MEMO

DIRETTIVA (UE) 2022/2555
DIRETTIVA NIS2

DECRETO LEGISLATIVO
N. 138/2024

Oggetto

Tramite il Decreto legislativo 4 settembre 2024, n. 138, in data **18 ottobre 2024**, è diventata applicabile in Italia la **Direttiva (UE) 2022/2555** relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (c.d. **Direttiva NIS2**).

La **Direttiva NIS2** mira a colmare le carenze delle norme precedenti:
(i) adattandole alle esigenze attuali; nonché
(ii) rendendole adeguate alle esigenze future.

Ambito di applicazione

La NIS2 prevede **nuovi settori** identificati in base al loro grado di digitalizzazione ed importanza per l'economia e per la società, includendo nel proprio ambito di applicazione anche tutte le imprese di medie e grandi dimensioni che operano in tali **settori critici** e **ad alta criticità**.

Allo stesso tempo, viene lasciato agli Stati membri un **margine di discrezionalità** nell'individuare entità più piccole con un elevato profilo di rischio per la sicurezza.

Inoltre, la NIS2 prevede che i soggetti che rientrano nel proprio ambito di applicazione siano classificati in base alla propria importanza e suddivisi in **due categorie**:
a) soggetti **essenziali**; e
b) soggetti **importanti**.

A tali soggetti si applicheranno **regimi di vigilanza diversificati**.

Obblighi di sicurezza e notifica degli incidenti

La NIS2 prevede l'adozione di **misure tecniche, operative e organizzative** adeguate e proporzionate per:

a) gestire i **rischi posti alla sicurezza** dei sistemi informatici e di rete che i soggetti essenziali e importanti utilizzano nelle proprie attività o nella fornitura dei propri servizi; nonché

b) prevenire o ridurre al minimo l'**impatto degli incidenti** per i destinatari di tali servizi.

In particolare, viene adottato un **approccio multirischio** mirante a proteggere sia ***(i)*** i sistemi informatici e di rete sia ***(ii)*** il loro ambiente fisico da incidenti individuando un **elenco minimo** di elementi di sicurezza che devono essere applicati.

Vengono introdotte disposizioni più precise sul **processo di segnalazione degli incidenti**, imponendo, a seconda delle circostanze, di effettuare:

a) un preallarme;
b) una notifica dell'incidente;
c) una relazione intermedia; nonché
d) una relazione finale dell'incidente.

Inoltre, viene affrontato il tema della **sicurezza della catena di approvvigionamento** e delle relazioni con i fornitori imponendo ai soggetti importanti ed essenziali di tenere in considerazione gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i propri diretti fornitori (c.d. **sicurezza della *supply chain***).

Misure di vigilanza e regime sanzionatorio

La NIS2 introduce **misure di vigilanza** più rigorose per le Autorità nazionali e mira ad armonizzare i **regimi sanzionatori** in tutti gli Stati membri.

In particolare, per rafforzare l'applicazione della Direttiva sui soggetti obbligati, viene previsto un **elenco minimo di mezzi di vigilanza** attraverso i quali le Autorità competenti possono vigilare sui soggetti essenziali e importanti (come audit periodici e mirati, controlli in loco e a distanza, richieste di informazioni e accesso a dati o documenti) contemplando, inoltre, una **differenziazione** dei regimi di vigilanza tra soggetti essenziali e importanti per garantire un giusto **bilanciamento degli obblighi** che i soggetti sono tenuti a rispettare.

Per quanto riguarda i **casi di non conformità** rispetto a quanto stabilito dalla normativa:

a) i **soggetti essenziali** sono soggetti a sanzioni amministrative pecuniarie pari a un massimo di **10 000 000 euro** o ad un massimo del **2 % del totale del fatturato mondiale annuo** per l'esercizio precedente dell'impresa a cui il soggetto essenziale appartiene, se tale importo è superiore;

b) i **soggetti importanti** sono soggetti a sanzioni amministrative pecuniarie pari a un massimo di **7 000 000 euro** o a un massimo dell'**1,4 % del totale del fatturato mondiale annuo** per l'esercizio precedente dell'impresa a cui il soggetto importante appartiene, se tale importo è superiore.

Cooperazione a livello dell'Unione Europea

La NIS2 intende anche promuovere una **cooperazione operativa** rapida ed efficace fra gli Stati membri dell'Unione istituendo una **rete europea di organizzazioni di collegamento per le crisi informatiche** (c.d. **EU-CyCLONe**) al fine di:

(i) sostenere la **gestione coordinata degli incidenti** e delle crisi di cybersicurezza su larga scala, nonché

(ii) garantire il regolare **scambio di informazioni** pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione.

Timeline

Per quanto riguarda l'Italia, il **D.Lgs 4 settembre 2024, n. 138** indica che:

- **entro il 31 dicembre 2024**: è consigliabile svolgere un assessment per comprendere se si rientri nell'ambito di applicazione della NIS2;

- **tra il 1° gennaio e il 28 febbraio 2025**: sulla base dell'assessment, i soggetti che ritengano di rientrare nell'ambito di applicazione del decreto dovranno registrarsi su una piattaforma digitale messa a disposizione dall'Agenzia per la Cybersicurezza Nazionale (ACN) inserendo le informazioni richieste;

- **entro il 31 marzo 2025**: sulla scorta delle registrazioni effettuate mediante la piattaforma, l'ACN redigerà un elenco dei soggetti essenziali e dei soggetti importanti;

- **successivamente**, l'ACN, per mezzo della piattaforma, comunicherà ai soggetti registrati il proprio inserimento nell'elenco dei soggetti essenziali o importanti predisposto;

- **tra il 15 aprile e il 31 maggio 2025**: i soggetti a cui verrà inviata la comunicazione di inclusione nell'elenco dovranno fornire, mediante la piattaforma, le ulteriori informazioni richieste, tra cui il nome, il ruolo e i recapiti della persona fisica responsabile di un soggetto essenziale che assicura, sotto la propria responsabilità, il rispetto di quanto stabilito nel decreto.

In merito alla effettiva applicazione degli obblighi previsti dalla normativa, il **D.Lgs. 4 settembre 2024, n. 138** prevede infine che:

- **entro 9 mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti essenziali e importanti**, diviene applicabile l'obbligo di **notifica degli incidenti**;

- **entro 18 mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti essenziali e importanti**, i soggetti dovranno conformarsi agli obblighi:

  (i) relativi agli **organi di amministrazione e direttivi**;
  (ii) in materia di **misure di gestione dei rischi** per la sicurezza informatica; nonché
  (iii) di raccolta e mantenimento di una **banca dei dati** di registrazione dei nomi di dominio, ove applicabile.

Because we care

ITALIA

Roma
Via Principessa Clotilde, 7
00196 (RM)
T +39 06 36227.1
F +39 06 3235161
mail@tonucci.com

Milano
Via Gonzaga, 5
20123 (MI)
T +39 0285919.1
F +39 02860468
milano@tonucci.com

Padova
Via Trieste, 31/A
35121 (PD)
T +39 049 658655
F +39 049 8787993
padova@tonucci.com

Prato
Via Giuseppe Valentini, 8/A
59100 (PO)
T +39 0574 29269
F +39 0574 604045
prato@tonucci.com

Trieste
Via Del Coroneo, 33
34133 (TS)
T +39 040 366419
F +39 040 0640348
trieste@tonucci.com

Foggia
Via Vincenzo Lanza, 14
71121 (FG)
T +39 0881 707825
F +39 0881 567974
foggia@tonucci.com

ALBANIA

Tirana
Torre Drin - Rruga Abdi Toptani
1001 (TR)
T +355 (0) 4 2250711/2
F +355 (0) 4 2250713
tirana@tonucci.com

ROMANIA

Bucharest
Clădirea Domus II
Str. Știrbei Vodă nr. 114-116
Etaj 2, Sector 1
010119 București
T +40 31 4254030/1/2
F +40 31 4254033
bucharest@tonucci.com