Punti chiave del Decreto Legislativo 138/2024 di recepimento della Direttiva NIS 2

La Direttiva EU 2022/2555 (nota anche come "**NIS 2**") è stata recepita nella normativa nazionale con il Decreto Legislativo del 4 settembre 2024, n°138, pubblicato in Gazzetta Ufficiale il 1° ottobre 2024.

Le disposizioni del nuovo Decreto Attuativo NIS 2 si applicheranno a decorre dal **18 ottobre 2024**. Alla stessa data è prevista l'abrogazione del Decreto Legislativo 65/2018 (con l'eccezione di alcuni articoli), che aveva recepito la **Direttiva NIS (UE) 2016/1148**, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

1. ***Qual è l'obiettivo?***

La nuova versione della Direttiva mira a garantire un livello elevato di sicurezza informatica in ambito nazionale proteggendo le reti e i sistemi informativi utilizzati per fornire servizi essenziali in settori chiave.

L'obiettivo principale è quello di vincolare i soggetti pubblici e privati che operano i determinati settori considerati critici per il funzionamento del sistema economico e sociale all'adozione di determinate misure volte **a prevenire, resistere a rimediare agli incidenti informatici**.

In questo contesto, uno dei punti principali della nuova normativa è l'estensione del suo campo di applicazione, rispetto alla precedente normativa NIS1 facente capo Direttiva NIS (UE) 2016/1148, a nuove entità e a nuovi settori di attività.

2. ***Chi è l'Autorità competente?***

- **L'Agenzia per la cybersicurezza nazionale** è l'Autorità nazionale competente NIS. Quest'Autorità è il **punto di contatto unico** e dovrà, tra l'altro, individuare i soggetti essenziali e i soggetti importanti.

- **CSIRT Italia** è il Gruppo nazionale di risposta agli incidenti di sicurezza informatica, operante all'interno dell'Agenzia per la cybersicurezza nazionale.

Al sensi dell'articolo 15, comma 3, del Dlgs il **CSIRT Italia**, *tra l'altro*:

- **monitora e analizza le minacce informatiche**, le vulnerabilità e gli incidenti a livello nazionale;

- su richiesta, fornisce assistenza ai soggetti essenziali e ai soggetti importanti interessati **per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informativi e di rete**;
- **emette preallarmi, allerte e bollettini** e divulga informazioni ai soggetti essenziali e ai soggetti importanti interessati;
- **fornisce una risposta agli incidenti** e assistenza ai soggetti essenziali e ai soggetti importanti interessati

3. *A chi si applica?*

Ai **soggetti pubblici e privati** che operano nei settori chiave elencati negli allegati I, II, III, e IV al decreto.

Gli allegati I e II riportano **i settori ad alta criticità** (energia; trasporti; settore bancario; infrastrutture dei mercati finanziari; settore sanitario; acqua potabile; acque reflue; infrastrutture digitali; gestione dei servizi TIC; spazio) **e gli altri settori critici** (servizi postali e di corriere; gestione dei rifiuti; fabbricazione, produzione e distribuzione di sostanze chimiche; produzione, trasformazione e distribuzione di alimenti; fabbricazione; fornitori di servizi digitali; ricerca).
Gli allegati III e IV indicano le amministrazioni pubbliche soggette alla normativa.

Il Dlgs si applica altresì, indipendentemente dalle loro dimensioni, *ad esempio* ai prestatori di servizi fiduciari; ai gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio.

In parallelo, assume importanza fondamentale la distinzione tra **soggetti essenziali** e **soggetti importanti** sulla base del settore in cui operano e di criteri dimensionali.

Per quanto riguarda i soggetti privati, l'articolo 6 del Dlgs stabilisce che **sono considerati soggetti essenziali**:

- I soggetti che operano nei settori ad alta criticità che *superano i massimali per le medie imprese* (ossia imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR.);

- I fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese.

Poi indipendentemente dalle loro dimensioni:

- i soggetti identificati critici dal Decreto Legislativo 134/2024 di recepimento della Direttiva CER;
- i prestatori di servizi fiduciari qualificati;
- i gestori di registri dei nomi di dominio di primo livello;
- i prestatori di servizi di sistema dei nomi di dominio;
- i soggetti individuati critici da parte dell'Autorità nazionale competente NIS.

Per quanto riguarda **i soggetti importanti**, sono tutti quelli coperti dal Dlgs che non vengono considerati essenziali.

Sarà competenza dell'Agenzia per la cybersicurezza nazionale preparare l'elenco dei soggetti essenziali e importanti, dopo la loro auto registrazione su una piattaforma dedicata.

4. ***Quali sono gli obblighi?***

Esistono degli obblighi per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei servizi.

- **Auto registrazione:** è prevista la registrazione sulla piattaforma digitale fornita dall'Autorità nazionale competente NIS da parte dei soggetti che rientrano nel campo di applicazione della normativa.

- **Adottare delle misure tecniche, operative e organizzative.**

  Le misure comprendono:

- delle politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
- una procedura di gestione degli incidenti (anche per eseguire le notifiche di incidente o di informazioni pertinenti);
- assicurare la continuità operativa (organizzare la gestione del backup, il ripristino in caso di disastro, procedure di gestione delle crisi);
- assicurare la sicurezza della catena di approvvigionamento (sicurezza dei rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi);
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete (gestione e divulgazione della vulnerabilità);
- politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;
- pratiche di igiene di base e di formazione in materia di sicurezza informatica;
- politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;

- sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;
- uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

- **Notifica degli incidenti:**

Cos'è un incidente?

È definito come un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi.

Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

- La notifica obbligatoria

I soggetti essenziali e i soggetti importanti devono notificare al CSIRT Italia ogni incidente che ha un impatto significativo sulla fornitura dei servizi.

a) Senza ritardo o **entro 24 ore** dalla conoscenza dell'incidente significativo, una pre-notifica deve essere trasmessa al CSIRT Italia (ove possibile, indicando se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero);
b) Senza ritardo o **entro 72 ore** dalla conoscenza dell'incidente significativo, una notifica dell'incidente deve essere trasmessa al CSIRT Italia (ove possibile, con aggiornamento delle informazioni e una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione);
c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;
d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente, che comprenda una descrizione dettagliata dell'incidente; il tipo di minaccia o la causa originale; le misure di attenuazione adottate e in corso; ove noto l'impatto transfrontaliero dell'incidente.

- La notifica volontaria

I soggetti possono, su base volontaria, notificare al CSIRT Italia incidenti diversi da quelli con un impatto significativo, quali in particolare **le minacce informatiche** (i.e. qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone) e **i quasi-incidenti** (i.e. un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato).

- **Proporzionalità**

Gli obblighi si applicano secondo un criterio di proporzionalità. In tal senso, l'articolo 31, comma 1, del Dlgs prevede che "*l'Autorità nazionale competente NIS stabilisce* ***obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico***".

5. *Prossimi passi*

- **Auto registrazione**

Dal 1° gennaio al 28 febbraio di ogni anno, i soggetti pubblici e privati devono registrarsi sulla piattaforma resa disponibile dall'Autorità nazionale competente NIS.

Entro il 17 gennaio 2025, i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network che rientrano nell'ambito di applicazione del decreto, **si devono registrare sulla piattaforma digitale**.

- **Designazione dei soggetti**

Entro il 31 marzo 2025, l'agenzia per la cybersicurezza nazionale preparerà l'elenco dei soggetti essenziali e dei soggetti importanti**.** La decisione sarà presa sulla base della registrazione effettuata sulla piattaforma e dei criteri indicati nella stessa.

6. ***Le sanzioni***

La mancata osservanza degli obblighi previsti dal Decreto Attuativo NIS 2 può comportare gravi sanzioni:

- fino ad un massimo di euro 10.000.000 o del 2% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, per i soggetti essenziali (escluse le pubbliche amministrazioni).
- fino ad un massimo di euro 7.000.000 o dell'1,4% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto per i soggetti importanti (escluse le pubbliche amministrazioni).

Le sanzioni sono severe proprio perché queste misure sono volte a proteggere i servizi essenziali forniti in Italia. In ogni caso, devono sempre essere proporzionate alla gravità dell'incidente.