Evoluzione per la **Data Governance**: dal **GDPR** al **DORA**

Le istituzioni finanziarie devono implementare misure di sicurezza conformi alle normative GDPR e DORA per evitare conseguenze legali e reputazionali, oltre all'applicazione di sanzioni diverse tra loro

Crediti immagine: tete_escape/shutterstock

Il Digital Operational Resilience Act (DORA) è strettamente legato alla gestione dei dati e alla sicurezza del mondo finanziario. In un contesto dove cyber security e data protection sono sempre più interdipendenti e il GDPR costituisce la cornice di riferimento in materia di tutela dei dati personali, la risposta non può che essere nell'integrazione del DORA con il quadro normativo europeo in materia di privacy.

Occorre quindi coniugare resilienza operativa e protezione dei dati personali, adottando governance aziendali che, in un ecosistema sempre più data-driven, muovano le premesse da un'attenta analisi dei punti di contatto esistenti.

Da qui l'inserimento di misure di sicurezza relative ai rischi ICT (Information and Communication Technologies) progettate per rispondere a entrambe le esigenze: resilienza operativa e protezione dei dati.

Inoltre, sarà necessaria una cultura aziendale che promuova la consapevolezza e la formazione continua, con sguardo rivolto all'adeguamento tecnologico, ai processi interni e ai protocolli di comunicazione in caso di incidenti.

Il rischio di duplicazione degli obblighi

Questo, tuttavia, non esclude il pericolo di duplicazione degli obblighi (ad esempio, notifiche multiple per lo stesso incidente), ma Commissione Europea e autorità di vigilanza (ESMA, EBA, EIOPA) sono già al lavoro per fornire linee guida coordinate in grado di garantire che i requisiti del DORA si integrino con quelli del GDPR.

In attesa, pertanto, che il quadro regolamentare si completi di alcune disposizioni che rendano la governance sui rischi ICT e privacy più organica, il consiglio è quello di adottare un approccio aziendale integrato.

Quantomeno con riferimento ai seguenti punti:

(i) valutazione congiunta dei rischi ICT e del rischio di violazione dei dati, da declinare in un esercizio di previsione degli scenari aziendali in cui potrebbero verificarsi delle violazioni dei dati e dei sistemi informatici. In questa direzione, è inevitabile muovere le premesse dall'analisi del DIPA (Data Protection Impact Assessment) in modo che il pro-

cesso di raccolta delle informazioni consenta di definire in maniera più efficace le misure tecniche e organizzative necessarie;

(ii) adozione di processi aziendali che consentano di minimizzare i rischi di data breach nell'impiego dei sistemi ICT o che prevedano di gestire sia i rischi ICT che quelli per la privacy attraverso l'impiego di una policy unica.

(iii) formazione di dipendenti e collaboratori in materia di rischi ICT e di obblighi derivanti dalla normativa privacy. In ordine a questo aspetto vi è però da precisare che, se per il GDPR la formazione è obbligatoria, per il DORA invece no. È pur vero, tuttavia, che per quanto il DORA non parli di una formazione specifica obbligatoria in tema di cyber security, questa costituisce comunque un elemento imprescindibile per dimostrare la conformità dei processi aziendali alla normativa di riferimento.

Delineato in questi termini il contesto, è chiaro dunque che resilienza informatica e protezione dei dati rappresentano oggi due facce della stessa medaglia.

Le differenze sanzionatorie

Come visto, l'intreccio tra DORA e GDPR trova il suo snodo principale nel completamento reciproco, poiché entrambi gli interventi normativi sono orientati a garantire sicurezza, integrità e riservatezza dei dati.

@ Margherita Domenegotti, Partner di La Scala Società tra Avvocati

Questo, però, non vale per le sanzioni. DORA e GDPR presentano, infatti, due reticolati sanzionatori diversi.

Il primo, in particolare, distingue tra sanzioni amministrative pecuniarie nei confronti delle persone giuridiche e sanzioni amministrative pecuniarie nei confronti di «soggetti apicali», ossia le persone fisiche. Parliamo di sanzioni importanti, che nei confronti delle persone giuridiche possono raggiungere, in alcuni casi, addirittura il 10% del fatturato globale.

Il tutto, salvo che il fatto "costituisca reato..." e con la possibilità, in ogni caso, di applicare misure accessorie interdittive.

Per quanto riguarda, invece, la protezione dei dati personali, l'art. 83 del GDPR stabilisce due livelli di sanzioni, a seconda della gravità della violazione.

In particolare: (i) per le violazioni meno gravi è prevista una multa fino a 10 milioni di euro, oppure fino al 2% del fatturato annuo; (ii) per violazioni più gravi è prevista una multa fino a 20 milioni di euro, oppure fino al 4% del fatturato annuo.

Infine, a queste si aggiungono le misure penali e i rimedi di tutela risarcitoria.

E ciò in un contesto in cui, se la violazione dei dati personali è avvenuta a causa della mancanza di conformità al modello DORA, la circostanza potrebbe addirittura innescare due regimi sanzionatori paralleli.

Per rendere più concreta la prospettiva, è utile fare un esempio:

- un ente finanziario (immaginiamo una banca), che è anche titolare del trattamento ai sensi del GDPR, subisce un attacco informatico che causa una compromissione di dati personali dei propri clienti;
- a quel punto, la banca ha l'obbligo di notificare la circostanza di intervenuta violazione (data breach) al Garante e, parallelamente, segnalare l'incidente informatico agli organismi di vigilanza competenti in ambito DORA;
- conseguentemente, Garante della privacy e Autorità di Vigilanza avviano un procedimento nei confronti della banca e rilevano la mancanza di sistemi di sicurezza adeguati a evitare i rischi ICT e la violazione dei dati personali.

@ Francesco Concio, Partner di La Scala Società tra Avvocati

Da qui il dilemma. In alcuni casi, come quello appena descritto, il regime sanzionatorio del GDPR e quello previsto dal DORA possono infatti sovrapporsi e coesistere.

E allora quid iuris?

Nel quadro appena descritto, purtroppo, non possiamo escludere l'applicazione di sanzioni diverse tra loro, ossia quelle previste dal DORA e dal GDPR.

È quindi fondamentale che tutte le entità finanziarie implementino misure di sicurezza conformi a entrambe le normative per evitare conseguenze legali e reputazionali.

Il tutto, in ogni caso, senza trascurare che le autorità competenti saranno comunque tenute a coordinarsi per evitare ingiuste duplicazioni e garantire che le sanzioni siano proporzionate, efficaci e dissuasive.

Avv. Margherita Domenegotti
Avv. Francesco Concio
Partner di La Scala Società tra Avvocati