GattiPavesiBianchiLudovici

TMT, PROPRIETÀ INTELLETTUALE E DATA PROTECTION

Secondo round di standard e linee guida per l'implementazione DORA

Il Regolamento UE 2022/2554, (cd. "DORA" Digital Operational Resilience Act), entrerà in vigore a gennaio 2025 e mira a creare un settore finanziario europeo più sicuro, armonizzando e migliorando il modo in cui le entità finanziarie europee gestiscono la propria resilienza digitale operativa.
Il 17 luglio 2024, EBA, EIOPA e ESMA, le tre Autorità di vigilanza europee ("ESA"), hanno rilasciato il secondo round di *final report* relativi all'implementazione del DORA.

I documenti pubblicati il 17 luglio

In particolare, i documenti pubblicati forniscono più dettagli sui test di penetrazione per le minacce, sul framework di supervisione, sui gruppi comuni di esperti che svolgeranno i compiti di vigilanza, sulle modalità per la stima di costi e le perdite relativi agli incidenti, nonché gli standard tecnici normativi per formato, contenuto e scadenze della notifica di incidenti gravi.
Gli standard tecnici sono stati inviati alla Commissione Europea e saranno finalizzati nei prossimi mesi.
La seconda serie di prodotti normativi non contiene, come sperato, le linee guida sull'affidamento a terzi, lasciando ancora incertezza su un elemento fondamentale per l'adeguamento.

Gli standard per la notifica degli incidenti

Di particolare importanza per gli operatori è il documento "JC 2024 33", è che delinea gli standard tecnici normativi (RTS) per **il contenuto, il formato, le scadenze e le procedure per la segnalazione degli incidenti, con particolare attenzione alla necessità di proporzionalità e all'allineamento con altre normative come la direttiva NIS2.**

La chiarezza sul template e sulle modalità di segnalazione, infatti, consentirà agli operatori di strutturare in modo più efficienti le procedure interne di segnalazione, creando approcci scalabili idonei a concentrare gli sforzi di compliance rispetto a diverse normative (ad esempio, il GDPR).

Di seguito, alcuni degli elementi più importanti che emergono dagli standard tecnici normativi.

Template Unico: Ai sensi del Regolamento DORA le informazioni sugli incidenti informatici significativi andranno forniti in tre fasi (**Notifica iniziale**, **Relazione intermedia** e **Relazione finale**) Per semplificare questo processo e garantire la qualità dei dati raccolti, è stato redatto un template unico per la segnalazione di questi incidenti. Il template è strutturato in modo da raccogliere tutte le informazioni necessarie alle autorità competenti per valutare l'incidente in modo esaustivo. Le entità finanziarie sono tenute a compilare solo i campi pertinenti alla specifica fase di segnalazione in corso (iniziale, intermedia, finale). Pur essendo suddiviso in sezioni specifiche per ciascuna fase, il template offre un certo grado di flessibilità. Se un'entità finanziaria dispone già di informazioni richieste in una fase successiva, può anticiparle e compilarle nel template, semplificando così il processo di segnalazione.

Incidenti Ricorrenti Il template è progettato per gestire anche segnalazioni di incidenti multipli o ricorrenti che, se presi singolarmente, non soddisferebbero i criteri per essere classificati come "incidenti gravi", ma che, considerati cumulativamente, raggiungono la soglia di gravità. In particolare, si tratta di incidenti non gravi verificatisi almeno due volte nell'arco di sei mesi, che condividono la stessa causa apparente e, collettivamente, si qualificano come un incidente grave. Gli standard prevedono uno spostamento delle informazioni sugli incidenti ricorrenti nella relazione finale, per rispondere alle preoccupazioni sollevate dalle entità finanziarie durante la consultazione pubblica, relative alla difficoltà di fornire un'analisi completa della causa principale in una fase così iniziale del processo di segnalazione e all'eccessivo onere di dover classificare e compilare tutti gli incidenti minori per determinare il raggiungimento delle soglie di segnalazione.

Notifiche aggregate: Le informazioni aggregate sono previste nei casi in cui più entità finanziarie subiscono un incidente informatico importante a causa di un fornitore terzo di servizi ICT. La specifica sugli incidenti aggregati completa la disciplina relativa all'affidamento a terzi delle attività connesse alla notifica degli incidenti. In questi casi, il fornitore terzo può presentare una singola relazione aggregata per tutte le entità finanziarie interessate, a condizione che siano soddisfatte specifiche condizioni.

Contenuti del modello di segnalazione: Il modello di segnalazione è stato semplificato riducendo significativamente il numero di campi obbligatori, passando da 84 a 59, in particolare riducendo il template di notifica iniziale a 7 campi obbligatori. Questa modifica risponde alle preoccupazioni espresse durante la consultazione pubblica riguardo all'onere della segnalazione, soprattutto nelle prime fasi della gestione di un incidente.

Tempistiche di segnalazione: Molti partecipanti alla consultazione hanno ritenuto le tempistiche inizialmente proposte troppo brevi, in particolare per quanto riguarda la relazione intermedia. Di conseguenza, le ESA hanno deciso di estendere i termini per la presentazione della relazione intermedia a 72 ore dalla presentazione della notifica iniziale, anziché dal momento della classificazione dell'incidente. Inoltre, è stata chiarita la possibilità di presentare la relazione intermedia senza indebito ritardo una volta ripristinate le attività ordinarie. Per quanto riguarda la relazione finale, la scadenza sarà a un mese dalla presentazione dell'ultima relazione intermedia, eliminando il riferimento alla risoluzione "permanente" dell'incidente.

Segnalazioni nel fine settimana: Per garantire un approccio più proporzionato, le ESA hanno esentato le entità finanziarie più piccole dall'obbligo di presentare relazioni nel fine settimana, a meno che l'incidente non abbia un impatto sistemico o transfrontaliero. eliminando la necessità per tutte le entità finanziarie di disporre di una funzione di supporto alla segnalazione degli incidenti attiva 24 ore su 24, 7 giorni su 7.

***

Lo Studio resta a disposizione per qualsivoglia ulteriore informazione e per fornire tutto il supporto necessario al fine di adeguarsi, nei termini, alla normativa in materia.

GATTI PAVESI BIANCHI LUDOVICI

TMT, Proprietà intellettuale e Data Protection

Gilberto Nava gilberto.nava@gpblex.it

Elisabetta Nunziante elisabetta.nunziante@gpblex.it