunicazione tra reparti e funzioni dell'entità finanziaria. Gestire le risorse finanziarie da dedicare alla resilienza digitale.; **3.** L'impatto del Regolamento DORA sull'organigramma delle entità finanziarie: nuovi compiti a funzioni esistenti e nuovi ruoli alla luce della resilienza operativa digitale.;**4.** I nuovi adempimenti documentali previsti dal Regolamento DORA; inventari, registri e clausole contrattuali.; **5.** La centralità nel Regolamento DORA delle iniziative di sensibilizzazione e di formazione – ad ogni livello – in materia di rischi informatici e resilienza operativa digitale.; **6.** Conclusioni: il quadro normativo complessivo tra Regolamento DORA, Implementing e Regulatory Technical Standard e atti delegati della Commissione UE.

1. Introduzione: una nuova cultura di impresa nella gestione del rischio informatico quale presupposto della corretta attuazione del Regolamento DORA.

L'approssimarsi del 17 gennaio 2025 - data di applicabilità del *Regolamento 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario* (di seguito, per brevità, il "*Regolamento DORA*") – induce a svolgere qualche riflessione sul corretto approccio a tale complessa normativa, nell'ottica della *compliance* alle numerose prescrizioni che impongono onerosi adempimenti alle entità finanziarie[1] a cui il

1 Si ricordi che per "*entità finanziarie*" tenute all'osservanza del Regolamento DORA intendono: enti creditizi; istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366; prestatori di servizi di informazione sui conti; istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE; imprese di investimento; fornitori di servizi per le cripto-attività autorizzati ed emittenti di token collegati ad attività; depositari centrali di titoli; controparti centrali; sedi di negoziazione; repertori di dati sulle negoziazioni; gestori di fondi di investimento alternativi; società di gestione; fornitori di servizi di comunicazione dati; imprese di assicurazione e di riassicurazione; intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio; enti pensionistici aziendali o professionali; agenzie

vedi l'articolo online

Regolamento DORA si applica.

Sarebbe difatti un approccio miope quello che releghi il Regolamento DORA e la sua implementazione agli ambiti specificatamente tecnici, infrastrutturali e tecnologici a cui rinviano i concetti di gestione del "*rischio informatico*" e di "*resilienza*[2] *operativa digitale*". In altri termini: sarebbe un grave errore considerare l'implementazione del Regolamento DORA e le misure di gestione dei rischi informatici come questione di stretta pertinenza dei Dipartimenti IT.

La nuova normativa, difatti, richiede, in primo luogo, un nuovo approccio coerente e coordinato – quasi una nuova "cultura d'impresa" – alla gestione dei rischi informatici e alla prevenzione e gestione degli incidenti connessi alle tecnologie dell'Informazione e Comunicazione ("*TIC*"), passando da approccio *quantitativo* alla gestione dei rischi (fino ad ora basato sulla definizione di un requisito patrimoniale a copertura dei rischi informatici) a uno *qualitativo*, mirante a introdurre presso le entità finanziarie quelle "*capacità generali*" (cfr. Considerando 21 del Regolamento DORA) di protezione, individuazione, contenimento, ripristino e rimedio in relazione ai rischi e agli incidenti connessi alle TIC.

E, in effetti, il Regolamento DORA - che tramite il consolidamento e l'aggiornamento delle diverse norme sui rischi informatici, per la prima volta ha riunito in un unico testo normativo tutte le disposizioni in materia di *rischio digitale* nel settore finanziario prima sparse in un quadro legislativo frammentato e poco coordinato – mette al centro di questo sistema gestionale non una figura tecnica (es: il CTO – *Chief Technology Officer*, oppure il CISO – *Chief of Information Security Officer*, o analoghe figure dell'organizzazione aziendale) ma direttamente l'*organo di gestione*.

di rating del credito; amministratori di indici di riferimento critici; fornitori di servizi di crowdfunding; repertori di dati sulle cartolarizzazioni.

2 Per resilienza di intende la capacità di prevenire, attenuare, assorbire un incidente, di proteggersi da esso, di rispondervi, di resistervi, di adattarvisi e di ripristinare le capacità operative. Il Regolamento DORA offre anche una definizione tecnico-legale di *«resilienza operativa digitale»: la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni* [articolo 3, n. (1)].

Per comprendere meglio il concetto di una nuova "*cultura di impresa*" nella gestione dei rischi informatici, nonché il nuovo ruolo a cui è chiamato l'organo di gestione, è illuminante la lettura del *Considerando* 45 del Regolamento DORA:

"*45. Per garantire il pieno allineamento e la coerenza complessiva tra le strategie aziendali delle entità finanziarie, da un lato, e la gestione dei rischi informatici, dall'altro, è opportuno richiedere agli organi di gestione delle entità finanziarie di mantenere un ruolo attivo e fondamentale nella guida e nell'adeguamento del quadro per la gestione dei rischi informatici e della strategia globale di resilienza operativa digitale. Gli organi di gestione dovrebbero adottare un approccio che non consideri solamente i mezzi per assicurare la resilienza dei sistemi di TIC, ma si estenda anche alle persone e ai processi mediante un ventaglio di strategie che promuovano, a ciascun livello dell'azienda e per tutto il personale, un forte senso di consapevolezza dei rischi informatici nonché l'impegno a osservare a tutti i livelli una rigorosa igiene informatica (cyber hygiene). La responsabilità principale dell'organo di gestione nell'affrontare i rischi informatici di un'entità finanziaria dovrebbe concretizzarsi nel principio guida di tale approccio complessivo, tradotto ulteriormente nel costante coinvolgimento dell'organo di gestione a controllare il monitoraggio della gestione dei rischi informatici*".

Dunque, la nuova cultura di impresa si concretizza in un rinnovato sistema di *governance* e organizzazione (cfr. art. 5 Regolamento DORA) in cui diventa centrale la *strategia globale di resilienza operativa digitale* impostata, attuata e costantemente monitorata e aggiornata dall'organo di gestione.[3] E tale strategia è non solo tecnica, ma coinvolge tutto il personale e tutti i processi interni dell'entità finan-

3 L' "organo di gestione" costituente il centro di responsabilità complessiva e finale dell'attuazione di tutti gli obblighi del Regolamento DORA è definito in via generale come: *"l'organo - o gli organi - designato conformemente al diritto nazionale, cui è conferito il potere di stabilire gli indirizzi strategici, gli obiettivi e la direzione generale dell'entità, che supervisiona e monitora le decisioni della dirigenza e comprende persone che dirigono di fatto l'attività dell'ente"*. Questa definizione è identica in tutte le fonti normative alle quali il Regolamento DORA rinvia per l'individuazione – nello specifico settore bancario e finanziario - del concetto di organo di gestione o di amministrazione. Dove non c'è un organo di gestione, il Regolamento DORA imputa le prescrizioni alle "*persone equivalenti che gestiscono di fatto l'entità o che assolvono funzioni chiave conformemente al pertinente diritto dell'Unione o nazionale*" (cfr. art. 3, n. 30 Reg. DORA).

vedi l'articolo online

ziaria[4].

Il presente contributo intende allora analizzare – in particolare – non i profili e gli adempimenti specificatamente tecnico-informatici introdotti dal Regolamento DORA in tema di gestione dei rischi informatici e perseguimento d i una globale resilienza operativa digitale, bensì concentrarsi sulle procedure gestionali ed organizzative, sui ruoli (anche nuovi) della dirigenza e del personale, sulla nuova documentazione che le entità finanziarie – mediante l'organismo di gestione, che ne assume integrale responsabilità - devono predisporre, attuare e monitorare nel quadro di un rinnovato sistema di *governance* e organizzazione della sicurezza in senso lato.

2. I nuovi compiti e le responsabilità operative dell'organo di gestione delle entità finanziarie: adempimenti organizzativi, gestionali e documentali.

Come detto, al centro del sistema volto alla attuazione della *strategia globale di resilienza operativa digitale* c'è l'organo di gestione dell'entità finanziaria, che assume la piena, complessiva e finale responsabilità della predisposizione del cosiddetto *quadro per la gestione dei rischi informatici* (cfr. Art. 6 Regolamento DORA) da predisporre, documentare e monitorare nell'ambito del sistema di gestione globale del rischio.

Dal momento che il *quadro per la gestione dei rischi informatici* è un insieme di strategie, politiche, procedure, protocolli e strumenti in materia di TIC necessari per proteggere debitamente e adeguatamente tutti i *patrimoni informativi* (sostanzialmente le informazioni cruciali dal punto di vista commerciale, operativo e finanziario dell'entità) e le risorse TIC, compresi software, hardware e server, nonché tutte le pertinenti infrastrutture e componenti fisiche, quali i locali, i centri di elaborazione dati e le aree designate come sensibili, così da garantire che tutti i patrimoni informativi e i risorse TIC siano

4 Un aspetto che non va mai dimenticato nella corretta impostazione delle attività di *compliance* al Regolamento DORA è l'attuazione dei numerosi e complessi adempimenti alla luce del *principio di proporzionalità*. L'articolo 4 del Regolamento DORA – appunto rubricato "*Principio di proporzionalità*" – rappresenta una sorta di bussola operativa a cui detti piani di *compliance* devono ispirarsi: le entità finanziarie gli obblighi previsti tenendo conto delle loro dimensioni e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività. E le stesse autorità competenti valutano il grado di conformità al Regolamento DORA delle entità finanziarie tenendo in considerazione il medesimo principio di proporzionalità.

adeguatamente protetti contro i rischi, compresi i danneggiamenti e l'accesso o l'uso non autorizzati, risulta evidente che i componenti dell'organo di gestione debbano avere - in proprio - le competenze e le *capacità generali*, anche di natura tecnica, per assolvere i rilevanti compiti assegnati[5]. È altresì conseguente – anche in termini di azioni di responsabilità – che l'incompetenza e/o la insufficiente capacità dei componenti dell'organo di gestione diventano a loro volta *rischi* da evitare e presidiare. In tale prospettiva l'articolo 5, comma 4, del Regolamento DORA prevede che i membri dell'organo di gestione dell'entità finanziaria debbano mantenere attivamente aggiornate conoscenze e competenze adeguate per comprendere e valutare i rischi informatici e il loro impatto sulle operazioni dell'entità finanziaria, anche seguendo una *formazione specifica* su base regolare, commisurata ai rischi informatici gestiti.

Centrale diviene dunque – anche come procedura a se stante di gestione del rischio – la *formazione* dei membri dell'organo di gestione, obbligo che le entità finanziarie (e gli stessi membri dell'organo di gestione) non dovrebbero prendere alla leggera (ad esempio partecipando a generiche iniziative di aggiornamento professionale), sia perché la norma ne prevede precise caratteristiche e contenuti (*adeguatezza* della formazione rispetto alla finalità di comprendere e valutare tecnicamente i rischi informatici e il loro impatto sulla operatività; *diversificazione* della formazione, che va commisurata ai rischi informatici gestiti dal membro dell'organo di gestione; *specificità* della formazione; *periodicità* su base regolare), sia perché l'articolo 50 (*Sanzioni amministrative e misure di riparazione*) del Regolamento DORA prevede che le autorità competenti alle quali gli Stati Membri hanno affidato il potere di imporre sanzioni amministrative e misure di riparazione potranno comminarle direttamente nei confronti di membri dell'organo di gestione e di altre persone che, ai sensi del diritto nazionale, siano responsabili di violazioni (cfr. art 50, comma 5 del Regolamento DORA).

Sulla formazione in materia di rischi informatici come obbligo fondamentale per le entità finanziarie si tornerà nel prosieguo del presente contributo. È invece ora opportuno analizzare quali sono i compiti *non tecnici*, le procedure gestionali ed organizzative nonché la documentazione da predisporre e attuare ad opera dell'organo di gestione.

5 È vero che le entità finanziarie possono esternalizzare a imprese interne o esterne al gruppo i compiti di verifica della conformità ai requisiti in materia di gestione dei rischi informatici, ma esse – e di conseguenza anche l'organo di gestione – restano completamente responsabili.

vedi l'articolo online

2.1 Segue. Gli adempimenti organizzativi, gestionali e documentali a carico dell'organo di gestione per garantire standard elevati di accessibilità, disponibilità, autenticità, integrità e riservatezza dei dati personali e non personali. I rapporti tra DORA e GDPR.

Tra i principali compiti di tipo organizzativo, gestionale e documentale demandati dal Regolamento DORA all'organo di gestione vi è l'obbligo di predisporre "*politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati*" [cfr. art. 5, comma 2, lettera (b) del Regolamento DORA].

Va in prima battuta evidenziato che il Regolamento DORA non fornisce una definizione di "*dati*", né elenca formalmente, all'articolo 3, per rinvio (come spesso accade in altre normative) le formali definizioni di dato personale[6] e di dato non personale[7] come contenute nelle rispettive normative. Vi è anche da sottolineare – più in generale – che le recenti leggi del cosiddetto *Decennio Digitale della UE* hanno introdotto politiche di *governance* dei dati che hanno modificato la prospettiva per cui – soprattutto a partire dal 2018, con l'emanazione del GDPR – si era posto al centro del dibattito e della disciplina giuridica il *dato personale*. Oggi, a parere di chi scrive, viviamo una situazione assai diversa dalla impostazione appena riferita. Non che abbia perso centralità o importanza il "*dato personale*", ma ci si è resi sempre più conto in questi anni del valore (anche commerciale), della rilevanza e della necessità di un approccio rinnovato ai *dati non personali*. Di ciò troviamo un riflesso in molte normative, che – da un lato – offrono una nuova e complessiva definizione del concetto di "*dati*"[8] e – dall'altro – pongono sullo stesso piano i dati personali e non personali nella prospettiva della loro protezione e del loro sfruttamento. Per fare solo un esempio, appare illuminante la definizione che – proprio nel comparto bancario e finanziario – è offerta dall'articolo 3, n. 3 della proposta di *Regolamento relativo a un quadro per l'accesso ai dati finanziari* nell'ambito del pacchetto normativo c.d. FIDA: *"dati del cliente": dati personali e non personali raccolti, conservati e altrimenti trattati da un ente finanziario nell'ambito della sua normale attività commerciale con i clienti, che comprendono sia i dati forniti da un cliente sia i dati generati dall'interazione del cliente con l'ente finanziario.*

Quali *dati*, dunque, deve debitamente proteggere, e con specifiche politiche, l'organo di gestione ai sensi del Regolamento DORA?

Intanto, ogni volta che il Regolamento DORA fa riferimento ai "*dati*" si devono ritenere implicati sia i "*dati personali*" che quelli "*non personali*".

Inoltre, il Regolamento DORA ha introdotto alcuni concetti e definizioni giuridiche (non sempre felici) come quella di «patrimonio *informativo*»: *una raccolta di informazioni, tangibili o intangibili, che* è *importante proteggere* (questa definizione crea più confusione interpretativa che chiarezza...).

Ancora, molto spesso il Regolamento DORA menziona concetti generici come "*informazioni sensibili*" (cfr. art. 21) o "*informazioni riservate dell'entità finanziaria*" (cfr. art. 27).

Indipendentemente dalla maggiore o minore precisione lessicale e definitoria, non vi è dubbio che l'organo di gestione delle entità finanziarie debba predisporre politiche di protezione *ad hoc* di tutto il complesso di dati personali e non personali, di informazioni, di patrimoni informativi, etc garantendo l'*accessibilità*, la *disponibilità, l'autenticità, l'integrità e la riservatezza dei dati*. Le caratteristiche di *accessibilità, disponibilità, autenticità, integrità e riservatezza dei dati* sono una delle articolate declinazioni del più ampio concetto di "*sicurezza dei dati*" e vengono mutuate dal mondo *data protection*, anche se – come indicato più sopra – il Regolamento DORA estende anche ai dati non personali l'obbligo di garantire mediante idonee politiche tecniche e organizzative la loro autenticità, integrità, disponibilità e riservatezza.

La sicurezza di (tutti) i dati va garantita sia sotto un profilo tecnico, che sotto un profilo documentale e organizzativo. Anche se i profili tecnici non sono oggetto di approfondimento in tale sede, va comun-

6 Cfr. art. 4, n. 1 del Regolamento Generale UE 679/2016 sulla protezione dei dati personali: «dato personale»: *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

7 Cfr. art. 3, n. 1 del Regolamento (UE) 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea: «*dati*»: *i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679*".

8 La definizione di "*dati*" è identica in normative quali: il Regolamento 2022/868 (Data Governance Act), il Regolamento 2023/2854 (Data Act), il Regolamento 2022/1925 (Digital Markets Act), ed è la seguente: "*«dati»: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva*".

que ricordato che ogni evento che compromette la sicurezza dei sistemi informatici e di rete (a loro volta da proteggere adeguatamente) e ha un impatto avverso sulla disponibilità, autenticità, integrità o riservatezza dei dati o sui servizi forniti dall'entità finanziaria è – tecnicamente e a seconda dei casi – un "*incidente connesso alle TIC*" o un "*incidente operativo o di sicurezza dei pagamenti*", che possono poi essere "*incidenti gravi*" se i sistemi informatici e di rete colpiti sono a supporto delle funzioni *essenziali* o *importanti* o dei servizi di pagamento dell'entità finanziaria. L'organo di gestione è chiamato ad impostare "*elevati standard di disponibilità, autenticità, integrità o riservatezza dei dati*" sia in sede preventiva (es: procedure di backup – cfr. art.12 del Regolamento DORA – procedure di *audit* tecnico, procedure di *penetration test*, ai sensi degli articoli 26 e 27, etc) che successiva al verificarsi di incidenti (piani di ripristino, *disaster recovery*, *business continuiity*, notifiche degli incidenti alle autorità competenti, alla clientela, ai portatori di interessi, etc).

Garantire invece la accessibilità, autenticità, integrità, disponibilità e riservatezza dei dati da un pinto di vista organizzativo, documentale e gestionale significa per l'organo di gestione approntare quanto segue.

Intanto, le nuove procedure di qualifica e di contrattualizzazione dei fornitori terzi di servizi TIC (cfr. artt. 28 e ss. del Regolamento DORA e il successivo paragrafo 4) impongono alle entità finanziarie di effettuare una *due diligence* dei potenziali fornitori che include anche la loro idoneità sotto il profilo delle garanzie di protezione dei dati personali e non personali.

Gli accordi contrattuali con i fornitori per l'utilizzo di servizi TIC comprendono inoltre – tra le clausole obbligatorie – alcune disposizioni che rendono centrale in tali accordi la disciplina negoziale dei dati personali e non personali implicati dalla fornitura. Non dunque clausole di stile, meramente burocratiche e inutilmente formali, come spesso si vede nei contrati di settore. In primo luogo – infatti - i contratti con i fornitori di terzi di servizi TIC (che rappresentano uno specifico rischio da presidiare, si veda *infra*) devono includere specifiche "*disposizioni in materia di disponibilità, autenticità, integrità e riservatezza in relazione alla protezione dei dati, compresi i dati personali*" [cfr. art.30, comma 2, lettera c del Regolamento DORA] comunque "*conservati, in uso o in transito*" sui sistemi. In secondo luogo, nei casi di insolvenza, risoluzione o interruzione delle operazioni commerciali del fornitore terzo di servizi TIC o in caso di risoluzione degli accordi commerciali, fin dall'inizio i contratti devono prevedere specifiche disposizioni relative alle garanzie di accesso, ripristino e restituzione, in un formato facilmente accessibile, di dati personali e non personali trattati dall'entità finanziaria [cfr. art. 30, comma 2, lettera d) del Regolamento DORA]. Tra l'altro, proprio in tema di risoluzione del contratto, una causa di risoluzione *ex lege* che va inserita negli accordi riguarda il caso dei "*punti deboli del fornitore terzo di servizi TIC emersi riguardo alla sua gestione complessiva dei rischi informatici e, in particolare, nel modo in cui il fornitore garantisce la disponibilità, autenticità, integrità e riservatezza dei dati, siano essi dati personali o altrimenti sensibili, oppure dei dati non personali*" [cfr. art. 28, comma 7, lettera c) del Regolamento DORA].

Con riferimento alla specifica prospettiva dei *dati personali*, diviene dunque fondamentale nella *governance* della entità finanziaria coordinare il Regolamento DORA con il Regolamento generale della UE sulla protezione dei dati personali 679/2016 ("GDPR").

Questo vale sia in generale che in merito alle specifiche clausole dei contratti con i fornitori terzi di servizi TIC. In via generale, difatti, quando l'organo di gestione è chiamato dal Regolamento DORA a predisporre le politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati, ciò significa che potrà basarsi sul lavoro di *compliance* al GDPR che l'entità finanziaria fin dal 2018 avrà realizzato, introducendo politiche sul trattamento dei dati, documenti, procedure *data protection* e misure di sicurezza[9]che oramai dovrebbero essere consolidate e rodate da anni. E non è illogico suggerire di estendere alla tutela dei dati non personali le medesime procedure e misure organizzative, documentali e tecniche vigenti nell'entità finanziaria ai sensi del GDPR (ovviamente adattandole, stante il carattere non personale dei dati da tutelare: ad esempio non si applicherà la procedura di gestione dei diritti degli interessati, ma potranno essere applicabili misure di tutela del know-how o dei diritti di proprietà intellettuale e/o industriale). Né è illogico adattare alcune procedure GDPR in chiave DORA: si pensi alla procedura per le notifiche di incidente che riguarda le TIC ai clienti o alle autorità compenti richieste agli articoli 17 e 19 del Regolamento DORA: il Legislatore DORA muta molti aspetti delle procedure di notifica dal mondo *data protection* e dalle procedure di notifica e comunicazione delle violazioni di dati personali (*data breach*) disciplinati dagli articoli 33 e 34 del GDPR.

Anche l'implementazione delle misure pre-contrattuali e contrattuali per la gestione del rischio rappre-

9 Cfr. artt. 24 e 32 del Regolamento 679/2016.

sentato dai fornitori terzi di servizi TIC vede nelle verifiche GDPR un presidio fondamentale. Ad esempio, in sede di *due diligence* obbligatoria dei potenziali fornitori l'entità finanziaria controllerà anche tutte le procedure in essere presso il fornitore per garantire la *compliance* a tutte le misure organizzative, documentali e tecniche previste dal GDPR. Si suggerisce, ad esempio, di farsi consegnare dal fornitore (ove sia obbligatoria la redazione e la tenuta) il registro delle attività di trattamento (art. 30 GDPR); di verificare se il fornitore ha nominato il *Responsabile della Protezione dei dati personali* (RPD/DPO) ricorrendone i presupposti obbligatori di cui all'art. 37 del GDPR; di farsi consegnare le istruzioni scritte sul trattamento dei dati personali che tale fornitore deve aver rilasciato al personale (le cosiddette "*persone autorizzate al trattamento*" ai sensi dell'art. 29 e 32, comma 4 del GDPR o soggetti designati ai sensi dell'art. 2-*quaterdecies* del Codice della privacy), di rendere disponibile la documentazione sulle misure di sicurezza implementate dal fornitore ai sensi dell'art. 32 del GDPR, la documentazione su eventuali trasferimenti leciti dei dati personali al di fuori dello Spazio Economico europeo (eventualità assai frequente, ad esempio nell'ambito della fornitura di servizi c*loud*), la documentazione su come il fornitore gestisce le richieste di esercizio dei diritti degli interessati ai sensi egli artt. 15-22 del GDPR, la documentazione sul *design* dei servizi e dei sistemi TIC offerti dal fornitore, ai sensi dei principi di *privacy by design* e *privacy by default* di cui all'art. 25 del GDPR, la documentazione su come il fornitore gestisce le eventuali violazioni di dati personali, facendosi consegnare la apposita procedura di *data breach*, e – infine – di verificare l'eventuale possesso di certificazioni ai sensi dell'art. 42 del GDPR o l'adesione del fornitore a codici di condotta ai sensi dell'art. 40 del GDPR.

Ovvio che tale approfondito controllo in sede di *due diligence*, ove l'esito sia positivo e il fornitore terzo di servizi TIC venga poi contrattualizzato, sarà utile anche per strutturare successivamente il contenuto – sostanziale e non di mera forma - delle specifiche clausole contrattuali che il Regolamento DORA ha reso obbligatorie in tema di garanzie di disponibilità, autenticità, integrità e riservatezza dei dati. E sarà altresì utile anche per formalizzare la designazione del fornitore terzo di servizi TIC – se del caso – come responsabile del trattamento dei dati personali ai sensi dell'articolo 28 del GDPR[10].

10 Si ricordi che la designazione dei fornitori come Responsabili del trattamento ai sensi dell'articolo 28 del GDPR non è un automatismo, nel senso che devono essere nominati tali solo le persone fisiche o giuridiche che trattano i dati *per conto* del Titolare del trattamento e su istruzione documentata e nell'interesse di quest'ultimo, senza poter prendere alcuna decisione sulle finalità del trattamento, ma potendo godere di una certa discrezionalità decisoria in merito alle modalità e ai mezzi del trattamento. Per la individuazione della corretta soggettività *data protection*, da valutarsi sempre caso per caso, si rinvia alle *Linee Guida 7/2020 sui concetti di Titolare del trattamento e di Responsabile del trattamento nel Regolamento 679/2016* come adottate dal Comitato europeo per la protezione dei dati personali.

Va poi sottolineato, anche se il Regolamento DORA non lo menziona mai, che il DPO dell'entità finanziaria (figura che – come è noto - è obbligatoria – tra gli altri - per banche e assicurazioni) assume un ruolo centrale per supportare l'organo di gestione nell'adempimento del compito di predisporre politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati. Uno snodo pratico centrale sarà dunque quello di verificare l'efficace coordinamento e l'esistenza di solidi canali di comunicazione tra DPO e organo di gestione (coordinamento che già dovrebbe essere rodato da anni, visti gli obblighi in materia previsti sia dal GDPR che dalle *Linee Guida sul DPO*[11] del Comitato europeo per la protezione dei dati personali – EDPB).

Infine, un ulteriore punto di contatto tra DORA e GDPR è dato dall'articolo 45 del Regolamento DORA. Tale norma disciplina la istituzione di meccanismi su base facoltativa e volontaria per l'interscambio tra entità finanziarie di informazioni e analisi delle minacce informatiche, tra cui indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cibersicurezza e strumenti di configurazione. Ciò, al fine di potenziare la rispettiva resilienza operativa digitale, in particolare aumentando la consapevolezza in merito alle minacce informatiche, contenendo o inibendo la capacità della loro diffusione, sostenendo le capacità di difesa, le tecniche di individuazione delle minacce, le politiche di mitigazione o le fasi di risposta e ripristino. La istituzione di tali meccanismi implica la necessità che – in caso di dati personali – la condivisione tra "*comunità fidate di entità finanziare*" avvenga in piena conformità al GDPR (quanto, ad esempio, alla base di legittimità della comunicazione a terzi dei dati, che può ben essere il legittimo interesse dell'entità finanziaria che condivide quale Titolare del trattamento o l'adempimento del medesimo articolo 45 del Regolamento DORA). Inoltre, l'articolo 45, comma 1, lettera (c) prescrive che i meccanismi di condivisione delle informazioni – ove attuati – debbano fondarsi su specifiche *norme di condotta* (applicabili ai partecipanti) "*pienamente rispettose della riservatezza dell'attività economica, della protezione dei dati personali ai sensi del regolamento (UE) 2016/679 e delle*

11 Cfr. le Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016 Adottate il 13 dicembre 2016 e emendate il 5 aprile 2017.

vedi l'articolo online

linee guida sulla politica in materia di concorrenza". Dunque, una ulteriore politica interna che l'entità finanziaria – nei casi di adesione a meccanismi di condivisione – dovrà predisporre e adottare.

2.2 Segue. Definire chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC. Istituire efficaci canali di comunicazione tra reparti e funzioni dell'entità finanziaria. Gestire le risorse finanziarie da dedicare alla resilienza digitale.

Tra i compiti operativi della rinnovata *governance* aziendale che il Regolamento DORA pone a carico dell'organo di gestione, vi è anche quello di definire chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC (non a tutte le TIC, lo si ricordi, ma a quelle che sostengono i processi commerciali delle entità finanziarie) e stabilire adeguati meccanismi di *governance* al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi tra tali funzioni [cfr. art. 5, comma 2, lettera c) del Regolamento DORA].

Questo compito implica una attenta analisi – per tutte le funzioni – dei ruoli e delle responsabilità ricoperte da ogni membro del personale e del *management* dell'entità finanziaria nella specifica prospettiva della connessione tra gli addetti e le TIC da questi impiegate/utilizzate a sostegno dei processi commerciali. Va analizzato – cioè – in che misura risulti centrale per ciascun addetto nell'espletamento dei compiti e delle responsabilità affidate l'utilizzo o il supporto delle TIC nella gestione da parte sua dei processi commerciali in cui il medesimo addetto è coinvolto. Tra l'altro, tale censimento generale appare preordinato all'altro obbligo previsto dall'articolo 8 del Regolamento DORA e per cui nell'ambito del *quadro per la gestione dei rischi informatici*[12] le entità finanziarie devono identificare, classificare e documentare adeguatamente tutte le funzioni commerciali supportate dalle TIC, i ruoli e le responsabilità, i patrimoni informativi e le risorse TIC a supporto delle suddette funzioni, nonché i ruoli e le dipendenze rispettivi in materia di rischi informatici, riesaminando secondo necessità e almeno una volta all'anno, l'adeguatezza di tale classificazione e di altri documenti eventualmente pertinenti. Dunque, un'altra procedura di carattere gestionale, documentale ed operativa che appare centrale nell'ottica della compliance ai numerosi obblighi del Regolamento DORA.

Tra l'altro, una volta definiti – nell'ottica sopra specificata – ruoli e responsabilità all'interno delle varie funzioni dell'entità finanziaria, l'organo di gestione dovrà altresì stabilire adeguati meccanismi di *governance* al fine di garantire una (1) comunicazione, una (2) cooperazione e un (3) coordinamento efficaci e tempestivi tra tali funzioni, nell'ottica del coinvolgimento delle funzioni nella implementazione del quadro di gestione dei rischi informatici e dell'attuazione della resilienza operativa digitale come previsto dal Regolamento DORA. In tale prospettiva può ritenersi opportuna la istituzione da parte dell'organo di gestione di un Comitato interno/Steering Committee composto dai rappresentanti di tutte le funzioni (e anche da chi ricopre i nuovi ruoli che il Regolamento DORA istituisce: si veda il paragrafo 4), che si riunisca periodicamente e funga da centro di coordinamento tra le funzioni e di ricezione/smistamento di tutte le necessarie comunicazioni tra organo di gestione e varie funzioni e tra varie funzioni tra di loro.

Sul tema dei necessari meccanismi di comunicazione da istituire per garantire una sempre rapida ed efficace circolazione delle informazioni, assume particolare rilevanza la gestione delle comunicazioni contrattuali. L"organo di gestione – difatti – deve istituire un canale diretto di comunicazione con le pertinenti funzioni per essere sempre debitamente informato e aggiornato (dalle funzioni che si occupano della gestione della qualifica e contrattualizzazione dei fornitori terzi di servizi TIC) in merito agli accordi conclusi con i fornitori terzi di servizi TIC sull'uso di tali servizi; circa le eventuali modifiche importanti e pertinenti (si pensi ad esempio al caso di cambiamento di un fornitore di servizi TIC ed alle necessarie valutazioni sulla *concentrazione* e sulla *dipendenza* – si veda *infra* – o alla tematica delicata della gestione degli *outsourcing* in subappalto) e in merito al potenziale impatto di tali modiche sulle funzioni *essenziali* o *importanti* soggette agli accordi in questione. In tali casi, la funzione competente deve sempre fornire all'organo di gestione una specifica sintesi dell'analisi del rischio per valutare l'impatto di tali modifiche, nonché indicazioni sui gravi incidenti TIC (legati alle modifiche) e il loro impatto, le misure di risposta e ripristino e le misure correttive. Dal momento che il Regolamento DORA prescrive anche il ruolo – da istituire *ex novo* o da assegnare a un dirigente esistente, purché di rango

12 Si ricordi che ai sensi dell'articolo 6, commi 1 e 2 del Regolamento DORA, nell'ambito del sistema di gestione globale del rischio, le entità finanziarie devono predisporre un *quadro per la gestione dei rischi informatici* composto da strategie, politiche, procedure, protocolli e strumenti in materia di TIC che consenta loro di affrontare i rischi informatici in maniera rapida, efficiente ed esaustiva e di proteggere debitamente e adeguatamente contro i rischi (compresi i danneggiamenti e l'accesso o l'uso non autorizzati) tutti i patrimoni informativi e i risorse TIC, i software, gli hardware e i server, nonché i locali, i centri di elaborazione dati e le aree designate come sensibili.

elevato – di sorvegliante degli accordi contrattuali conclusi dall'entità finanziaria con i fornitori terzi di servizi TIC, per monitorare la esposizione al rischio derivante dagli accordi con i terzi fornitori di servizi TIC, è conseguente che l'obbligo di istituire un canale di comunicazione diretta per il monitoraggio di tali accordi contrattuali vedrà la necessaria centralità di tale nuova figura, che dovrà coordinarsi con l'organo di gestione e con le funzioni pertinenti.

Infine, tutti gli onerosi adempimenti organizzativi e gestionali per far sì che l'entità finanziaria sia integralmente conforme a quanto previsto dal Regolamento DORA passano attraverso una oculata pianificazione delle esigenze finanziarie per attuare tutto il necessario. L'organo di gestione è chiamato ad assegnare e riesaminare periodicamente le risorse finanziarie adeguate a soddisfare le esigenze di resilienza operativa digitale dell'entità finanziaria. Ciò implica, ad esempio, valutare i differenti costi derivanti dalla decisione di affidare o meno – come il Regolamento consente – a società esterne in outsourcing l'attuazione di adempimenti quali la strutturazione del quadro di gestione dei rischi informatici, o lo svolgimento degli audit, etc. Particolare attenzione deve essere inoltre dedicata dall'organo di gestione alla copertura finanziaria dei programmi di sensibilizzazione sulla sicurezza delle TIC e delle attività di formazione sulla resilienza operativa digitale per tutto il personale.

3. L'impatto del Regolamento DORA sull'organigramma delle entità finanziarie: nuovi compiti a funzioni esistenti e nuovi ruoli alla luce della resilienza operativa digitale.

Il Regolamento DORA impatta fortemente non solo sul ruolo, sui compiti e sulle funzioni dell'organo di gestione, ma impone alle entità finanziarie – a più ampio raggio – di assegnare nuovi compiti a funzioni esistenti o di istituire nuovi ruoli nella complessiva rivisitazione della *governance* in materia di gestione dei rischi informatici e attuazione della resilienza operativa digitale.

Alcune funzioni e taluni ruoli hanno caratteristiche eminentemente tecniche. Ad esempio, le entità finanziarie devono attribuire la responsabilità della gestione e della sorveglianza dei rischi informatici a una funzione di controllo, di cui assicurano un livello appropriato d'indipendenza per evitare conflitti d'interessi[13].

In altri scenari, la figura/funzione/ruolo appare di natura mista: è il caso, ad esempio, dell'obbligo per le entità finanziarie di dotarsi di una funzione di gestione delle crisi a seguito di incidenti o attacchi informatici. Questa figura appare tecnica (interviene anche in caso di attivazione dei piani di continuità operativa delle TIC o dei piani di risposta agli incidenti e ripristino relativi alle TIC) ma – per altro verso - deve avere anche competenze nel campo della comunicazione, se è vero che il Regolamento gli richiede di fissare, tra l'altro, procedure chiare per la gestione della comunicazione interna (al personale) ed esterna delle crisi.

Sul punto, l'articolo 14 ("*Comunicazione*") del Regolamento DORA prescrive alle entità finanziarie di prevedere all'interno del quadro per la gestione dei rischi informatici degli specifici piani di comunicazione delle crisi che consentano una divulgazione responsabile - ai clienti e alle controparti nonché al pubblico, a seconda dei casi - delle informazioni riguardanti, almeno, gravi incidenti connessi alle TIC o vulnerabilità.

Sempre all'interno del quadro per la gestione dei rischi informatici, le entità finanziarie sono inoltre chiamate ad attuare politiche di comunicazione per il personale interno e per i portatori di interessi esterni. Le politiche di comunicazione per il personale devono tenere conto dell'esigenza di operare un distinguo tra il personale coinvolto nella gestione dei rischi informatici (saranno ovviamente comunicazioni a più elevato tasso tecnico), il personale responsabile della risposta e del ripristino, e il personale che è comunque necessario informare.

Deve essere inoltre affidato ad (almeno) una persona incaricata il compito di attuare la strategia di comunicazione per gli incidenti connessi alle TIC (predisposta dalla funzione competente, come visto) che proceda a informare il pubblico e i media: sembrerebbe una funzione tipica di Ufficio Stampa o di Responsabile della Comunicazione dell'ente. Dunque, nel riparto di competenze, sembrerebbe che l'addetto (o gli addetti) della funzione di gestione delle crisi a seguito di incidenti o attacchi informatici

13 Deve essere difatti garantita la separazione e indipendenza tra funzione di gestione dei rischi informatici, funzione di controllo e funzione di audit interno, secondo il modello cosiddetto delle tre linee di difesa.

adotta/adottano gli specifici piani di comunicazione delle crisi e procede/procedono alla comunicazione al personale, ai clienti, alle controparti e ai portatori di interessi, mentre appare compito della diversa persona incaricata la comunicazione al pubblico e ai media in merito alla crisi.

Innovativo è poi il ruolo a cui viene attribuito lo specifico compito di monitorare gli accordi contrattuali conclusi dall'entità finanziaria con i fornitori terzi di servizi TIC per l'uso di tali servizi (altro presidio di rischio). Tale ruolo può essere istituito *ex novo,* oppure può attribuirsi la relativa competenza a un dirigente di rango elevato, il quale sarà appositamente designato quale responsabile della sorveglianza sulla esposizione al rischio derivante dagli accordi contrattuali stipulati con i fornitori terzi e sulla relativa documentazione pertinente.

Si ricordi - in merito a questa figura da ultimo esaminata - il necessario coordinamento con l'organo di gestione, a cui più sopra si è già fatto cenno. Come già illustrato, difatti, l'organo di gestione ha l'obbligo di approvare e riesaminare periodicamente la politica dell'entità finanziaria sui contratti per l'uso dei servizi TIC prestati dai fornitori terzi di servizi TIC e deve istituire a livello aziendale specifici canali di comunicazione che gli consentano di essere sempre debitamente informato:

i) sugli accordi conclusi con i fornitori terzi di servizi TIC sull'uso di tali servizi;

ii) sulle relative eventuali modifiche importanti e pertinenti previste riguardo ai fornitori terzi di servizi TIC;

iii) sul potenziale impatto di tali modiche sulle *funzioni essenziali o importanti*[14] soggette agli accordi in questione, compresa una sintesi dell'analisi del rischio per valutare l'impatto di tali modifiche, nonché almeno gli gravi incidenti TIC e il loro impatto, le misure di risposta e ripristino e le misure correttive.

Appare conseguente che il responsabile della sorveglianza sulla esposizione al rischio derivante dagli accordi contrattuali stipulati con i fornitori terzi (ruolo appositamente istituito oppure funzione assegnata ad alto dirigente esistente dell'entità finanziaria) debba essere l'interfaccia principale dell'organo di gestione in tale prospettiva.

Continuando l'esame dell'impatto del Regolamento DORA sull'organigramma delle entità finanziarie, va ricordato che nell'ambito del processo di gestione degli incidenti connessi alle TIC - e al fine di individuare, gestire e notificare tali incidenti - le entità finanziarie devono adeguare l'organigramma assegnando ruoli e responsabilità necessari per i diversi scenari e tipi di incidenti connessi alle TIC.

Infine, si richiama quanto più sopra già illustrato in merito al fondamentale compito dell'organo di gestione di definire chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC, stabilendo adeguati meccanismi di *governance* al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi tra i vari ruoli e le varie funzioni.

4. I nuovi adempimenti documentali previsti dal Regolamento DORA; inventari, registri e clausole contrattuali.

Oltre alla considerazione che il Regolamento DORA prescrive alle entità bancarie, finanziarie e assicurative di dotarsi delle specifiche politiche e procedure tecnico-informatiche (ovviamente anche documentali[15]) nell'ambito del quadro di gestione dei rischi informatici, vi sono anche alcune specifiche prescrizioni del Regolamento che hanno introdotto l'obbligo di dotarsi di nuovi documenti interni - non necessariamente tecnici o di *security* in senso stretto – che le entità finanziarie devono redigere, mantenere e aggiornare periodicamente – almeno una volta all'anno o in occasione di qualsiasi modifica di rilievo – come ad esempio inventari, registri, modelli contrattuali, etc.

14 Nel Regolamento DORA è centrale la definizione di «*funzione essenziale o importante*» perché gli obblighi in materia di gestione dei rischi informatici e di segnalazione degli incidenti che riguardano i servizi TIC sono diversi a seconda che tali servizi siano o meno a supporto di una «*funzione essenziale o importante*» e cioè: "*una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività, o la cui esecuzione interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi inerenti alla sua autorizzazione o di altri obblighi previsti dalla normativa applicabile in materia di servizi finanziari*".

15 D'altra parte, il quadro per la gestione dei rischi informatici "*comprende almeno strategie, politiche, procedure, protocolli e strumenti in materia di TIC*" e "*va documentato*" (cfr. art. 6, commi 1 e 2 del Regolamento DORA) e inoltre, sono comunque da documentare (anche) in appositi atti: (1) la strategia di resilienza operativa digitale; (2) le politiche miranti a garantire la resilienza, la continuità e la disponibilità dei sistemi di TIC; (3) l'organizzazione dei piani di audit interno; (4) la politica di continuità operativa delle TIC; (5) i piani di risposta e ripristino relativi alle TIC, etc

Questi documenti, la loro redazione e aggiornamento hanno un impatto sui profili gestionali e organizzativi dell'entità finanziaria.

Ad esempio, un primo inventario – di natura organizzativa – è quello che le entità finanziarie devono redigere per classificare e documentare tutte le funzioni commerciali supportate dalle TIC (quindi va integrato l'organigramma con l'evidenza delle funzioni che usano tool, devices, servizi, programmi e risorse TIC che sostengono i processi commerciali[16]), i rispettivi ruoli ricoperti da chi opera in queste funzioni così individuate, con l'evidenza delle relative responsabilità, i patrimoni informativi[17] coinvolti e le specifiche risorse TIC a supporto delle suddette funzioni (cioè tutto il software o l'hardware presenti nei sistemi informatici e di rete utilizzati dall'entità finanziaria a supporto dei processi commerciali, con l'ulteriore obbligo di individuare le risorse TIC ritenute essenziali), nonché i ruoli e le dipendenze rispettivi in materia di rischi informatici.

Occorre dunque disporre di una sorta di mappatura organizzativa come presupposto delle specifiche strategie in materia di gestione del rischio informatico e di implementazione della resilienza operativa digitale. E - tra l'altro - questa mappatura deve riguardare anche "*i patrimoni informativi e le risorse TIC su siti remoti*" (cfr. art. 8, comma 4), il che vuol dire includere nell'inventario anche le soluzioni in *cloud* (e gli accordi con i terzi fornitori).

Le entità finanziarie devono diramare istruzioni interne per cui, secondo necessità e almeno una volta all'anno, vengano riesaminate l'adeguatezza della classificazione e di altri documenti eventualmente pertinenti.

Altri documenti non strettamente tecnici o di tipo *security* riguardano i numerosi obblighi di gestione del rischio derivante da accordi contrattuali per l'utilizzo di servizi TIC conclusi con fornitori terzi di servizi TIC, obblighi graduati in base alla criticità o importanza dei rispettivi servizi, processi o funzioni

16 Si ricordi, difatti, che gli obblighi del Regolamento DORA in relazione alla sicurezza dei sistemi informatici e di rete sono relativi specificatamente alle TIC che sostengono i processi commerciali delle entità finanziarie (e non, ad esempio, alle TIC impiegate per finalità diverse, ad esempio per la gestione del personale).

17 Per «*patrimonio informativo*» si intende: "*una raccolta di informazioni, tangibili o intangibili, che è importante proteggere*" [cfr. art. 3, n. (6) del Regolamento DORA].

e in base al potenziale impatto sulla continuità e sulla disponibilità delle attività e dei servizi finanziari, a livello individuale e di gruppo.

Un primo documento in tale ambito è la cosiddetta una strategia per gestire i rischi informatici derivanti da terzi, a partire dalla necessità di evitare i cosiddetti rischi di *concentrazione*, cioè la circostanza che l'esternalizzazione per l'approvvigionamento dei servizi TIC in capo a un ristretto numero di fornitori di servizi TIC (quando non in capo ad un unico fornitore di servizi TIC) determina la dipendenza dell'entità finanziaria da quel/quei fornitore/i (cfr. art. 6, comma 9 e 28, comma 2)[18]. Dunque, nel quadro della gestione delle esigenze connesse all'approvvigionamento contrattuale dei servizi TIC a supporto dei propri processi commerciali, l'entità finanziaria deve rivedere e impostare - in base ad un approccio *risk-based* – i processi di qualifica dei fornitori come anche quelli di pianificazione delle successive stipule contrattuali per i servizi TIC forniti dai terzi. Tra l'altro, a proposito dei processi di qualifica dei fornitori impattati dagli obblighi del Regolamento DORA, vi è la prescrizione per cui prima di stipulare un accordo contrattuale per l'utilizzo di servizi TIC, le entità finanziarie devono svolgere una specifica *due diligence* sui potenziali fornitori terzi di servizi TIC onde garantirne l'idoneità lungo tutto il processo di selezione e valutazione[19]. Ecco, dunque, un ulteriore documento (*report due diligence*) che è necessario predisporre.

Si diceva più sopra del necessario approccio *risk-based* anche alla tematica contrattuale della stipula di accordi con i fornitori terzi di servizi TIC[20]. In primo luogo, le entità finanziarie devono preliminarmente identificare e documentare tutti i processi commerciali dipendenti da fornitori terzi di servizi TIC e devono identificare e le interconnessioni con detti fornitori che offrono servizi a supporto di funzioni *essenziali* o *importanti* (cfr. art. 8, comma 5 Reg. DORA).

18 Rischi di dipendenza e di concentrazione che possono dar vita anche a un vero e proprio rischio sistemico: si vedano in merito anche le considerazioni del Legislatore ai Considerando 30 e 32 del Regolamento DORA.

19 Infatti, le entità finanziarie possono stipulare accordi contrattuali soltanto con fornitori terzi di servizi TIC che soddisfano standard appropriati in materia di sicurezza delle informazioni. Laddove tali accordi contrattuali riguardino funzioni essenziali o importanti, tali standard sono quelli di qualità più aggiornati ed elevati in materia di sicurezza delle informazioni.

20 Si veda nello specifico il Capo V, Sezione I, articoli da 28 a 30 del Regolamento DORA.

vedi l'articolo online

In secondo luogo, le entità finanziarie hanno un obbligo generale di identificare e valutare in generale tutti i rischi relativi ad un accordo contrattuale con i terzi fornitori di servizi TIC, così come devono preliminarmente verificare l'esistenza di conflitti di interesse[21]. Devono poi essere oggetto di esame i rischi specifici che riguardano – tra gli altri – la valutazione se il contratto che si intende stipulare riguarda l'utilizzo di servizi TIC a supporto di una funzione *essenziale* o *importante*[22]; se la stipula del contratto soddisfa le condizioni di vigilanza; se la conclusione del contratto possa aggravare il rischio di *concentrazione* delle TIC rappresentato (1) dall'essere il fornitore terzo di servizi TIC non facilmente sostituibile o (2) dalla esistenza di molteplici accordi contrattuali relativi alla prestazione di servizi TIC a supporto di funzioni *essenziali* o *importanti* con lo stesso fornitore terzo oppure con fornitori terzi strettamente connessi.

Appare dunque logico – anche ai fini delle eventuali richieste di esibizione delle relative valutazioni svolte in merito che possono essere avanzate dalle autorità di vigilanza – che l'entità finanziaria debba redigere e conservare specifici documenti (a forma libera) contenenti l'esame, l'analisi del rischio e tutte le valutazioni sui rischi contrattuali che precedono, da allegare – insieme alla *due diligence* svolta sul fornitore – al (1) *Registro delle informazioni su tutti gli accordi contrattuali sull'utilizzo di servizi TIC forniti da fornitori terzi di servizi TIC* e – ove del caso – al (2) documento più generale recante la *strategia contrattuale* per la gestione dei rischi derivanti da terzi fornitori dei servizi TIC.

Infatti, continuando ad analizzare i documenti di natura contrattuale che l'entità finanziaria deve redigere, conservare e aggiornare, si deve fare appunto riferimento all'obbligo di detenzione di un *Registro delle informazioni su tutti gli accordi contrattuali sull'utilizzo di servizi TIC forniti da fornitori terzi di servizi TIC* che censisca a livello di entità e su base sub-consolidata e consolidata tali accordi. Struttura e contenuti di tale registro sono stati individuati dalle AEV con la proposta di *implementing technical standard* - ITS del 10 Gennaio 2024, ora all'esame della Commissione UE[23]. Tale registro deve documentare tutti gli accordi contrattuali, distinguendo quelli che si riferiscono a servizi TIC a supporto di funzioni *essenziali* o *importanti* dagli altri. Su richiesta, le entità finanziarie mettono a disposizione dell'autorità competente il registro delle informazioni completo o, a seconda della richiesta, determinate sezioni del registro insieme alle informazioni giudicate necessarie per consentire l'efficace vigilanza sull'entità finanziaria.

Altro adempimento documentale rilevante in tema di accordi contrattuali con fornitori terzi di servizi TIC riguarda le vere e proprie clausole del contratto. Non solo i contratti devono essere redatti includendo un set minimo di clausole obbligatorie[24] (cfr. art. 30, comma 2), ma nel caso di contratti aventi ad oggetto servizi TIC a supporto di funzioni *essenziali* o *importanti*, devono prevedersi sia clausole aggiuntive (cfr. art. 30, comma 3) che una disciplina stringente della risoluzione, nell'ambito delle cosiddette *strategie di uscita*. Tali strategie tengono conto dei rischi che possono emergere a livello dei fornitori terzi di servizi TIC, in particolare possibili disfunzioni dei fornitori stessi, il deterioramento della qualità dei servizi TIC forniti, una perturbazione dell'attività commerciale conseguente a una fornitura di servizi TIC inadeguata o carente, oppure gravi rischi connessi all'adeguatezza e alla continuità dell'esercizio del rispettivo servizio TIC. I piani preventivi di uscita mirano nei casi più delicati del supporto a funzioni *essenziali* o *importanti* a far sì che la risoluzione del contratto avvenga da parte della entità finanziaria senza perturbare le proprie attività commerciali, impattare sul rispetto dei requisiti normativi (a partire da quelli fissati dal Regolamento DORA) e senza pregiudicare la continuità e la qualità dei servizi forniti ai clienti.

Dal momento che i piani di uscita devono essere "*esaustivi e documentati*" (cfr. art. 28, comma 8), ecco

21 Si ricordi che in base al *principio di proporzionalità* di cui all'articolo 4 del Regolamento DORA vanno analizzati non la totalità dei contratti per qualsiasi servizio TIC stipulati con fornitori terzi – per qualsiasi finalità – dall'entità finanziaria, ma solamente i contratti con fornitori terzi di servizi TIC utilizzati a supporto dei processi e delle operazioni commerciali dell'entità finanziaria.

22 Per accordi con fornitori terzi di servizi TIC a supporto di funzioni *essenziali* o *importanti* vanno difatti inserite le clausole contrattuali aggiuntive di cui all'articolo 30, comma 3 del Regolamento DORA, redatti i piani di uscita per la risoluzione del contratto ai sensi dell'art. 28, comma 8 ed effettuate le valutazioni specifiche del rischio ai sensi dell'articolo 29. Si ricordino anche le specifiche prescrizioni di cui alla Sezione II del Capo V. articoli 31 e ss. in caso di designazione da parte delle AEV di un fornitore terzo di servizi TIC come "*critico*".

23 Cfr. il *Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554* con particolare riferimento all'Allegato III che elenca 19 tipologie di contratti per servizi TIC da registrare.Il Registro è composto da 15 distinti *templates*.

24 Le entità finanziarie e i fornitori terzi di servizi TIC possono anche avvalersi di clausole contrattuali standard per specifici servizi (es: servizi cloud) elaboratore dalla Commissione UE o da autorità pubbliche: cfr. Considerando n. 75 e articolo 30, comma 4 del Regolamento DORA.

un ulteriore adempimento documentale di cui le entità finanziarie devono tenere conto.

Infine, rientrano negli adempimenti documentali anche le varie *valutazioni del rischio* (oltre quelle contrattuali appena sopra viste) a cui sono chiamate le entità finanziarie, come ad esempio l'obbligo di svolgere un *risk assessment* e di documentare la valutazione del rischio:

1) in occasione di ogni modifica di rilievo dell'infrastruttura del sistema informatico e di rete dell'entità, dei processi o delle procedure che incidono sulle funzioni commerciali supportate dalle TIC, sui patrimoni informativi o sulle risorse TIC;

2) sui sistemi c cosiddetti *legacy*, cioè un sistema di TIC che ha raggiunto la fine del suo ciclo di vita, non si presta ad aggiornamenti o correzioni per motivi tecnologici o commerciali, o non è più supportato dal suo fornitore o da un fornitore terzo di servizi TIC, ma è ancora in uso e supporta le funzioni commerciali dell'entità finanziaria.

5. La centralità nel Regolamento DORA delle iniziative di sensibilizzazione e di formazione – ad ogni livello – in materia di rischi informatici e resilienza operativa digitale.

Si è in precedenza sottolineato come il Regolamento DORA renda centrale nel rinnovato sistema di *governance* e organizzazione delle entità finanziarie il ruolo della *sensibilizzazione* e della *formazione* in materia di rischi informatici e di resilienza operativa digitale[25]. Intanto, il Legislatore distingue le *iniziative di sensibilizzazione sulla sicurezza delle TIC* dalle *attività di formazione sulla resilienza operativa digitale* (rendendole comunque entrambe obbligatorie): le prime possono consistere in programmi, prove, verifiche a campione, test sul grado di conoscenza dei rischi informatici presso i dirigenti e il personale, nonché possono essere direttive, orientamenti, linee guida e buone prassi in materia di sicurezza delle TIC diffuse dall'entità finanziaria nella propria organizzazione al fine di promuovere "*a ciascun livello dell'azienda e per tutto il personale un forte senso di consapevolezza dei rischi informatici nonché l'impegno a osservare a tutti i livelli una rigorosa igiene informatica (cyber hygiene)*" (cfr. Considerando 45). Le attività di formazione sono invece le attività didattiche e formative vere e proprie che l'entità finanziaria deve organizzare periodicamente allo scopo di formazione e aggiornamento professionale di dirigente e personale.

È l'organismo di gestione che ha il compito di assegnare e riesaminare periodicamente le specifiche risorse finanziarie (che devono essere *adeguate*) per attuare "*i pertinenti programmi di sensibilizzazione sulla sicurezza delle TIC e le attività di formazione sulla resilienza operativa digitale, nonché le competenze in materia di TIC per tutto il personale*" [cfr. art. 5, comma 2, lettera (g) del Regolamento DORA].

L'individuazione e l'allocazione di risorse finanziarie adeguate è propedeutica all'attuazione dell'obbligo di elaborare sia (1) programmi di sensibilizzazione sulla sicurezza delle TIC che (2) attività di formazione sulla resilienza operativa digitale. Tali programmi e attività rappresentano moduli obbligatori nei programmi di formazione del personale, riguardano tutti i dipendenti e gli alti dirigenti, e devono essere articolati in modo tale da presentare un livello di complessità commisurato all'ambito delle loro funzioni. Dunque, occorre pianificare con attenzione le iniziative di sensibilizzazione e formazione, i cui contenuti dovranno essere diversificati a seconda dei destinatari.

Nuova è anche l'opzione ("*se del caso*", cfr. art. 13, comma 6. Regolamento DORA) per le entità finanziarie di far partecipare anche i propri fornitori terzi di servizi TIC contrattualizzati alle iniziative di sensibilizzazione e alle attività di formazione di dirigenti e personale (con l'ovvio valore aggiunto rappresentato dall'apporto esperienziale e tecnico dei fornitori), tanto che gli accordi contrattuali per l'utilizzo di servizi TIC tra entità finanziarie e fornitori terzi di servizi TIC possono includere *ab origine* specifiche clausole che stabiliscono le condizioni riguardanti la partecipazione dei fornitori terzi di servizi TIC ai programmi di sensibilizzazione sulla sicurezza delle TIC e alle attività di formazione sulla resilienza operativa digitale delle entità finanziarie [cfr. art. 30, comma 2, lettera (i) del Regolamento DORA].

La formazione in materia di rischi informatici e di resilienza operative digitale è allora un rilevante tema non solo *organizzativo*, ma anche *contrattuale* per le entità finanziarie, sia per i peculiari obblighi in materia di programmazione, articolazione e contenuti (vedi *supra*) da tenere presenti negli accordi con gli organizzatori ed erogatori delle iniziative di formazione, sia perché – come appena visto – l'articolo 30 del Regolamento DORA include la partecipazione dei fornitori terzi di servizi TIC alle attività di sensibi-

25 Tanto che gli obblighi di sensibilizzazione e formazione in materia di rischi informatici e sicurezza delle TIC sono applicabili anche a dirigenti e personale di entità non soggette alla gran parte degli obblighi DORA, come ad esempio istituti di pagamento esenti, piccole imprese di investimento non interconnesse, piccoli enti pensionistici, etc.

lizzazione e formazione nel contenuto minimo delle clausole che disciplinano i loro rapporti di fornitura con le entità finanziarie.

Ancora, possiamo logicamente includere nel tema della formazione e del continuo aggiornamento (che nel settore delle TIC deve essere se non quotidiano, quasi) tre peculiari adempimenti previsti dal Regolamento DORA.

Il primo (cfr. art. 13, comma 7) è rappresentato dall'obbligo per le entità finanziarie: (1) di monitorare costantemente i pertinenti sviluppi tecnologici, anche al fine di comprendere i possibili effetti dell'impiego di tali nuove tecnologie sui requisiti in materia di sicurezza delle TIC e sulla resilienza operativa digitale (2) di tenersi aggiornate sui più recenti processi di gestione dei rischi informatici, in modo da contrastare efficacemente le forme nuove o già esistenti di attacchi informatici. Dunque, vi è un obbligo di monitorare i mercati, le uscite di nuove soluzioni tecnologiche di *security*, così come vi è l'obbligo di seguire il progresso e le evoluzioni della tecnologia (es: monitorando le grandi fiere internazionali dell'ICT o seguendo le presentazioni periodiche delle Big Tech, etc). Dovrebbero essere gli stessi membri dell'organo di gestione (o un responsabile ICT – come il CTO o il CISO - che ad essi relazioni) a provvedere.

Il secondo adempimento (cfr. art. 13, comma 3) riguarda l'integrazione costante nel processo di valutazione dei rischi informatici degli insegnamenti che l'entità finanziaria ha tratto dai test sulla resilienza operativa digitale effettuati in conformità degli articoli 26 e 27 del Regolamento DORA, dagli incidenti connessi alle TIC realmente avvenuti (es: attacchi informatici), dall'esperienza in generale maturata in sede di attivazione dei piani di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC.

Il terzo profilo riguarda la (in)formazione che – di fatto – deriva dallo scambio di informazioni e di analisi che è facoltà delle entità finanziarie condividere tra di loro (cfr. art. 45 sui meccanismi di condivisione delle informazioni e delle analisi delle minacce informatiche tra le entità finanziarie). Il Regolamento DORA incoraggia difatti le entità finanziarie a scambiarsi reciprocamente informazioni e analisi delle minacce informatiche (es: indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cybersicurezza e strumenti di configurazione, etc) e a sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le proprie capacità di individuare, valutare e monitorare adeguatamente le minacce informatiche e di difendersi dai loro effetti e rispondervi.

Infine, appare opportuno in tale sede esaminare il ruolo dei revisori alla luce del Regolamento DORA, in quanto argomento comunque connesso alla necessaria competenza, formazione e capacità generale che tale normativa richiede. In particolare, è fissato un principio fondamentale per cui l'entità finanziaria deve verificare 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 richieste (ad esempio, l'articolo 28 prevede che laddove gli accordi contrattuali conclusi dall'entità finanziaria con fornitori terzi di servizi TIC per l'utilizzo di servizi TIC comportino un'elevata complessità tecnica, entrano in campo i revisori che devono possedere le dovute competenze per esaminarli e valutarli)[26].

6. Conclusioni: il quadro normativo complessivo tra Regolamento DORA, Implementing e Regulatory Technical Standard e atti delegati della Commissione UE.

In apertura del presente contributo si è definita come particolarmente complessa la normativa in materia di resilienza operativa digitale. Ed in effetti, i piani di *compliance* in corso da parte delle entità finanziarie devono attuarsi alla luce di un quadro regolatorio che è ben più ampio del Regolamento DORA, il quale rinvia in molti casi ad una serie di standard tecnici di implementazione o di regolamentazione (ciascuno un *implementing technical standard* o ITS o *regulatory technical standard* o RTS) che devono adottati dalle autorità di vigilanza europee - AEV[27] con lo scopo di definire in modo più dettagliato e/o

26 De *iure condendo*, l'articolo 58, comma 3 del Regolamento DORA prevede che entro il 17 gennaio 2026, la Commissione, dopo aver consultato le AEV e il comitato degli organismi europei di controllo delle attività di revisione contabile, effettua un riesame e presenta al Parlamento europeo e al Consiglio una relazione accompagnata, se del caso, da una proposta legislativa sull'opportunità di rafforzare i requisiti per i revisori legali e le imprese di revisione contabile per quanto riguarda la resilienza operativa digitale, mediante l'inclusione dei revisori legali e delle imprese di revisione contabile nell'ambito di applicazione del Regolamento DORA

27 Ai sensi del Regolamento DORA sono denominate collettivamente «autorità europee di vigilanza» o «AEV»: l'Autorità bancaria europea — ABE, istituita dal regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio; l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali — EIOPA, istituita dal rego-

ampliare alcuni dei requisiti e degli adempimenti introdotti dal Regolamento DORA.

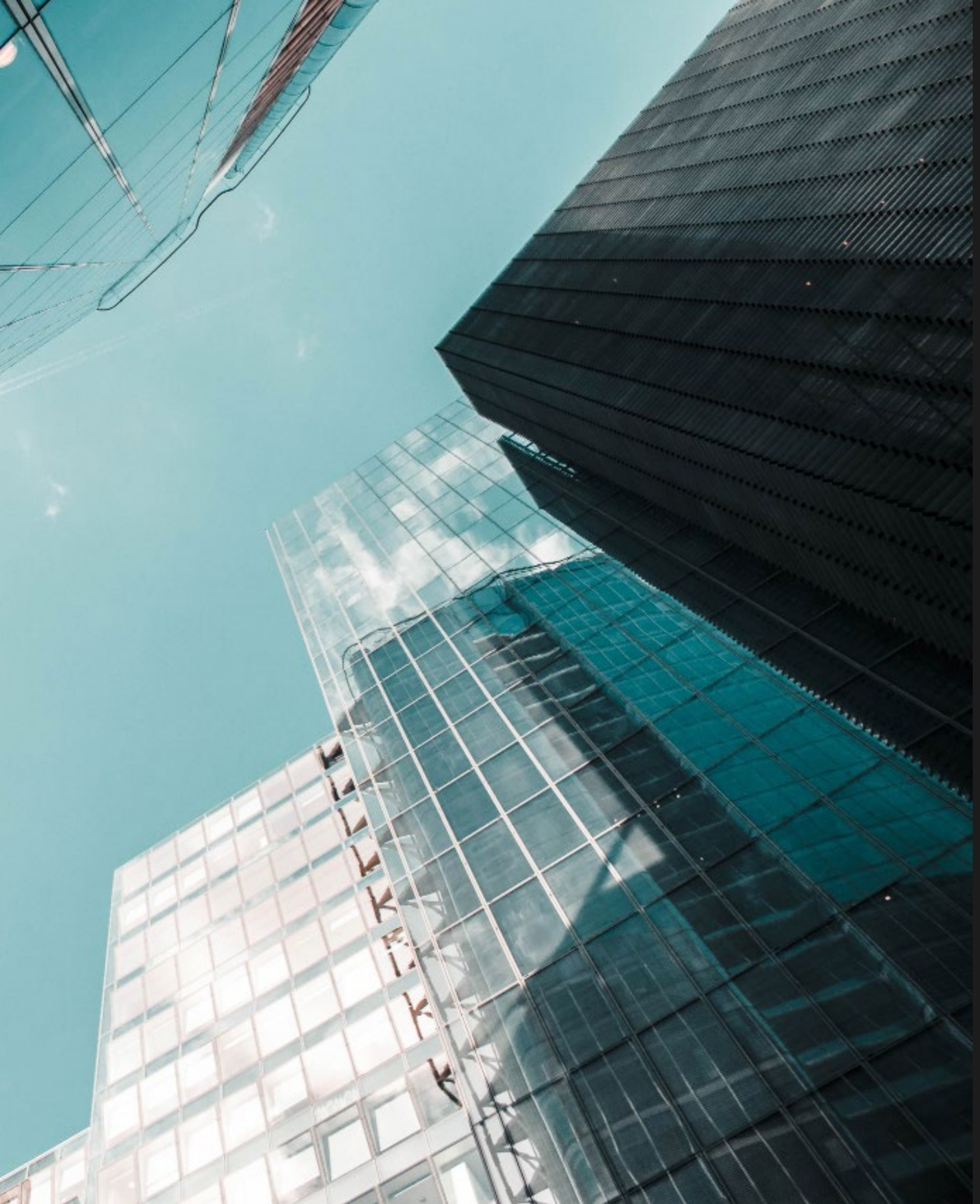
Le AEV presentano le pertinenti norme tecniche di implementazione o regolamentazione alla Commissione europea – ciò che è avvenuto secondo le scadenze previste del 17 Gennaio e del 17 Luglio 2024 - che ha quindi il potere di integrare il Regolamento DORA adottando le norme tecniche sotto forma di regolamento delegato.

Ad oggi, a fronte di numerosi progetti di norme tecniche di implementazione e regolamentazione adottati dalle AEV, di seguito le proposte delle AEV formalmente confluite in atti delegati adottati dalla Commissione UE (pubblicati nella Gazzetta Ufficiale della UE del 30 Maggio 2024 e del 25 Giugno 2024):

- il Regolamento delegato (UE) 2024/1502 della Commissione del 22 febbraio 2024 che integra il Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio specificando i criteri per la designazione dei fornitori terzi di servizi TIC come critici per le entità finanziarie;
- il Regolamento delegato (UE) 2024/1502 della Commissione del 22 febbraio 2024 che integra il Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio determinando l'importo delle commissioni per le attività di sorveglianza che l'autorità di sorveglianza capofila addebita ai fornitori terzi critici di servizi TIC e le relative modalità di pagamento;
- il Regolamento delegato (UE) 2024/1772 della Commissione del 13 marzo 2024 che integra il Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri per la classificazione degli incidenti connessi alle TIC e delle minacce informatiche, stabiliscono le soglie di rilevanza e specificano i dettagli delle segnalazioni di gravi incidenti;
- il Regolamento delegato (UE) 2024/1773 della Commissione del 13 marzo 2024 che integra il Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che precisano il contenuto dettagliato della politica relativa agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC;
- il Regolamento delegato (UE) 2024/1774 della Commissione del 13 marzo 2024 che integra il Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano gli strumenti, i metodi, i processi e le politiche per la gestione dei rischi informatici e il quadro semplificato per la gestione dei rischi informatici.

Dunque, un quadro di regole vincolanti per le entità finanziarie, in costante divenire, e che rende continua l'esigenza di monitorare e adeguare i processi interni e la *governance* generale in materia di sicurezza, rischi informatici e resilienza operativa digitale.

lamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio e l'Autorità europea degli strumenti finanziari e dei mercati — ESMA, istituita dal regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio.



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it