La Direttiva NIS 2

La Direttiva NIS 2 mira a garantire una **maggiore uniformità del livello di cybersecurity all'interno dell'UE.** Si tratta di una evoluzione della precedente Direttiva NIS 1 e presenta un ambito di applicazione più ampio, imponendo notevoli obblighi a coloro che ne sono soggetti.

Quando entrerà in vigore?

Entrerà in vigore il prossimo il **17 ottobre 2024**, data in cui tutti gli stati membri dovranno recepirla.

E in Italia? Lo scorso 7 agosto 2024 il Consiglio dei Ministri ha approvato il decreto legislativo di attuazione della direttiva NIS 2 che **non è però ancora stato pubblicato in Gazzetta ufficiale**.

A chi si applica?

! I tre criteri sono **cumulativi**, ad eccezione del caso in cui un soggetto sia identificato come essenziale o importante dallo Stato membro e gli si applichi comunque la Direttiva NIS 2 a prescindere dagli altri criteri.

Requisito territoriale

Soggetti che prestano i propri servizi o svolgono le proprie attività all'**interno dell'UE**.

+

Requisito dimensionale

Soggetti che si qualificano come media o grande impresa ai sensi della Raccomandazione (CE) 2003/361*, ossia:

- occupano **più di 50 persone**, e
- superano un **fatturato annuo di € 50 milioni**, o un **totale di bilancio annuo di € 43 milioni**

* Soglie da determinarsi al netto di eventuali imprese "collegate" o "associate

+

Requisito settoriale

Soggetti che appartengono a **settori economici critici o ad alta criticità**

Settori ad alta criticità

- Energia (con specifico riferimento al sub-sector elettricità, riscaldamento e raffreddamento, olio, gas, idrogeno)
- Trasporti (via aria, via mare, ferroviari, via strada)
- Bancario e infrastrutture finanziarie
- Sanitario
- Acqua potabile e rifiuti
- Infrastrutture digitali
- ICT service management (B2B)
- Pubbliche amministrazioni
- Aerospaziale

Altri settori critici

- Servizi postali
- Gestione dei rifiuti
- Produzione e distribuzione di prodotti chimici
- Grande distribuzione
- Manifatturiero (con specifico riferimento ai dispositivi medici, computer e prodotti elettronici)
- Fornitori di servizi digitali (in particolare, fornitori di online marketplace, motori di ricerca online, piattaforme di *social network*)
- Ricerca

Cosa impone?

Prevede **stringenti obblighi di sicurezza** che devono essere adottati dalle rilevanti società e codificati in vere e proprie policy interne.
In particolare, le società sono tenute a:

- Rispettare obblighi di governance
- Adottare misure di gestione del rischio
- Prevedere specifici obblighi di sicurezza per i terzi, valutando i contratti con i fornitori di servizi ICT
- Notificare gli incidenti informatici alle autorità competenti

Come adeguarsi?

Le società devono prepararsi alla NIS 2 non solo attraverso un'analisi delle misure tecniche, ma anche attraverso attività di compliance, secondo i seguenti step:

ANALISI PRELIMINARE

Analisi dei criteri e valutazione dell'applicabilità della Direttiva NIS 2 alla società.

Sulla base del perimetro di applicabilità individuato, conduzione di una ***gap analysis*** in merito al rispetto dei requisiti previsti dalla NIS 2 in termini di: **governance; misure tecniche e organizzative; procedure di notifica; controllo della supply chain e contratti sottoscritti**.

REMEDIATION

Implementazione delle **azioni rimediali** a seconda dei gap individuati. In particolare:

- Definizione di un **modello di governance interno** in linea con i requisiti previsti dalla NIS 2;
- **Revisione delle procedure organizzative e operative interne** (es. vendor management, gestione degli incidenti, sicurezza e utilizzo dei dispositivi);
- **Creazione di un Documento unico NIS 2** che fornisca una panoramica generale dell'approccio alla cybersicurezza; indichi il perimetro di applicazione della NIS 2; contenga una checklist di compliance che indichi come la società si sia conformata alla normativa NIS 2; contenga i riferimenti della documentazione (es. procedure, policy, misure) rilevante ai fini NIS 2;
- ***Remediation*** **dei contratti con i fornitori di tecnologie**, attraverso la redazione di un Addendum NIS 2 da allegare ai contratti con i fornitori che incorpori – ove necessario – le misure di sicurezza e controllo necessarie ad adeguarsi ai requisiti di gestione della *supply chain* richiesti dalla Direttiva NIS 2.

FORMAZIONE

Attività formativa in ambito cyber per il board interno, formulata in maniera accessibile e customizzata in base all'impostazione cyber adottata.

Perché DLA Piper vi può aiutare al meglio

I nostri professionisti, che lavorano sempre con un **approccio multi-giurisdizionale**, forniscono soluzioni in modo rapido, efficiente e con una **prospettiva integrata** delle esigenze aziendali e dell'ambiente legale in cui operano i clienti, con un'ampia conoscenza dei settori di operatività della NIS 2.

A tal proposito, DLA Piper ha sviluppato una **metodologia che minimizza gli impatti operativi** e consente alle aziende di conformarsi con gli obblighi normativi di compliance **senza creare un ulteriore livello di complessità interna**.

Contatta i professionisti di DLA Piper per preparare la tua azienda alla NIS 2!