2 ottobre 2024

lawalert *le ultime novità in tema di normative e giurisprudenza*

CYBER NEWS: pubblicato il Decreto Legislativo 4 settembre 2024, n. 138 che recepisce la direttiva NIS II.

In data 1 ottobre 2024 è stato pubblicato in Gazzetta Ufficiale il Decreto Legislativo 4 settembre 2024, n. 138 (di seguito «Decreto NIS II»), che entrerà in vigore in data 18 ottobre 2024 e stabilisce:

- La **Strategia nazionale di cybersicurezza** per garantire un livello elevato di protezione dei sistemi informatici;
- L'integrazione del **quadro di gestione delle crisi informatiche**;
- La **conferma dell'Agenzia per la Cybersicurezza Nazionale** (o «ACN») come i) autorità nazionale competente NIS; ii) punto di contatto unico NIS; e iii) gruppo di intervento nazionale per la sicurezza informatica in caso di incidente nazionale (o «CSIRT»).
- La **designazione dell'ACN e del Ministero della difesa** – ciascuno per i propri ambiti di competenza – quali autorità competenti a gestire le crisi informatiche su larga scala;
- L'**individuazione di autorità di settore** (con riferimento ai settori inclusi nell'ambito applicativo del Decreto NIS II) competenti che collaborano con l'ACN;
- L'indicazione dei **criteri per individuare i soggetti** a cui si applica la nuova norma, nonché i relativi **obblighi di gestione e notifica**;
- L'adozione di **misure in materia di cooperazione e condivisione delle informazioni** a livello di Unione Europea.

AMBITO DI APPLICAZIONE

Il Decreto NIS II si applica ai soggetti che operano nei settori indicati nei suoi quattro allegati, prevedendo quindi due allegati aggiuntivi rispetto a quelli già allegati alla Direttiva NIS II, e ad altri soggetti elencati nel corpo del decreto stesso.

In particolare, il Decreto NIS II si applica:

1. ai settori ad **alta criticità**: energia; trasporti; settore bancario; infrastrutture dei mercati finanziari; settore sanitario; acqua potabile; acque reflue; infrastrutture digitali; gestione dei servizi TIC B2B; e spazio;
2. ai **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 e ricerca;

Per essere inclusi i soggetti appena menzionati devono anche essere considerati **almeno medie imprese** alla luce della Raccomandazione 2003/361/CE, salvo qualora i) rientrino nelle eccezioni previste dal Decreto NIS II (come ad esempio soggetti che rappresentano elementi sistemici delle catene di approvigionamento di soggetti essenziali o importanti), o ii) si applichi la cd. «**clausola di salvaguardia**», ossia l'inclusione possa essere ritenuta sproporzionata tenuto conto dell'indipendenza informatica e di rete che sussiste tra imprese collegate (in questo caso i soggetti vengono esclusi dall'ambito applicativo della nuova normativa).

3. indipendentemente dalle dimensioni, alle **Pubbliche Amministrazioni** (centrali, regionali, locali e di altro tipo) indicate all'allegato III; ed
4. indipendentemente dalle dimensioni, alle **ulteriori tipologie di soggetti** indicate all'allegato IV (ossia soggetti che operano nei settori del trasporto pubblico locale, delle attività di ricerca, delle attività di interesse culturale ed alle società in house, partecipate e a controllo pubblico ai sensi del D.Lgs. 175/2016).

5. **ai soggetti identificati come critici ai sensi della Direttiva CER** -> rimandiamo al nostro **alert** per un approfondimento su questo tema;
6. alle seguenti **ulteriori tipologie di soggetti**: prestatori di servizi fiduciari; gestori di registri di nomi a dominio;
7. Alle **imprese collegate ad un soggetto essenziale od importante per la sicurezza cyber**, ossia che: i) adotta decisioni o esercita un'influenza dominante in relazione alle misure di gestione del rischio per la sicurezza informatica del soggetto essenziale o importante; ii) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura del servizio essenziale o importante; iii) Effettua operazioni di sicurezza informatica; iv) Fornisce allo stesso servizi TIC o di sicurezza.

I soggetti previsti ai precedenti punti sono tenuti ad autoidentificarsi iscrivendosi presso la piattaforma ACN secondo le tempistiche indicate nella timeline più sotto.

Per quanto riguarda invece i soggetti rientranti nei punti da **1**. a **4**. che non rientrerebbero nell'ambito applicativo della normativa ma che l'ACN decida di includere in base a criteri aggiuntivi di valutazione (previsti dall'articolo 3 del Decreto NIS II), questi sono individuati specificamente dall'ACN su proposta delle singole autorità di settore previste dalla nuova normativa. L'ACN comunica a tali soggetti l'inclusione nell'apposito elenco tenuto a livello nazionale.

I soggetti inclusi nell'ambito applicativo del Decreto NIS II vengono differenziati in essenziali ed importanti secondo quanto stabilito nell'articolo 6 del decreto stesso, e ad essi si applicheranno obblighi e sanzioni differenti (sono previste sanzioni di importo più elevato per i soggetti essenziali e più contenute per i soggetti importanti).

TIMELINE

Successivamente alla pubblicazione del Decreto NIS II:

- Entro il **31 dicembre 2024** i soggetti previsti ai punti precedenti dovranno effettuare un'autovalutazione per verificare se siano ricomprese nell'ambito di applicazione del Decreto NIS II;
- Dal **1 gennaio** al **28 febbraio** di ogni anno i soggetti che all'esito della valutazione di cui sopra ritengano di rientrare nell'ambito applicativo della nuova normativa devono registrarsi (o aggiornare la propria registrazione per gli anni successivi al primo) sulla piattaforma digitale dell'ACN. I soggetti essenziali ed importanti possono iniziare a registrarsi a partire dalla data di pubblicazione del portale ACN (non ancora raggiungibile);
- Entro il **31 marzo** di ogni anno l'ACN redige l'elenco dei soggetti **essenziali** o **importanti**;
- Tra il **1 aprile** ed il **15 aprile 2025** l'ACN comunicherà ai soggetti registrati l'inserimento o meno nell'elenco dei soggetti a cui si applica la normativa;
- Dal **15 aprile** al **31 maggio** di ogni anno tramite la piattaforma dell'ACN i soggetti che hanno ricevuto la comunicazione forniscono o aggiornano le seguenti informazioni: i) lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso o nella disponibilità del soggetto; i responsabili individuati per i soggetti extra-UE che forniscono i propri servizi nel territorio europeo; iii) un eventuale sostituto del punto di contatto indicato dal soggetto in fase di registrazione.
- Sono previsti ulteriori obblighi di comunicazione per: fornitori dei servizi di nomi a dominio; gestori dei registri dei nomi a dominio di primo livello; fornitori dei servizi di registrazione dei nomi a dominio; fornitori di servizi di cloud computing; fornitori di servizi di data center; fornitori di reti di distribuzione dei contenuti; fornitori di servizi gestiti; fornitori di servizi di sicurezza gestiti; fornitori di mercati online; fornitori di motori di ricerca online; fornitori di piattaforme e social network. Per tali ultimi soggetti – peraltro – è previsto dal Decreto NIS II un termine per registrarsi alla piattaforma ACN fissato nel **17 gennaio 2025**.
- Dal **1 maggio** al **30 giugno** di ogni anno i soggetti essenziali ed importanti dovranno comunicare ed aggiornare mediante la piattaforma dell'ACN un elenco delle proprie attività e dei propri servizi.
- Dal **1 gennaio 2026** i soggetti dovranno adempiere all'obbligo di notifica degli incidenti.

OBBLIGHI

Il Decreto NIS II richiede ai soggetti destinatari di adottare misure tecniche, operative ed organizzative atte a tutelare la propria sicurezza informatica e di notificare gli incidenti attendendosi a tempistiche rigorose.

L'ACN avrà la possibilità di imporre l'utilizzo di determinati prodotti e servizi TIC che siano certificati nell'ambito di sistemi europei di certificazione della cybersicurezza.

Inoltre, l'ACN potrà stabilire obblighi che siano proporzionati alle diverse categorie di soggetti considerati ed al grado di esposizione ai rischi di questi, tenuto anche conto dell'impatto socio/economico che un eventuale incidente potrebbe comportare.

A fini di controllo, l'ACN potrà altresì richiedere ai soggetti di fornire dati che dimostrino l'attuazione di politiche di sicurezza informatica, o richiedere di sottoporsi ad audit o scansioni di sicurezza, di attuare le raccomandazioni, adempiere agli obblighi imposti dal Decreto NIS II, di cessare eventuali comportamenti in violazione o attuare istruzioni.

SANZIONI

In caso di violazione del Decreto NIS II sono previste sanzioni amministrative pecuniarie che vanno:

- per i soggetti **essenziali**: fino a 100.000.000,00 euro o al 2% del fatturato totale annuo su scala mondiale dell'esercizio precedente;
- per i soggetti **importanti**: fino a 7.000.000,00 euro o all'1,4% del fatturato totale annuo su scala mondiale dell'esercizio precedente.

In caso di mancato adempimento ad un'eventuale diffida ad adempiere inviata dall'ACN, inoltre, è possibile per la stessa sospendere temporaneamente un certificato o un'autorizzazione relativi ad una parte o alla totalità dei servizi o delle attività svolte dal soggetto essenziale o disporre nei confronti delle persone fisiche (inclusi gli organi di amministrazione e direttivi) l'applicazione della sanzione amministrativa accessoria dell'incapacità a svolgere funzioni dirigenziali all'interno del soggetto essenziale o importante.

Questo articolo è redatto a scopo informativo.
Non si tratta di un parere legale esaustivo in materia di Cybersicurezza. Per eventuali ulteriori informazioni e approfondimenti specifici vi invitiamo a contattare roberto.camilli@bdo.it, gabriele.ferrante@bdo.it e sofia.ferri@bdo.it.

CONTATTI

Viale Abruzzi, 94
20131 Milano
Tel. 02 58 20 10

BDO Law S.r.l. Sta

bdolaw@bdo.it

BDO è tra le principali organizzazioni internazionali di servizi alle imprese.

La Law Alert viene pubblicata con l'intento di tenere aggiornati i clienti sugli sviluppi in ambito legale. Questa pubblicazione non può, in nessuna circostanza, essere associata, in parte o in toto, ad un'opinione espressa da BDO. Nonostante l'attenzione con cui è preparata, BDO non può essere ritenuta responsabile di eventuali errori od omissioni contenuti nel documento. La redazione di questo numero è stata completata il 2 ottobre 2024.

www.bdo.it

NEWSLETTER

Vuoi ricevere le notizie da BDO direttamente via email?
Iscriviti alle nostre mailing list.