# LA DIRETTIVA NIS2

Direttiva UE n. 2022/2555

Avv. Marco Verani

STUDIO LEGALE
VERANI

# DIRETTIVA NIS 2 – IL CONTESTO LEGISLATIVO

La direttiva (UE) n. 2022/2555, nota anche come «Direttiva NIS2», del Parlamento Europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cyber sicurezza nell'Unione Europea, abroga la precedente Direttiva NIS.

La Direttiva è entrata in vigore il 17 gennaio 2023 e dovrà essere recepita dagli Stati membri entro il 17 ottobre 2024.

**Novità: recepita con il D.Lgs. 138/2024 (Gazz. Uff. ottobre 2024)**.

Attraverso l'adozione della NIS2 verranno rafforzati dei livelli standard di sicurezza, incidendo in via prioritaria su tre pilastri fondamentali.

STUDIO LEGALE VERANI

# Decreto di recepimento (D.lgs. 138/2024)
# NOVITÀ OTTOBRE 2024

## PRINCIPALI DIFFERENZE TRA LA DIRETTIVA NIS2 E IL D.LGS. 138/2024

**D.lgs. 138/2024**: Adotta la struttura imposta dalla Direttiva ma con dettagli specifici per l'Italia, includendo la designazione delle autorità nazionali, le procedure operative locali e specificazioni – con allargamento dei settori di operatività.

### Adattamenti Specifici Nazionali:

Il D.lgs. 138/2024 è più dettagliato rispetto alla direttiva su come le entità italiane devono rispondere ai requisiti, prevedendo ad esempio la collaborazione con autorità specifiche italiane come l'Agenzia per la cybersicurezza nazionale.

### Inclusione di PMI Strategiche:

Mentre la Direttiva NIS2 pone criteri generali, il D.lgs. italiano **amplia l'obbligo includendo le PMI italiane che svolgono attività strategiche**, definendo anche criteri specifici per queste aziende.

### Settori Aggiuntivi:

Il **D.lgs. 138/2024 include settori specifici** non menzionati esplicitamente nella NIS2, adattando la normativa a settori strategici italiani non presenti in altri Stati membri.

STUDIO LEGALE VERANI

# DIRETTIVA NIS2 – I PILASTRI FONDAMENTALI

capacità degli Stati membri di gestione delle crisi cibernetiche in relazione all'architettura istituzionale e alla strategia nazionale

gestione del rischio da parte degli operatori, prevedendo misure di sicurezza adeguate e un sistema di notifica degli incidenti efficace e reattivo

cooperazione e condivisione delle informazioni, attraverso diverse modalità di scambio, a livello nazionale ed europeo

STUDIO LEGALE VERANI

# DIRETTIVA NIS 2 – Applicabilità

La NIS2 effettua una distinzione tra settori «ad alta criticità» e ad «altri settori critici» (Allegati I e II) e tra operatori di servizi «essenziali» e di servizi «importanti» (Articolo 3), a seconda del livello di criticità che essi rivestono per la cybersicurezza europea.

La Direttiva si applica, in generale, ai soggetti pubblici o privati, operanti in uno dei settori ad alta criticità o altri settori critici, che presentano le caratteristiche proprie delle medie imprese (**meno di 250 dipendenti, fatturato annuo non superiore ai 50 milioni di euro, bilancio anno non superiore a 43 milioni di euro**) o che superano i massimali previsti per le stesse.

** Le organizzazioni che rientrano nella categoria delle piccole imprese e delle micro imprese (meno di 50 dipendenti, fatturato annuo non superiore ai 10 milioni di euro) possono comunque essere soggette alla NIS2 se sono l'**unico fornitore di un servizio essenziale** all'interno di uno stato membro o se l'interruzione del loro servizio potrebbe avere un impatto significativo sulla sicurezza pubblica o sulla salute.

STUDIO LEGALE VERANI

# DIRETTIVA NIS 2 – Applicabilità

## Settori ad alta criticità (Allegato I)

- **Energia**: elettricità, petrolio, gas, idrogeno, riscaldamento e raffreddamento
- **Trasporti**: strada, ferrovia, aria e acqua
- **Bancario**: banche, borse, istituzioni finanziarie, infrastrutture dei mercati fin.
- **Sanità**: ospedali, laboratori, centri di ricerca, farmaceutica e dispositivi medici
- **Acqua**: acque reflue e acqua potabile
- **Infrastrutture digitali**: data center, cloud computing, fornitori DNS ecc.
- **Servizi ICT**: servizi gestiti e servizi di sicurezza gestiti
- **Pubblica Amministrazione**: entità governative centrali e regionali
- **Spazio**: operatori di infrastrutture terrestri

## Altri settori critici (Allegato II)

- **Posta e corrieri**: spedizione di posta e pacchi
- **Gestione dei rifiuti**: raccolta, trattamento e riciclaggio dei rifiuti
- **Prodotti chimici**: produzione e distribuzione di prodotti chimici
- **Alimentare**: produzione, trasformazione e distribuzione di generi alimentari
- **Manifatturiero**: produttori di dispositivi medici, macchine e macchinari, veicoli e dispositivi elettrici / elettronici
- **Servizi digitali**: motori di ricerca, mercati online e reti sociali
- **Ricerca**

STUDIO LEGALE VERANI

# Decreto di recepimento (D.lgs. 138/2024)
# NOVITÀ OTTOBRE 2024

## PRINCIPALI DIFFERENZE TRA LA DIRETTIVA NIS2 E IL D.LGS. 138/2024

La prima fase consisterà nell'identificare con precisione gli operatori che saranno soggetti alla normativa. In particolare, seguendo il testo europeo, il Decreto Legislativo 138/2024 stabilisce innanzitutto che tra tali operatori vi saranno soggetti sia pubblici che privati operanti nei settori elencati negli allegati I-II e III-IV del decreto. Tuttavia, rispetto alla Direttiva europea, il testo italiano aggiunge un dettaglio, specificando che gli operatori devono essere sottoposti alla giurisdizione nazionale.

**Quando è applicabile la normativa anche alle piccole imprese?**

Il D.lgs. 138/2024 estende l'applicabilità della normativa all'ente che sia (anche se considerato piccola impresa):

- identificato come "critico" ai sensi della Direttiva RCE;
- fornitore di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico;
- prestatore di servizi fiduciari;
- gestore di registri di dominio di primo livello o fornitore di servizi di sistema dei nomi a dominio;
- fornitore di servizi di registrazione dei nomi a dominio;
- già stato identificato come operatore di servizi essenziali o fornitore di servizi digitali ai sensi della Direttiva NIS;
- l'unico fornitore nazionale di un servizio essenziale;
- fornitore di un servizio che, se perturbato, potrebbe comportare un rischio sistemico significativo;
- critico per la sua particolare importanza a livello nazionale;
- critico in quanto elemento sistemico della catena di approvvigionamento di soggetti essenziali o importanti.

STUDIO LEGALE VERANI

# Decreto di recepimento (D.lgs. 138/2024)
# NOVITÀ OTTOBRE 2024

## IMPORTANZA DELLA FILIERA (SUPPLY CHAIN)

Il D.lgs. 138/2024 approfondisce il concetto di **filiera** rispetto alla Direttiva NIS2, ampliando il perimetro delle **entità obbligate** ad adottare misure di cybersicurezza per includere non solo i soggetti principali, ma **anche gli attori coinvolti nei processi e nelle catene di fornitura collegati**. Questo è particolarmente rilevante in Italia, dove molte aziende dipendono da un ampio ecosistema di fornitori e partner. Ecco come viene trattata la filiera:

### 1. Estensione ai Fornitori Critici

**Differenza con la Direttiva NIS2**: La direttiva si focalizza principalmente sui fornitori di servizi essenziali e sugli operatori principali. Il D.lgs. 138/2024, invece, prevede che non solo le entità principali, ma anche i loro **fornitori critici** siano inclusi nel perimetro delle misure di cybersicurezza. Questi includono:

- **Fornitori di servizi tecnologici che supportano infrastrutture critiche**, come i fornitori di software, hardware e servizi cloud specifici per settori critici.
- **Subappaltatori e partner logistici** che gestiscono operazioni essenziali o che hanno accesso a dati sensibili legati alle attività delle entità principali.

### 2. Obblighi per le Catene di Fornitura nel Settore ICT

Il D.lgs. stabilisce obblighi specifici per gli attori coinvolti nella **filiera delle tecnologie dell'informazione e comunicazione (ICT)**. Questi includono:

- Le aziende che forniscono componenti hardware e software essenziali per la gestione delle reti di telecomunicazione e delle infrastrutture digitali.
- I fornitori di servizi di manutenzione e supporto tecnico per sistemi informatici e infrastrutture di rete.

STUDIO LEGALE VERANI

# Decreto di recepimento (D.lgs. 138/2024)
# NOVITÀ OTTOBRE 2024

## IMPORTANZA DELLA FILIERA (SUPPLY CHAIN)

### 3. Filiera nel Settore Energetico e delle Infrastrutture Critiche

Nel **settore energetico**, il decreto richiede che non solo i produttori e i distributori principali, ma anche i loro **fornitori di materiali e servizi di manutenzione** siano inclusi nel perimetro di protezione. Ad esempio:

- Fornitori di apparecchiature per la **gestione e la manutenzione delle reti elettriche e del gas**.
- **Partner logistici e operatori di trasporto** che gestiscono la distribuzione di energia o di risorse critiche.

### 4. Filiera Agroalimentare e dei Trasporti

In linea con l'importanza attribuita alla **filiera agroalimentare**, il D.lgs. estende gli obblighi di cybersicurezza anche ai **fornitori e partner logistici** che operano nella catena di **distribuzione alimentare**. Questo include:

- Le aziende che forniscono **sistemi di tracciamento** digitale per la gestione della logistica e della **catena del freddo**.
- I partner che operano nei servizi di trasporto, inclusi quelli che gestiscono la **distribuzione alimentare e i sistemi di stoccaggio**.

### 5. Misure Specifiche di Coordinamento per la Filiera

Il D.lgs. 138/2024 prevede anche che le entità principali implementino misure di **valutazione e controllo** per i propri fornitori e partner, tra cui:

- **L'obbligo di sottoporre i fornitori a verifiche di conformità e audit** periodici per accertarsi che rispettino gli standard di cybersicurezza.
- La necessità di stabilire **contratti specifici che includano clausole di sicurezza cibernetica**

STUDIO LEGALE VERANI

# DIRETTIVA NIS 2 – Principali obblighi (1)

## Gestione del Rischio

Le organizzazioni sono tenute ad implementare processi idonei alla **valutazione dei rischi informatici** e **all'adozione delle misure tecniche e organizzative necessarie**. Tra queste rientrano la presenza di processi di gestione degli incidenti, il **rafforzamento della sicurezza della supply chain**, il potenziamento della sicurezza delle reti, l'implementazione di misure adeguate per il controllo degli accessi e l'adozione di soluzioni crittografiche.

## Responsabilità aziendale

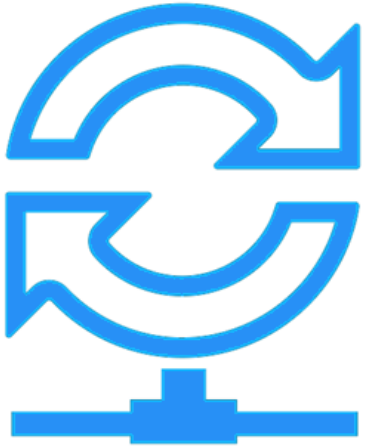
La Direttiva prevede che il management aziendale abbia il compito di supervisionare, approvare e partecipare a programmi formativi inerenti le procedure di sicurezza informatica dell'organizzazione e la gestione dei rischi informatici. In caso di violazioni, i dirigenti possono essere soggetti a sanzioni, comprese responsabilità personali, amministrative e contabili e la sospensione temporanea dalle loro funzioni dirigenziali.

STUDIO LEGALE VERANI

# DIRETTIVA NIS 2 – Principali obblighi (2)

## Obblighi di comunicazione

Le entità essenziali e importanti sono tenute a dotarsi di sistemi che consentano la tempestiva comunicazione degli eventi di sicurezza aventi un impatto significativo sui loro servizi o sui destinatari dei medesimi. La Direttiva stabilisce specifiche tempistiche di notifica, come ad esempio l'obbligo di un «*early warning*» entro 24 ore dall'evento.



## Continuità operativa

Le organizzazioni devono elaborare piani strategici per garantire la continuità delle operazioni in caso di gravi incidenti informatici. Tali piani devono includere strategie per il ripristino dei sistemi, procedure di emergenza e la costituzione di un team di risposta alle crisi.

STUDIO LEGALE VERANI

# DIRETTIVA NIS 2 – L'impatto sulle aziende italiane

La direttiva NIS2 adotta un approccio «**Risk Based**»: secondo l'articolo 21, le organizzazioni devono adottare misure tecniche, organizzative e operative adeguate e proporzionate per la gestione del rischio inerente alla **sicurezza dei sistemi informatici e delle reti utilizzate nelle loro attività e nella fornitura di servizi**.

## Quali sono le attività necessarie per le organizzazioni soggette alla Direttiva?

**Comprendere la propria categoria di appartenenza** sulla base dei parametri delineati nell'articolo 3 della Direttiva, che specifica le categorie di soggetti essenziali e importanti.

Elaborare e adottare una **strategia basata sul rischio** (Risk Based Strategy). Ciò include la realizzazione di una gap analysis e la redazione di un documento di analisi dei rischi.

Sviluppare un **piano di gestione degli incidenti** chiaro, concretamente applicabile e allineato a quanto previsto dalla Direttiva circa gli obblighi di notifica.

**Implementare soluzioni tecniche adeguate** e adottare un approccio di **monitoraggio continuo** per garantire che le misure di sicurezza siano sempre aggiornate ed efficaci.

STUDIO LEGALE VERANI

# DIRETTIVA NIS 2 – Sanzioni per le organizzazioni

## Soggetti Essenziali:

**Violazioni Gravi**:

- *Definizione*: **Inosservanza obblighi di implementazione delle misure di sicurezza**, monitoraggio, **formazione dirigenti e dipendenti**, mancata gestione del rischio, **notifica di incidenti** significativi, mancato rimedio a tali incidenti, inosservanza delle istruzioni vincolanti dall'Autorità NIS, o fornitura di informazioni false o inesatte.
- *Sanzioni*: **Multa fino a 10.000.000 di euro o il 2% del fatturato annuo globale**, se superiore.

**Altre Violazioni**:

- *Definizione*: Mancata registrazione, aggiornamento delle informazioni richieste, o mancata collaborazione con l'Autorità NIS.
- *Sanzioni*: Sanzione massima dello 0,1% del fatturato annuo.

STUDIO LEGALE VERANI

# DIRETTIVA NIS 2 – Sanzioni per le organizzazioni

## Soggetti importanti:

**Violazioni Gravi:**

- *Definizione*: Simili a quelle per i soggetti essenziali, inclusa la mancata conformità alle istruzioni NIS in casi gravi.
- *Sanzioni*: **Multa fino a 7.000.000 di euro o l'1,4% del fatturato annuo globale, se superiore**

**Altre Violazioni:**

- *Definizione*: Violazioni minori come la mancata osservanza di obblighi documentali o comunicazioni ritardate.
- *Sanzioni*: Sanzione massima dello 0,07% del fatturato annuo.

STUDIO LEGALE VERANI

# DIRETTIVA NIS 2 – Sanzioni (amministratori e dirigenti)

## Amministratori e dirigenti:

**Violazioni Gravi**: Mancata adozione delle misure necessarie per conformarsi alle istruzioni o inosservanza degli obblighi di gestione del rischio e notifica (Artt. 23 e 38, comma 6 D.lgs. 138-2024).

- *Conseguenze*: **Sospensione temporanea dalle funzioni dirigenziali** fino alla rettifica delle violazioni (Art. 38, comma 6 D.lgs. 138-2024).

**Altre Violazioni**: Violazioni amministrative come il mancato rispetto di obblighi documentali.

- *Conseguenze*: Possibile responsabilità disciplinare o amministrativo-contabile (Art. 38, comma 7 D.lgs. 138-2024).

STUDIO LEGALE VERANI

# POSSIAMO AIUTARTI?

Lo Studio Legale Verani, in collaborazione con i propri partners, fornisce consulenza legale e trasversale per ciò che concerne l'implementazione delle normative inerenti la protezione dei dati personali, la privacy e la cybersicurezza.

Ti possiamo aiutare a valutare l'impatto della Direttiva NIS2 e della normativa italiana ed europea sulla privacy e protezione dei dati personali (GDPR) sulla tua attività, al fine di attuare strategie pragmatiche volte ad assicurare la conformità delle policy aziendali al rinnovato contesto normativo.

STUDIO LEGALE VERANI

# Avv. Marco Verani

verani@studiolegaleverani.com

Corso Vittorio Emanuele II, n. 8

Lodi


Seguimi su linkedin:

linkedin.com/in/marco-verani

STUDIO LEGALE VERANI