NUOVA NORMATIVA NETWORK AND INFORMATION SECURITY (NIS2)

Entro il 28 febbraio 2025 tutti i soggetti di cui all'ALLEGATO II (altri settori critici - soggetti importanti) della Direttiva (UE) n. 2022/2555, di seguito anche "**NIS2**", del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione Europea, dovranno registrarsi sulla piattaforma ACN.

Tali soggetti riguardano i seguenti settori:

- servizi postali e di corriere;
- gestione dei rifiuti;
- fabbricazione, produzione e distribuzione di sostanze chimiche (che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui al Regolamento (CE) n. 1907/2006, articolo 3, punti 9), cioè "fabbricante: ogni persona fisica o giuridica stabilita nella Comunità che fabbrica una sostanza all'interno della Comunità;" e 14) quindi "distributore: ogni persona fisica o giuridica stabilita nella Comunità, compreso il rivenditore al dettaglio, che si limita ad immagazzinare e a immettere sul mercato una sostanza, in quanto tale o in quanto componente di un preparato, ai fini della sua vendita a terzi" e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3) del medesimo Regolamento: oggetto a cui sono dati durante la produzione una forma, una superficie o un disegno particolari che ne determinano la funzione in misura maggiore della sua composizione chimica);
- produzione, trasformazione e distribuzione di alimenti (definite all'articolo 3, punto 2), del Regolamento (CE) n. 178/2002 che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione, che definisce «impresa alimentare», ogni soggetto pubblico o privato, con o senza fini di lucro, che svolge una qualsiasi delle attività connesse ad una delle fasi di produzione, trasformazione e distribuzione degli alimenti);
- fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro (soggetti che fabbricano dispositivi medici e di dispositivi definiti all'articolo 2, punto 1), del Regolamento (UE) 2017/745, nel quale si chiarisce che «dispositivo medico» include qualunque strumento, apparecchio, apparecchiatura, *software*, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: — diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie, — diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità, — studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico, — fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi; si considerano dispositivi medici anche i seguenti prodotti: — dispositivi per il controllo del concepimento o il supporto al concepimento, — i prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi);
- fabbricazione di computer e prodotti di elettronica e ottica (26.1 Fabbricazione di componenti elettronici e schede elettroniche, 26.11 Fabbricazione di componenti elettronici, 26.12 Fabbricazione di schede elettroniche integrate, 26.2 Fabbricazione di computer e unità periferiche, 26.20 Fabbricazione di computer e unità periferiche, 26.3 Fabbricazione di apparecchiature per le comunicazioni, 26.30 Fabbricazione di apparecchiature per le comunicazioni, 26.4 Fabbricazione di prodotti di elettronica di consumo, 26.40 Fabbricazione di prodotti di elettronica di consumo, 26.5 Fabbricazione di strumenti e apparecchi di misurazione, prova e navigazione; orologi, 26.51 Fabbricazione di strumenti e apparecchi di misurazione, prova e navigazione, 26.52 Fabbricazione di orologi, 26.6 Fabbricazione di strumenti per irradiazione, apparecchiature elettromedicali ed elettroterapeutiche, 26.60 Fabbricazione di strumenti per irradiazione,

apparecchiature elettromedicali ed elettroterapeutiche, 26.7 Fabbricazione di strumenti ottici e attrezzature fotografiche, 26.70 Fabbricazione di strumenti ottici e attrezzature fotografiche, 26.8 Fabbricazione di supporti ottici e magnetici, 26.80 Fabbricazione di supporti ottici e magnetici);
- fabbricazione di apparecchiature elettriche (27.1 Fabbricazione di motori, generatori e trasformatori elettrici e di apparecchiature per la distribuzione e il controllo dell'elettricità, 27.11 Fabbricazione di motori, generatori e trasformatori elettrici, 27.12 Fabbricazione di apparecchiature per la distribuzione e il controllo dell'elettricità, 27.2 Fabbricazione di batterie e accumulatori, 27.20 Fabbricazione di batterie e accumulatori, 27.3 Fabbricazione di cablaggi e apparecchiature di cablaggio, 27.31 Fabbricazione di cavi a fibre ottiche, 27.32 Fabbricazione di altri fili e cavi elettronici ed elettrici, 27.33 Fabbricazione di attrezzature per cablaggio, 27.4 Fabbricazione di apparecchiature per illuminazione, 27.40 Fabbricazione di apparecchiature per illuminazione, 27.5 Fabbricazione di apparecchi per uso domestico, 27.51 Fabbricazione di elettrodomestici, 27.52 Fabbricazione di apparecchi per uso domestico non elettrici, 27.9 Fabbricazione di altre apparecchiature elettriche, 27.90 Fabbricazione di altre apparecchiature elettriche);
- fabbricazione di macchinari e apparecchiature n.c.a. (28.1 Fabbricazione di macchine di impiego generale 28.11 Fabbricazione di motori e turbine, esclusi i motori per aeromobili, veicoli e motocicli, 28.12 Fabbricazione di apparecchiature fluidodinamiche, 28.13 Fabbricazione di altre pompe e compressori, 28.14 Fabbricazione di altri rubinetti e valvole, 28.15 Fabbricazione di cuscinetti, ingranaggi e organi di trasmissione, 28.2 Fabbricazione di altre macchine di impiego generale, 28.21 Fabbricazione di forni, caldaie per il riscaldamento centrale e bruciatori per caldaie, 28.22 Fabbricazione di apparecchi di sollevamento e movimentazione, 28.23 Fabbricazione di macchine e attrezzature per ufficio (esclusi computer e unità periferiche), 28.24 Fabbricazione di utensili portatili a motore, 28.25 Fabbricazione di attrezzature di uso non domestico per la refrigerazione e la ventilazione, 28.29 Fabbricazione di altre macchine di impiego generale n.c.a., 28.3 Fabbricazione di macchine per l'agricoltura e la silvicoltura, 28.30 Fabbricazione di macchine per l'agricoltura e la silvicoltura, 28.4 Fabbricazione di macchine per la formatura dei metalli e di altre macchine utensili, 28.41 Fabbricazione di macchine per la formatura dei metalli, 28.49 Fabbricazione di altre macchine utensili, 28.9 Fabbricazione di altre macchine per impieghi speciali, 28.91 Fabbricazione di macchine per la metallurgia, 28.92 Fabbricazione di macchine da miniera, cava e cantiere, 28.93 Fabbricazione di macchine per l'industria alimentare, delle bevande e del tabacco, 28.94 Fabbricazione di macchine per le industrie tessili, dell'abbigliamento e del cuoio, 28.95 Fabbricazione di macchine per l'industria della carta e del cartone, 28.96 Fabbricazione di macchine per l'industria delle materie plastiche e della gomma, 28.99 Fabbricazione di altre macchine per impieghi speciali n.c.a.);
- fabbricazione di autoveicoli, rimorchi e semirimorchi;
- fabbricazione di altri mezzi di trasporto;
- fornitori di servizi digitali (fornitori di mercati on line, fornitori di motori di ricerca on line, fornitori di piattaforme di social network, fornitori di servizi di registrazione dei nomi di dominio); e, infine
- ricerca (organizzazioni di ricerca).

La NIS2 aggiorna le norme dell'UE in materia di *cybersicurezza* introdotte nel 2016 modernizzando e uniformando il quadro giuridico esistente. La nuova normativa NIS2 mira a garantire un aumento del livello di sicurezza cibernetica comune, grazie all'armonizzazione delle norme applicabili ai diversi operatori nei diversi Stati membri e al rafforzamento dei livelli *standard* di sicurezza rispetto a quelli previsti dalla disciplina vigente.

Principali elementi della nuova normativa NIS2

1. l'estensione degli ambiti di applicazione rispetto alla precedente normativa NIS. La nuova normativa riguarda, in particolare:
    - oltre 80 tipologie di soggetto;
    - l'intera infrastruttura ICT del soggetto (originariamente solo reti e sistemi serventi i servizi essenziali);

2. l'identificazione dei soggetti, distinti tra essenziali e importanti:
    - prevede un meccanismo di identificazione automatica sulla base di criteri oggettivi, includendo nell'ambito di applicazione tutti i soggetti riconducibili alle specifiche tipologie individuate dalla normativa che sono ritenute medie o grandi imprese (micro e piccole imprese, salvo eccezioni, sono fuori ambito), infatti, le società in perimetro NIS2 sono, ai sensi dell'art. 2 par. 1, quelle qualificate come medie imprese o quelle che superano i massimali delle medie imprese (la Raccomandazione 2003/361/CE, chiarisce quali imprese si qualifichino come medie, piccole e micro: **media impresa**: occupa meno di 250 persone, e realizza un fatturato annuo che non supera i 50 milioni di euro oppure il totale di bilancio annuo non supera i 43 milioni di euro; **piccola impresa**: occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di euro; **microimpresa**: occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di euro), anche se va specificato che all'articolo 2 punti 2), 3) e 4) vengono specificati i soggetti a cui la Direttiva si applica, indipendentemente dalle loro dimensioni qualora: a) i servizi siano forniti da fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico o prestatore di servizi di fiducia, registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio, b) il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali, c) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica, d) una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero, e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro, f) il soggetto è un ente della pubblica amministrazione dell'amministrazione centrale quale definito da uno Stato membro conformemente al diritto nazionale o a livello regionale quale definito da uno Stato membro conformemente al diritto nazionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche; inoltre la Direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, identificati come soggetti critici ai sensi della Direttiva CER (UE) 2022/2557 o ai soggetti che forniscono servizi di registrazione dei nomi di dominio;
    - può anche essere esercitata dall'Autorità nazionale competente NIS, su proposta delle Autorità di settore competenti, per inserire nell'ambito di applicazione ulteriori soggetti;

3. il rafforzamento degli obblighi con:
    - l'obbligo di implementare misure di sicurezza in relazione ad almeno 10 ambiti, con un approccio multirischio e proporzionale rispetto al rischio posto al sistema informativo e di rete;
    - un processo di notifica degli incidenti più articolato;
    - un rafforzamento dei poteri di esecuzione, ispettivi e sanzionatori. In particolare, le sanzioni si allineano a quanto previsto dal GDPR;
4. l'introduzione di nuovi strumenti, quali:
    - la divulgazione coordinata delle vulnerabilità (CVD);
    - la gestione delle crisi, specie a carattere transfrontaliero, con l'istituzione del *Cyber crisis liaison organisation network (CyCLONe)* e dell'Autorità nazionale competente per la gestione delle crisi informatiche.

I principali obblighi previsti dal decreto

- la registrazione e l'aggiornamento delle informazioni (articolo 7);
- gli organi di amministrazione e direttivi (articolo 23);
- gli obblighi in materia di misure di sicurezza informatica (articolo 24);
- gli obblighi in materia di notifica di incidente (articolo 25);
- per alcune tipologie di soggetti, gli obblighi in materia di banca dei dati di registrazione dei nomi di dominio (articolo 29);
- la categorizzazione delle attività e dei servizi (articolo 30).

Registrazione

Come detto sopra, entro il 28 febbraio 2025 i soggetti sopra elencati devono manifestarsi all'Autorità nazionale competente NIS registrandosi sulla piattaforma digitale che è resa disponibile da ACN.
Tale adempimento è funzionale a consentire ad ACN di censire i soggetti operanti nei settori vigilati, anche al fine di fornire loro supporto in fase di implementazione degli obblighi, attraverso le articolate attività di monitoraggio e ausilio nel loro percorso condiviso di crescita.
La mancata registrazione è una violazione assistita da una sanzione amministrativa pecuniaria con un importo fino al 0.1% del fatturato annuo su scala mondiale del soggetto.
A valle della fase di registrazione, nel mese di aprile 2025, i soggetti che si sono registrati riceveranno una comunicazione per confermare, o meno, il loro l'inserimento nell'elenco dei soggetti NIS.

Ulteriori Principali scadenze previste

- Entro metà maggio 2025, trasmissione e aggiornamento, tempestivo (comunque non oltre 14 giorni dalla modifica) delle informazioni dei soggetti NIS (articolo 7, commi 4, 5 e 7).
- Entro gennaio 2026 (entro 9 mesi dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS), adempimento agli obblighi di base in materia di notifica di incidente.
- Entro ottobre 2026 (entro 18 mesi dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS), adempimento agli obblighi di base in materia di sicurezza informatica.

Non esitate a contattarci per qualsiasi ulteriore chiarimento si rendesse necessario.