DIRETTIVA NIS2: LE NOVITÀ IN MATERIA DI CYBERSICUREZZA

È stato pubblicato in Gazzetta Ufficiale il D.lgs. 138/2024 che recepisce la Direttiva (UE) 2022/2555, nota come NIS2 (Network and Information Security), la cui entrata in vigore è prevista per il 18 ottobre 2024, seppure il decreto di recepimento richiede l'emanazione di ulteriori e successivi atti normativi per rendere operativi molti degli obblighi che avranno un impatto diretto sulle aziende e sulle pubbliche amministrazioni.

CHE COS'È LA DIRETTIVA NIS2 E CHI SONO I SOGGETTI COINVOLTI

Con la Direttiva NIS2, l'Unione Europea intende migliorare la sicurezza e la resilienza delle infrastrutture digitali critiche. La Direttiva stabilisce norme dettagliate per la protezione delle infrastrutture essenziali, imponendo standard di sicurezza più stringenti e armonizzati tra i Paesi membri.
Nell'ambito di applicazione del decreto rientrano i soggetti pubblici e privati che appartengono alle tipologie indicate agli allegati I e II (che descrivono i settori ritenuti altamente critici e critici, ad esempio il settore bancario e delle infrastrutture dei mercati finanziari), III e IV (che descrivono le categorie di pubbliche amministrazioni cui si applica il decreto).
In estrema sintesi, le organizzazioni coinvolte nella direttiva possono essere suddivise in due categorie:

- Soggetti Importanti: comprendono settori come i servizi digitali, l'agroalimentare, la gestione dei rifiuti e i servizi postali, ossia quei servizi fondamentali per il corretto funzionamento delle economie e delle comunità.
- Soggetti Essenziali: includono organizzazioni attive in settori strategici come energia, sanità, finanza, trasporti, infrastrutture digitali, risorse idriche, spazio e difesa, nonché i soggetti individuati come critici dall'Agenzia per la Cybersicurezza Nazionale.

LE MISURE PRINCIPALI PER OTTENERE LA CONFORMITÀ ALLA NIS2

Le aziende devono adottare misure tecniche, operative ed organizzative adeguate e proporzionate per garantire la continuità operativa e la resilienza dei propri sistemi informatici e di rete di fronte a incidenti o attacchi informatici. In particolare, le misure tecniche richieste comprendono:

- Gestione del rischio cibernetico: identificare, valutare e mitigare i rischi legati alla sicurezza informatica.
- Policy di analisi dei rischi e di sicurezza dei sistemi informativi e di rete.
- Protezione della catena di fornitura: monitorare e proteggere la supply chain da potenziali vulnerabilità.
- Business Continuity Plan e Disaster Recovery Plan: procedure atte a garantire che le attività aziendali possano proseguire anche in caso di incidenti gravi.
- Gestione degli incidenti di sicurezza: predisporre piani di risposta rapida e strutturata in caso di violazioni della sicurezza.
- Formazione in materia di sicurezza informatica.
- Crittografia e autenticazione avanzata: implementare tecnologie come l'autenticazione a più fattori e la crittografia per proteggere i dati sensibili.

L'Agenzia per la Cybersicurezza Nazionale stabilirà degli obblighi proporzionati al grado di esposizione dei soggetti ai rischi individuati, alle dimensioni dei soggetti ed alla probabilità che si verifichino incidenti, nonché alla gravità, intesa come impatto sociale ed economico dell'eventuale incidente.

LE SANZIONI PREVISTE NEL DECRETO DI RECEPIMENTO DELLA DIRETTIVA

La Direttiva NIS2 prevede sanzioni molto severe per la mancata conformità. Per i Soggetti Importanti, le multe possono raggiungere i 7 milioni di euro o l'1,4% del fatturato globale annuo, mentre per i Soggetti Essenziali le sanzioni possono arrivare fino a 10 milioni di euro o al 2% del fatturato. Inoltre, non va sottovalutato l'aspetto reputazionale: il mancato coordinamento con i contenuti della Direttiva potrebbe comportare la perdita di fiducia da parte di clienti e investitori.

Complegal
AI servizio della compliance

02/80502196

Milano
via Carlo Maria Martini 1, 20122

info@complegal.it

www.complegal.it

complegal