



TMT, PROPRIETÀ INTELLETTUALE E DATA PROTECTION

NIS 2 In Italia: l'implementazione è vicina

Soggetti coinvolti

Manca poco all'implementazione e all'entrata in vigore della direttiva (UE) 2022/2555 avente ad oggetto misure per un livello comune elevato di cibersicurezza nell'Unione (cosiddetta, direttiva "NIS 2"). Lo scopo della Direttiva è garantire un livello comune elevato di cibersicurezza nell'Unione e mitigare le minacce ai sistemi informatici e di rete utilizzati per fornire servizi essenziali in settori chiave. L'iter legislativo dovrà concludersi entro il **17 Ottobre 2024**.

La nuova disciplina della NIS 2 si applica alla pubblica amministrazione e ad imprese in disparati settori tra i quali **energia (elettrica, gas, petrolio e oleodotti); trasporti; sanitario, biomedico e farmaceutico; nomi a dominio; servizi fiduciari (firme digitali, sigilli elettronici, servizi elettronici di recapito certificato, certificati relativi ai servizi, servizi relativi ai certificazione di autenticazione di siti web, servizi di conservazione, portafogli digitali); reti e servizi di comunicazioni elettroniche; alimentare; chimico; fabbricazione di computer, prodotti di elettronica e ottica; fabbricazione di veicoli e mezzi di trasporto.**

Le società soggette alla NIS2 saranno distinte tra essenziali, per le quali sarà previsto un regime di vigilanza ex ante, e importanti, che potranno essere oggetto di indagini solo in presenza elementi di prova, indicazioni o informazioni che suggeriscano possibili violazioni.

Le società essenziali e importanti saranno individuate dall'Agenzia per la cybersicurezza nazionale, all'interno dei settori sottoposti alla direttiva, in ragione della loro dimensione e del loro impatto sociale e economico.

In ogni caso, saranno considerati essenziali:

- I soggetti che operano in settori ad alta criticità: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC e spazio) che superano i massimali per le medie imprese;
- I soggetti che sono considerati infrastrutture critiche;
- I Servizi fiduciari qualificati;
- I gestori di registri dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio;
- I fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico di che si considerano medie imprese.

Il decreto legislativo attualmente in discussione in Parlamento prevede, ai fini dell'individuazione dei soggetti essenziali e importanti, una procedura di registrazione e di invio di informazioni su una piattaforma gestita dall' Agenzia per la cybersicurezza nazionale, a partire da gennaio 2025.

Obblighi

Alle società è richiesto di implementare **misure tecniche, operative e organizzative adeguate allo stato dell'arte e proporzionate al rischio** di impatto sociale ed economico e di notificare gli incidenti significativi **entro 24 ore**.

Le aziende comprese nel perimetro della nuova normativa dovranno implementare procedure minime in materia di cybersicurezza e, in particolare, procedure di analisi del rischio, di gestione degli incidenti e delle notifiche, gestione della continuità operativa, sicurezza delle reti, istruzioni di sicurezza alle risorse umane, crittografia e cifratura.

Inoltre, sarà obbligatorio attuare e documentare programmi di formazione per amministratori e dipendenti.

Sanzioni

Gli obblighi NIS ricadono direttamente sugli amministratori delle società che saranno direttamente responsabili del rispetto degli obblighi, delle violazioni e dell'implementazione delle misure di gestione dei rischi.

In caso di una diffida dell'Agenzia per la cybersicurezza nazionale relativamente all'adempimento degli obblighi NIS, il mancato adempimento potrà portare alla **sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali** all'interno del medesimo soggetto.

Le sanzioni previste in caso di inadempimento degli obblighi sono particolarmente alte. Per i servizi individuati come essenziali sono previste sanzioni **fino ad un massimo di 10.000.000 euro o del 2% del totale del fatturato annuo su scala mondiale** per l'esercizio precedente.

Provvedimenti attesi

La Commissione UE emanerà dei regolamenti esecutivi, attualmente in consultazione, per definire le soglie di significatività degli incidenti e specifiche sulle misure minime previste dal Regolamento. Inoltre, a seguito dell'approvazione del D.lgs. di implementazione Agenzia per la cybersicurezza nazionale individuerà obblighi parametrati al rischio per i soggetti essenziali e importanti e potrà persino **imporre di utilizzare categorie di prodotti certificati**.

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

DISCLAIMER

This publication is provided by Gatti Pavesi Bianchi Ludovici studio legale associato and has been duly and professionally drafted. However, the information contained therein is not a legal advice and cannot be considered as such. Gatti Pavesi Bianchi Ludovici studio legale associato cannot accept any liability for the consequences of making use of this issue without a further cooperation and advice is taken.