Novità normativa

CYBER SECURITY: IMPRESE, AMMINISTRATORI E DIRETTORI SOGGETTI DA SUBITO A NUOVE RESPONSABILITÀ E OBBLIGHI DI ADEGUAMENTO ALLA NORMATIVA NIS2

Il 16 ottobre 2024 è entrato in vigore il Decreto Legislativo del 4 settembre 2024, n. 138, con il quale l'Italia ha recepito nell'ordinamento nazionale la Direttiva (UE) 2022/2555, la nuova normativa in materia di **Network Information Security (NIS2)** con l'obiettivo di garantire un livello elevato di sicurezza informatica in ambito nazionale.
Il Decreto stabilisce nuovi **obblighi in capo ad imprese e relativi organi di gestione**, introducendo **sanzioni pecuniarie e responsabilità personali** e mirando ad integrare le misure di prevenzione e gestione dei rischi informatici nelle strategie imprenditoriali.

Gli attacchi informatici e la criminalità informatica sono in costante crescita da diversi anni, sia in termini quantitativi che di sofisticazione, sfruttando l'inesorabile *escalation* del numero di dispositivi collegati in tutto il mondo alla rete Internet.
Al riguardo, si è appurato che nei primi sei mesi del 2024 gli attacchi cyber, che hanno come obiettivo anche le imprese private, sono cresciuti del 23% rispetto al semestre precedente, con una media di 9 attacchi importanti al giorno nel mondo, di cui il 11% è avvenuto in Italia, per un totale di 310 attacchi. Nel 2023 sono stati analizzati 2.779 incidenti gravi a livello globale, registrando in Italia una crescita del +64,9% rispetto al 2022, anno in cui gli attacchi informatici erano aumentati addirittura del +168,6% rispetto al 2021.[1]
Secondo il report dell'Agenzia dell'Unione europea per la cibersicurezza pubblicato nel dicembre 2024,[2] i principali attacchi alla sicurezza informatica sono il **denial of service** (attacco che impedisce agli utenti di una rete o di un sistema di accedere a informazioni, servizi e altre risorse) ed il **ransomware** (mediante il quale i cyber criminali assumono il controllo di un dispositivo della vittima, bloccando l'accesso a tutti o ad alcuni dei suoi contenuti che rimetteranno a disposizione solo dietro riscatto), seguiti dalle **violazioni o fughe di dati**, attacchi tesi ad ottenere un accesso non autorizzato a dati ed a manipolarli per interferire con il comportamento dei sistemi.

La strategia dell'UE in materia di cyber sicurezza ed il recepimento in Italia nella normativa europea.
Nel dicembre 2020 la Commissione europea e il servizio europeo per l'azione esterna (SEAE) hanno presentato una nuova strategia dell'Unione Europea in materia di cibersicurezza;[3] tale *policy* include proposte concrete volte

[1] Rapporto Clusit 2024 sulla sicurezza ICT in Italia; https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_aggiornamento_10-2024_web.pdf

[2] ENISA, *2024 Report On The State Of Cybersecurity in The Union*, 2024; https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

[3] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

all'introduzione di **strumenti normativi con l'obiettivo di rafforzare la resilienza dell'Europa a fronte delle minacce informatiche** e di garantire che tutti i cittadini e le imprese possano beneficiare pienamente di servizi e strumenti digitali affidabili e attendibili.

Negli anni successivi, le Istituzioni dell'Unione Europea hanno attuato tale strategia mediante l'emanazione di atti giuridici vincolanti[4] ed altresì della Direttiva NIS2,[5] mediante la quale è stata abrogata la precedente Direttiva in materia, risalente al 2016 e considerata non più adeguata alla rapida trasformazione digitale ed all'espansione del panorama delle minacce informatiche, tenuto che conto che *"il numero, la portata, il livello di sofisticazione, la frequenza e l'impatto degli incidenti stanno aumentando e rappresentano una grave minaccia per il funzionamento dei sistemi informatici e di rete*".[6]

Gli obiettivi dichiarati della nuova direttiva sono quindi: (**i**) l'eliminazione delle divergenze tra le normative di settore degli Stati membri, stabilendo disposizioni minime riguardanti il funzionamento di un quadro normativo coordinato; (**ii**) la modifica dell'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza, esteso a una parte più ampia dell'economia per fornire una copertura completa dei settori e dei servizi di vitale importanza per le principali attività sociali ed economiche nel mercato interno; (**iii**) l'introduzione di sanzioni e misure di esecuzione effettive che siano funzionali all'efficace applicazione di tali obblighi.[7]

Le disposizioni del Legislatore europeo sono state recepite nell'ordinamento italiano con l'adozione del Decreto Legislativo n. 138/2024 (Decreto NIS 2) in vigore dal 16 ottobre 2024, il quale risulta calibrato sulle peculiarità del panorama imprenditoriale italiano, con particolare riferimento all'individuazione sia delle imprese rientranti nell'ambito di applicazione delle nuove disposizioni, sia dei membri della *governance* soggetti agli obblighi ed alle responsabilità introdotti con il decreto.

Le **imprese** impattate dalla normativa italiana di recepimento della Direttiva NIS2, ivi compresi per determinati aspetti i **relativi fornitori diretti di beni e servizi**, sono chiamati ad intraprendere un percorso complesso, indirizzato dagli organi amministrativi e direttivi, che comporta necessariamente una approfondita attività di *assessment*, adeguata e proporzionata alla propria realtà, volta al tempestivo e corretto adempimento dei rilevanti obblighi, sia formali che sostanziali, previsti dalla normativa in questione.

Quali imprese devono adeguarsi?

Nell'ambito di applicazione del Decreto NIS2 rientrano, fra gli altri, i soggetti pubblici e privati che sono attivi nei seguenti **settori economici critici ed altamente critici**:

- Gestione di energia (elettrica, termica, gas, petrolio)
- Trasporti (su strada, aereo, ferroviario, marittimo)
- Banche e mercati finanziari
- Sanità (assistenza sanitaria, laboratori e ricerca, fabbricazione di farmaci e dispositivi medici considerati critici)
- Acqua potabile (fornitura e distribuzione)
- Acque reflue (raccolta, smaltimento, trattazione di acque urbane, domestiche e industriali)
- Infrastrutture digitali (fornitori di internet exchange point, di reti di comunicazione elettronica pubbliche o accessibili al pubblico; fornitori di servizi di DSN, cloud computing, data center, servizi fiduciari)
- Gestione dei servizi TIC (tecnologie dell'informazione e della comunicazione)
- Servizi postali e di corriere
- Gestione dei rifiuti (raccolta, trasporto, recupero e smaltimento)

[4] Fra gli altri: l'*Artificial Intelligence Act* (AI Act), Regolamento (UE) 2024/1689; il *Cyber Resilience Act* (CRA), Regolamento (UE) 2024/2847; il *Digital Operational Resilience Act* (DORA), Regolamento (UE) 2022/2554; il *Digital Services Act* (DSA), Regolamento (UE) 2022/2065.

[5] Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.

[6] Considerando (3) Direttiva (UE) 2022/2555.

[7] Considerando (5) e (6) Direttiva (UE) 2022/2555.

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

- Fornitori di servizi digitali (mercati online, motori di ricerca online, social network)
- Sostanze chimiche (fabbricazione e distribuzione)
- Imprese alimentari (produzione, trasformazione e distribuzione)
- Fabbricazione (dispositivi medici, prodotti di elettronica ed ottica, apparecchiature elettriche, macchinari e apparecchiature n.c.a., autoveicoli, rimorchi e altri mezzi di trasporto)
- Ricerca e spazio

Il decreto si applica quindi alle imprese che svolgono le suddette attività a condizione che siano qualificabili come medie o grandi imprese; **devono quindi occupare almeno 50 persone e realizzare un fatturato annuo o un totale di bilancio annuo pari ad almeno 10 milioni di euro.**

Fanno tuttavia eccezione i c.d. **soggetti critici**, i quali ricadono nell'ambito di applicazione del decreto **indipendentemente dalla loro dimensione o dal volume d'affari**; sono classificati come "critici", ad esempio, i fornitori di reti e servizi di comunicazione elettronica, i prestatori di servizi fiduciari ed i fornitori di servizi di sistema e registrazione dei nomi di dominio.

Nell'ambito di applicazione della normativa di recepimento **rientrano anche le imprese attratte per effetto del collegamento con un soggetto NIS2**, dove la nozione di "collegamento di impresa" è quella sostanziale, legata al concetto di "direzione e coordinamento" di cui agli articoli 2497 e 2545-septies del Codice civile.[8]

Il Decreto si applica anche ai **fornitori diretti di beni e servizi** delle imprese che rientrano nelle suddette categorie, così coinvolgendo i soggetti che fanno parte della loro **catena di approvvigionamento** e che pertanto, seppur non soggetti a tutti gli obblighi introdotti dal decreto, dovranno adottare misure volte ad assicurare elevati standard di sicurezza informatica al fine di non vedersi espunti all'albo dei fornitori.

In tal senso, **risulterà essenziale, accanto all'adozione di misure di sicurezza informatica, l'adeguamento alla normativa degli accordi contrattuali, definendo con precisione la ripartizione delle reciproche responsabilità riguardo all'adozione di misure di prevenzione e di gestione dei rischi di sicurezza informatica.**

Il Decreto NIS2 delinea quindi un modello "a strati",[9] secondo il quale l'ambito di applicazione della normativa va ben oltre la semplice elencazione dei soggetti appartenenti a settori ivi riportati, con un potenziale espansivo la cui reale dimensione sarà misurabile solo al completamento del processo di autodichiarazione che le imprese sono chiamate a svolgere.

Quali sono gli obblighi imposti dal Decreto?

I soggetti NIS2 devono innanzitutto **registrarsi** sulla piattaforma digitale attivata il 1° dicembre 2024 dall'Agenzia per la cybersicurezza nazionale (ACN).[10]

In occasione di tale adempimento, le imprese dovranno designare un Punto di contatto, indicandone il ruolo presso l'impresa, ed effettuare una autovalutazione della propria organizzazione quale soggetto essenziale o importante.

Il decreto dispone che, a seguito della registrazione, i soggetti devono **notificare all'ACN qualsiasi modifica** delle informazioni trasmesse **entro 14 giorni** dalla data della modifica.

Inoltre, i soggetti NIS sono tenuti a comunicare ed aggiornare, tramite la piattaforma digitale ACN, l'**elenco delle proprie attività e dei propri servizi**, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza, nonché a fornire e ad **aggiornare annualmente le informazioni** relative allo spazio di

[8] In tal senso, la Determinazione del Direttore dell'Agenzia per la Cybersicurezza Nazionale n. 38565/2024, di attuazione del Decreto NIS2; https://www.acn.gov.it/portale/documents/d/guest/determina-acn_nis_piattaforma_2024_38565_signed

[9] DI MAIO, *NIS2, adeguarsi è difficile ma possibile: ecco una guida*, 2025; https://www.agendadigitale.eu/sicurezza/imprese-e-nis2-guida-alla-nuova-normativa/

[10] https://www.acn.gov.it/portale/nis/registrazione

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

indirizzamento IP pubblico, ai nomi di dominio in uso o nella propria disponibilità, ai soggetti apicali "responsabili" dell'impresa e, infine, ad un sostituto del Punto di contatto.
Oltre ai predetti adempimenti "formali", i soggetti NIS sono altresì tenuti ad implementare nella propria organizzazione la gestione della **notifica degli incidenti** al CSIRT Italia[11].
In particolare, è obbligatorio notificare - entro i termini molto stringenti stabiliti dal decreto[12] - ogni incidente che ha un impatto significativo sulla fornitura dei servizi erogati dai soggetti NIS ed altresì ogni incidente che potrebbe causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato o per altre persone fisiche o giuridiche.
Il "nocciolo duro" degli adempimenti sostanziali introdotti a carico dei soggetti NIS2 consiste negli obblighi di **misure di gestione e di prevenzione dei rischi per la sicurezza informatica**.
Le imprese sottoposte alla disciplina del decreto devono infatti adottare **misure tecniche, operative e organizzative** (**i**) adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché (**ii**) volte a prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.
Tali misure, precisa il decreto, sono basate su un approccio multi-rischio e comprendono, fra i vari elementi di analisi dei rischi, la **sicurezza della catena di approvvigionamento**, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi.

Quali obblighi riguardano direttamente la *governance* aziendale?
Nell'ambito dei sovra menzionati obblighi di adeguamento stabiliti per le imprese, il decreto NIS2 introduce specifici obblighi e responsabilità in capo ai soggetti apicali delle stesse, ovvero ai membri degli "**organi di amministrazione**" (responsabili delle decisioni strategiche dell'organizzazione) e degli "**organi direttivi**" (delegati dai primi di supervisionare la concreta attuazione operativa delle misure adottate), ivi inclusi coloro che svolgono funzioni dirigenziali a livello di **amministratore delegato** o **rappresentante legale**.
Nello specifico, le persone che fanno parte del management aziendale (**i**) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate dall'organizzazione, (**ii**) sovrintendono all'implementazione degli obblighi di cui al decreto NIS2, (**iii**) sono responsabili delle violazioni della normativa, e sono tenuti a (**iv**) seguire una formazione in materia di sicurezza informatica ed a (**v**) promuovere la formazione dei loro dipendenti.

Quali sono i tempi per adeguarsi?
La nuova normativa introduce degli obblighi per i soggetti NIS2 a partire dal 1° gennaio 2025. In particolare:

- **entro il 28 febbraio 2025**: registrazione sulla piattaforma digitale dell'ACN, con identificazione di un Punto di contatto;
- **entro il 31 maggio 2025**: comunicazione ad ACN dei soggetti "responsabili" e di un sostituto del Punto di Contatto, nonché dell'IP pubblico e dei nomi di dominio in uso;
- **dal 1° gennaio 2026**: adempimento agli obblighi di notifica degli incidenti informatici;
- **entro il 30 giugno 2026**: comunicazione ad ACN dell'elenco delle proprie attività e dei propri servizi;
- **entro il 30 settembre 2026**: adozione di misure legali, operative e organizzative di sicurezza informatica, adeguate e proporzionate alla propria realtà aziendale.

Quali sono le sanzioni per imprese e *management* previste dal Decreto?

[11] Il "CSIRT Italia" è il Gruppo nazionale di risposta agli incidenti di sicurezza informatica ex art. 15, c. 1 decreto NIS.

[12] L'art. 25, comma 5, decreto NIS prevede l'obbligo di una pre-notifica entro 24 ore da quando si è venuti a conoscenza dell'incidente, nonché un ulteriore obbligo di notifica entro 72.

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

Le violazioni ai suddetti obblighi, compreso quello della registrazione entro il 28/02/2025, sono punite con sanzioni amministrative pecuniarie **fino a 10 milioni di euro** o, se superiore, **fino al 2% del fatturato annuo su scala mondiale** per l'esercizio precedente del soggetto.

Il decreto, inoltre, sancendo una **responsabilità personale** per i soggetti apicali relativamente alle violazioni degli obblighi, stabilisce anche per i soggetti "responsabili" l'irrogazione della **sanzione accessoria della incapacità a svolgere funzioni dirigenziali** all'interno dell'ente.

La strategia europea in materia di sicurezza informatica e le successive normative adottate pongono gli operatori economici dinanzi ad una rivoluzione tecnologica che è già nel pieno del suo svolgimento e che stravolge il modo di lavorare, di gestire i rischi e di prendere decisioni, richiedendo competenze organizzative sempre più avanzate.
Risulta quindi fondamentale per le imprese attivare tempestivamente un piano di adeguamento legale e tecnologico, secondo l'approccio multi-rischio delineato dal recente Decreto NIS2, per:
- verificare se rientrano fra i soggetti sottoposti agli nuovi obblighi
- effettuare un'approfondita analisi dei rischi per la sicurezza informatica in base all'attività svolta, ai servizi offerti ed alla propria catena di approvvigionamento
- implementare le misure necessarie ad integrare la conformità dell'impresa alla nuova normativa.

ULTERIORI INFORMAZIONI SU QUESTO ARGOMENTO O SU FATTISPECIE CORRELATE POSSONO ESSERE RICHIESTE A:

Dipartimento Compliance SLM
Responsabile: avv. Selene Sontacchi
Autore: avv. Salvatore Varvato
+39 0461 23100 – 260200 – 261977
ss@slm.tn.it