consulenza e formazione alle organizzazioni e ai territori
via Giovanni Prati, 23 - 38079 Tione di Trento (TN)
via Lungadige Leopardi, 81 - 38122 Trento
viale Nogarole, 79 - 37047 San Bonifacio (VR)
p.iva 01871820229 tel. 0465 322514 info@dream.tn.it www. dream.tn.it

SCHEDA DI SINTESI

Recepimento ed attuazione della direttiva NIS 2 (2022/2555)

consulenza e formazione alle organizzazioni e ai territori
via Giovanni Prati, 23 - 38079 Tione di Trento (TN)
via Lungadige Leopardi, 81 - 38122 Trento
viale Nogarole, 79 - 37047 San Bonifacio (VR)
p.iva 01871820229 tel. 0465 322514 info@dream.tn.it www. dream.tn.it

La nuova direttiva NIS2, promulgata in ambito europeo, persegue l'obiettivo di una creazione di un framework di cybersicurezza europeo che armonizzi e superi le discrasie applicative fra stati membri.

A partire dal 18 ottobre, tutti gli stati membri sono tenuti ad adottare nel proprio impianto legislativo provvedimenti che rispettino la direttiva: in Italia la norma è stata implementata attraverso il D.lgs. 138/2024, che ha innanzitutto individuato **l'autorità di riferimento nell'Agenzia per la Cibersicurezza Nazionale (ACN)**

Rispetto alla precedente direttiva (anche conosciuta come NIS1), la NIS2:

1. è applicabile a più categorie di **soggetti** espressamente indicati;
2. richiede ai destinatari la compilazione di una specifica analisi dei **rischi** di cybersicurezza;
3. richiede l'adozione di adeguate **misure di sicurezza**, la specificità delle quali però sarà adeguata al contesto ed al settore di operatività, considerando quindi anche la capacità di spesa del singolo ente coinvolto.

ADEMPIMENTI e SCADENZE:

1. entro il **17 gennaio 2025 per alcuni settori essenziali o importanti** (o **28 febbraio**, per gli altri casi, come verrà specificato sotto alla sezione tempistiche) è richiesto alle imprese di valutare, sulla base dei criteri indicati nel decreto, il proprio coinvolgimento nell'attuazione della direttiva; pertanto, sarà necessario registrarsi sulla piattaforma presente sul sito dell'Agenzia per la Cybersicurezza Nazionale.

   Dal **1° dicembre 2024**, infatti, é disponibile sul sito dell'ACN la piattaforma per la registrazione di imprese e pubbliche amministrazioni tenute agli obblighi di cybersicurezza, al link https://www.acn.gov.it/portale/nis/registrazione;

   successivamente, entro il **15 Aprile 2024**, ACN dirà se il soggetto è effettivamente un soggetto a cui si applica la NIS2;

2. entro il **1° gennaio 2026**, i soggetti a cui si applica la NIS2 devono adeguarsi all'articolo 25 relativo alla notifica degli incidenti; questo richiede come minimo di stabilire il processo di gestione degli incidenti;

3. entro il **1° gennaio 2026**, i soggetti a cui si applica la NIS2 devono adeguarsi all'art. 30 e quindi aggiornare ogni anno le informazioni richieste dalla piattaforma ACN con l'elenco di attività e servizi e la descrizione delle loro caratteristiche;

4. entro **ottobre 2026**, i soggetti a cui si applica la NIS2 devono adeguarsi agli articoli 23 (sugli obblighi degli organi di amministrazione e direttivi), 24 (gestione dei rischi e implementazione delle misure di sicurezza) e 29 (relativo alla banca dati dei nomi a dominio).

consulenza e formazione alle organizzazioni e ai territori
via Giovanni Prati, 23 - 38079 Tione di Trento (TN)
via Lungadige Leopardi, 81 - 38122 Trento
viale Nogarole, 79 - 37047 San Bonifacio (VR)
p.iva 01871820229 tel. 0465 322514 info@dream.tn.it www. dream.tn.it

PRINCIPALI ELEMENTI D'ATTENZIONE DELLA NORMATIVA

Campo di applicazione	L'applicabilità dipende dai settori e dalla dimensione, in particolare si applica: - alle **imprese** rientranti nei settori "ad alta criticità" di cui all'allegato I del decreto, (tra cui energia, trasporti, settore bancario, sanitario, infrastrutture digitali) e "critici" di cui all'allegato II del decreto (altri settori critici) (tra cui alimentare, chimica, manifattura, servizi digitali, ricerca). Rispetto a questi settori, è inoltre stato introdotto un criterio di individuazione su base dimensionale, che estende l'applicazione della norma: - alle **grandi** aziende con più di 250 addetti e un fatturato maggiore ai 50 milioni di euro; - alle **medie** imprese con più di 50 dipendenti e un fatturato superiore ai 10 milioni di euro; - le **piccole** imprese qualora rientranti nei settori come indicato negli allegati I (settori ad alta criticità), II (altri settori critici), III (Amministrazioni centrali, regionali, locali e di altro tipo), IV (Ulteriori tipologie di soggetti) della norma. La NIS2 si applica infine: - agli ulteriori enti indicati all'articolo 3 comma 5 del decreto; - a qualsiasi impresa, indipendentemente dalle sue dimensioni, collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei criteri elencati all'articolo 3 comma 10.[1]

[1] a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;
b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;
c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale;

	Per determinare se un soggetto sia da considerarsi una media o grande impresa ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE, si applica l'articolo 6, paragrafo 2, del medesimo allegato. [2] Con la NIS 2 sono i soggetti che devono capire se rientrano in quelli a cui si applica la NIS 2 e registrarsi autonomamente sulla piattaforma messa a disposizione da ACN entro gennaio 2025. ACN potrebbe anche segnalare al soggetto che si è registrato che non rientra nei criteri. Gli ambiti di applicazione sono inoltre approfonditi sul sito di ACN all'indirizzo https://www.acn.gov.it/portale/nis/ambito
Tempistiche	La registrazione sulla piattaforma di ACN sarà possibile **tra il 1° dicembre 2024 e il 28 febbraio 2025**. Il termine ultimo, tuttavia, non è uguale per tutti. Saranno tenuti a registrarsi **entro il 17 gennaio 2025:** • i fornitori di servizi di sistema dei nomi di dominio, • i gestori di registri dei nomi di dominio di primo livello, • i fornitori di servizi di registrazione dei nomi di dominio, • i fornitori di servizi di cloud computing; • i fornitori di servizi di data center, • i fornitori di reti di distribuzione dei contenuti, • i fornitori di servizi gestiti,

d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

[2] ***Articolo 2*** **- Effettivi e soglie finanziarie che definiscono le categorie di imprese**
1. La categoria delle microimprese delle piccole imprese e delle medie imprese (PMI) è costituita da imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR.
2. Nella categoria delle PMI si definisce piccola impresa un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR.
3. Nella categoria delle PMI si definisce microimpresa un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di EUR.
Articolo 6 **- Determinazione dei dati dell'impresa:** si consiglia di consultare il testo della raccomandazione e Allegato.

	• i fornitori di servizi di sicurezza gestiti, • fornitori di mercati online, di motori di ricerca e di piattaforme social. **Entro il 31 marzo di ogni anno** successivo alla data di entrata in vigore del presente decreto, l'ACN redige l'**elenco dei soggetti essenziali e dei soggetti importanti**, sulla base delle registrazioni e, tramite la piattaforma, comunica agli interessati l'inserimento, la permanenza o l'espunzione da detto elenco. A questo punto, **entro aprile 2025 l'Agenzia dovrà definire gli obblighi** per le aziende italiane sulla base della direttiva. Una volta venute a conoscenza degli obblighi, a **maggio** le aziende registrate dovranno tornare sul sito dell'ACN per controllare e aggiornare i loro dati ed entrare a tutti gli effetti nel mondo Nis2. **La registrazione in piattaforma sarà aperta ogni anno** tra gennaio e febbraio.
Designazione del "Punto di Contatto"	In sede di registrazione sul portale ACN, sarà richiesta la designazione di una figura che funga da "Punto di Contatto" ovvero una persona fisica designata dal soggetto NIS con il compito di curare l'attuazione delle disposizioni del Decreto per conto del soggetto stesso, interloquendo con l'Autorità. Questo aspetto quindi, benché formale, presuppone da parte dell'ente interessato, il compimento di valutazioni sostanziali legate alla governance. Le funzioni di punto di contatto possono essere svolte dal **rappresentante legale**, da un **procuratore generale** o da un **dipendente** appositamente **delegato** dal rappresentante legale. Il punto di contatto riferisce direttamente al vertice gerarchico, nonché agli organi di amministrazione e direttivi della società.

Valutazione del rischio	Il decreto all'articolo 24 richiede un approccio al rischio informatico di tipo multiplo: logico, fisico, governo, lock-in tecnologico, utilities. A riguardo, i criteri interpretativi resi disponibili dalla Commissione Europea, indicano di considerare nell'apposita valutazione del rischio i seguenti elementi: 1. sabotaggi, 2. furti, 3. incendi, 4. inondazioni, 5. problemi di telecomunicazione, 6. problemi di interruzioni di corrente, 7. qualsiasi accesso fisico non autorizzato in grado di compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi, 8. guasti del sistema, 9. errori umani, azioni malevole, fenomeni naturali.
Obblighi per le imprese	Ai destinatari interessati dalla Direttiva, si richiede di adottare specifiche **misure tecniche, operative e organizzative adeguate e proporzionate,** che comprendano almeno i seguenti elementi: a. politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete; b. gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26; c. continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi; d. 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; e. sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;

	f. politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica; g. pratiche di igiene di base e di formazione in materia di sicurezza informatica (notare che l'articolo 23, correttamente, impone agli organi di amministrazione e gli organi direttivi dei soggetti NIS 2 una formazione in materia di sicurezza informatica); h. politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura (notare che non è chiara la differenza tra crittografia (cryptography) e cifratura (encryption), presente peraltro anche nella Direttiva); i. sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti; j. uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno. E' inoltre richiesto ai destinatari di rinforzare i controlli relativi alla propria **catena di approvvigionamento.** Infine, gli articoli 30, 31 e 32 dicono che ACN potrebbe richiedere l'applicazione di "misure minime", chiamate "obblighi": si resta pertanto in attesa di aggiornamenti da parte degli enti incaricati.
Gestione dei rischi Cyber e comunicazione di incidenti significativi (adeguamento richiesto entro il 1° gennaio 2026)	Anche grazie al supporto del Regolamento d'attuazione alla NIS2, la Commissione ha stabilito **requisiti tecnici e metodologici delle misure per la gestione dei rischi in materia di cyber sicurezza** previsti dalla direttiva ed individuato tutte **le ipotesi in cui un incidente va considerato "significativo" o "ricorrente"** ai sensi della direttiva stessa e perciò vi sia l'obbligo di notificarlo all'ACN o meno. 1. Si ricorda come nella direttiva sia sottolineato che un requisito tecnico o metodologico di una misura di gestione dei rischi di cibersicurezza dovrà essere applicato "*ove opportuno*", "*ove applicabile*" o "*nella misura in*

	cui ciò sia fattibile". Il regolamento individua come incidenti **significativi** i casi in cui risulti: 2. "un danno finanziario diretto all'entità interessata superiore a 500 000 EUR o al 5 % del fatturato totale annuo dell'entità interessata nell'esercizio finanziario precedente, se inferiore; 3. l'esfiltrazione di segreti commerciali ai sensi dell'articolo 2, punto 1, della direttiva (UE) 2016/943 dell'entità pertinente; 4. il decesso di una persona fisica; 5. danni considerevoli alla salute di una persona fisica"; 6. si sia verificato un accesso non autorizzato, sospetto di dolo e non autorizzato alla rete e ai sistemi informativi, che possa causare gravi perturbazioni operative. Gli incidenti **ricorrenti**, invece, singolarmente non sono considerati un incidente significativo, ma sono **considerati collettivamente come un unico incidente significativo se soddisfano altri criteri**, vale a dire: si sono verificati "almeno due volte nell'arco di 6 mesi; hanno la stessa causa apparente alla radice; e soddisfano collettivamente i criteri di cui all'articolo 3, paragrafo 1, lettera a)".

Incidenti informatici: a valle della NIS2, quando rivolgersi al Garante Privacy e quando ad ACN?

L'istituto del data breach in ambito privacy ruota intorno alla nozione di **violazione di dati personali**, per tale intendendosi "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
Parallelamente, ai fini NIS 2, deve essere considerato un **incidente**: "l' evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi".

Vediamo pertanto come non tutti gli incidenti sono automaticamente qualificabili come violazione di dati personali: pertanto, un soggetto destinatario degli obblighi della NIS 2 che si misuri con un incidente, e che sia chiamato a norma dell'art. 25 d.lgsl. 138/24 a valutare se notificarlo o meno all'ACN e segnatamente al CSIRT Italia (il Gruppo nazionale di risposta agli incidenti di sicurezza informatica che dell'ACN è un'articolazione interna), potrebbe trovarsi a monte nella condizione di non dover notificare alcunché al Garante.

Per quanto riguarda l'obbligo di notifica, inoltre, gli obblighi del GDPR assomigliano a quelli della NIS2, in quanto un titolare del trattamento, nel caso di subìta violazione di dati personali, non è tenuto a notificarla sempre e comunque al Garante, poiché la valutazione in tal senso è rimessa al titolare medesimo; similmente è previsto anche dal decreto NIS 2: non tutti gli incidenti devono esser notificati all'ACN.

Per queste ragioni, assumono un importantissimo rilievo le **disposizioni del d.lgsl. 138/24** dedicate alla **cooperazione tra le Autorità**. In particolare, l'art. 14 chiarisce che in caso di incidenti che comportino violazioni di dati personali, tale collaborazione debba avvenire senza reciproche invasioni di campo, tanto da inibire dall'ACN l'adozione di sanzioni in relazione a quello specifico evento laddove siano già state irrogate dal Garante.
Lo stesso art. 14 prevede tuttavia che qualora l'ACN venga a conoscenza di una **violazione degli obblighi di notifica** da parte di un soggetto essenziale o importante che possa comportare una violazione dei dati personali, la quale dovrebbe essere notificata ai sensi dell'articolo 33 del GDPR, **ne informa senza indebito ritardo il Garante.**

Ciò potrebbe comportare che un titolare del trattamento anche soggetto NIS che abbia scelto scientemente di non notificare un breach al Garante e di notificarlo invece all'ACN, potrebbe trovarsi nella situazione di vedersi segnalato al Garante medesimo su impulso dell'ACN stessa.