Sicurezza informatica
Decreto legislativo 138/2024 che recepisce la Direttiva NIS2
Quali operatori riguarda e cosa prevede

FAI INFORMA 198/2024 – NORME AUTOTRASPORTO

La Fai di Torino informa che è stato pubblicato sulla Gazzetta ufficiale Serie generale n. 230 del 01-10-2024 il decreto legislativo 4 settembre 2024, n. 138 "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148" (direttiva NIS 2).
Il d.lgs. in oggetto stabilisce misure volte a garantire un livello elevato di sicurezza informatica e prevede una serie di obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente che si applicano, per quanto di interesse del Sistema, agli operatori dei settori digitale, energia, ambiente e trasporti.

Sono escluse dal recepimento della NIS 2, ad eccezione di specifici casi, le piccole imprese.

Le disposizioni del presente decreto si applicano a decorrere dal 16 ottobre 2024.

Di seguito riportiamo una disamina del provvedimento a cura della Confcommercio. Con riserva di tornare sull'argomento con ulteriori e più specifici approfondimenti.

Soggetti a cui si applica il d.lgs. 138/2024

In base al comma 1 dell'articolo 3 (*Ambito di applicazione*) e agli allegati I (Settori ad alta criticità) e II (Altri settori critici), da esso richiamati, rientrano nell'ambito di applicazione del presente decreto, per quanto di interesse del Sistema, le tipologie di soggetti sotto riportate.
Quelle indicate nell'allegato I (Settori ad alta criticità) sono le seguenti:

- Per il settore **Energia**, le seguenti tipologie di soggetti: imprese elettriche (ovvero che svolgono servizi di generazione, trasmissione, distribuzione, aggregazione, gestione della domanda, stoccaggio, fornitura o acquisto di energia elettrica, che sono responsabili per i compiti commerciali, tecnici o di manutenzione legati a queste funzioni); gestori di rete elettriche e gas, produttori di energia; gestori del mercato elettrico, soggetti operanti nel mercato (aggregatori e gestori della domanda di energia), gestori delle reti di teleriscaldamento, gestori di oleodotti e di impianti di raffinazione, produzione e trattamento, trasporto, deposito e stoccaggio di petrolio; gestori di impianti di raffinazione e trattamento di gas, stoccaggio di gas e di GNL, imprese di gas naturale (ovvero che svolgono funzioni di: produzione, trasporto, distribuzione, fornitura, acquisto o stoccaggio di gas naturale, compresa la rigassificazione di GNL e che sono responsabili per i compiti commerciali, tecnici o di manutenzione legati a queste funzioni); gestori di impianti di produzione, trasporto, e stoccaggio di idrogeno.
- Per il settore trasporti, sottosettore **trasporto aereo**, le seguenti tipologie di soggetti:
    - vettori aerei, – imprese di trasporto aereo titolari di licenza di esercizio valida o documento equivalente (ex art. 3, comma 4, Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio) utilizzati a fini commerciali;
    - gestori aeroportuali – soggetti ai quali le disposizioni legislative, regolamentari o contrattuali affidano, insieme con altre attività o in via esclusiva, il compito di amministrare e di gestire le infrastrutture aeroportuali o della rete aeroportuale e di coordinare e di controllare le attività dei vari operatori presenti negli aeroporti e nella rete aeroportuale di interesse (ex art. 2, punto 2) Dir.2009/12/CE);
    - aeroporti – terreni appositamente predisposti per l'atterraggio, il decollo e le manovre di aeromobili, inclusi gli impianti annessi per le esigenze del traffico e per il servizio degli aeromobili nonché gli impianti necessari per fornire assistenza ai servizi aerei commerciali (ex art. 2, punto 1) Dir.2009/12/CE);
    - soggetti che gestiscono impianti annessi situati in aeroporti;
    - operatori attivi nel controllo della gestione del traffico che forniscono servizi di controllo del traffico aereo (ex art 2, primo paragrafo n. 1, Regolamento (UE) n. 549/2004 del Parlamento europeo e del Consiglio).

- Per il settore trasporti, sottosettore **trasporto ferroviario**, le seguenti tipologie di soggetti:
    - gestori dell'infrastruttura ferroviaria – organismi o imprese responsabili dell'esercizio, della manutenzione e del rinnovo dell'infrastruttura ferroviaria di una rete nonché della partecipazione al suo sviluppo come stabilito dallo Stato

nell'ambito della sua politica generale sullo sviluppo e sul finanziamento dell'infrastruttura (ex art 3, punto 2) Dir.2012/34/UE);

- imprese ferroviarie – imprese pubbliche o private titolari di una licenza, la cui attività principale consiste nella prestazione di servizi per il trasporto per ferrovia sia di merci sia di persone e che garantiscono obbligatoriamente la trazione (ex art 3, punto 2) Dir.2012/34/UE);
- operatori di impianti di servizio – entità pubbliche o private responsabili della gestione di uno o più impianti di servizio o della prestazione di uno o più servizi alle imprese ferroviarie (ex art 3, punto 12) Dir.2012/34/UE).

- Per il settore trasporti, sottosettore **trasporto per vie d'acqua**, le seguenti tipologie di soggetti:
  - compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci (disciplinata nell'allegato I Regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio), escluse le singole navi gestite da tali compagnie;
  - organi di gestione dei porti – aree terrestri e marittime, comprendenti impianti ed attrezzature intese ad agevolare le operazioni commerciali di trasporto marittimo (ex art.3, punto 1) della Dir.2005/65/CE), compresi i relativi impianti portuali (ex art. 2, punto 11) Reg. (CE) n. 725/2004) e soggetti che gestiscono opere e attrezzature all'interno di porti;
  - gestori di servizi di assistenza al traffico marittimo – servizi per la sicurezza della navigazione, l'efficienza del traffico marittimo e la tutela dell'ambiente, in grado di interagire con le navi che transitano nell'area coperta dal Vessel Traffic Service (ex art. 3, lettera o) Dir. 2002/59/CE).
- Per il settore trasporti, sottosettore **trasporto su strada**, le seguenti tipologie di soggetti:
  - autorità stradali – qualsiasi autorità pubblica responsabile della pianificazione, del controllo o della gestione delle strade che rientrano nella sua competenza territoriale (ex art 2, Regolamento delegato (UE) 2015/962), esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione dei sistemi di trasporto intelligente costituiscono soltanto una parte non essenziale della loro attività generale;
  - gestori di sistemi di trasporto intelligenti o ITS (*Intelligent Transport Systems*) – sistemi in cui sono applicate tecnologie dell'informazione e della comunicazione, nel settore del trasporto stradale, infrastrutture, veicoli e utenti compresi, e nella gestione del traffico e della mobilità nonché per interfacce con altri modi di trasporto (art.4, punto 1) Dir. 2010/40/UE).

- Per il settore **acqua potabile** si ritengono soggetti critici i fornitori e distributori di acque destinate al consumo umano ma sono esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni.
- Per il settore **acque reflue** si ritengono soggetti critici le imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali, escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale.
- Per il settore i**nfrastrutture digitali**: fornitori di punti di interscambio internet; fornitori di servizi di sistema dei nomi di dominio (*domain name system* – DNS), esclusi gli operatori dei server dei nomi radice; gestori di registri dei nomi di dominio di primo livello (*top level domain* – TLD); fornitori di servizi di cloud computing; fornitori di servizi di data center; fornitori di reti di distribuzione dei contenuti (*content delivery network*); prestatori di servizi fiduciari; fornitori di reti pubbliche di comunicazione elettronica; fornitori di servizi di comunicazione elettronica accessibili al pubblico.
- Per il settore **gestione dei servizi TIC** (*business-to-business*): fornitori di servizi gestiti; fornitori di servizi di sicurezza gestiti.

Le altre tipologie di soggetti indicate nell'allegato II (altri settori critici) che rientrano nell'ambito di applicazione del presente decreto sono:

- Per il settore **servizi postali e di corriere**: Fornitori di servizi postali quali definiti all'articolo 2, punto 1 bis), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere.
- Per il settore **gestione dei rifiuti**: le imprese che si occupano della gestione dei rifiuti che effettuano operazioni di raccolta, trasporto, recupero e smaltimento di rifiuti, compresi i commercianti e gli intermediari, escluse quelle per cui la gestione dei rifiuti non è la principale attività economica.
- Per il settore **produzione, trasformazione e distribuzione di alimenti:** Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglioche si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione.
- Per il settore **fornitori di servizi digitali**: fornitori di mercati online; fornitori di motori di ricerca online; fornitori di piattaforme di social network; fornitori di servizi di registrazione dei nomi di dominio.

Esclusione delle piccole imprese dall'applicazione del d.lgs 138/2024, salvo eccezioni

Il comma 2 dell'articolo 3 (Ambito di applicazione) dispone che, quanto previsto nel decreto, **si applica ai soggetti delle tipologie di cui all'allegato I (Settori ad alta criticità) e II (Altri settori**

critici), che superano i massimali per le piccole imprese ai sensi dell'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE.

In base a tale raccomandazione è definita 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.

Il comma 4 del medesimo articolo 3 dispone che: per determinare se un soggetto è da considerarsi una media o grande impresa, si applica l'articolo 6, paragrafo 2, dell'allegato della raccomandazione 2003/361/CE, salvo che ciò non sia proporzionato, tenuto anche conto dell'indipendenza del soggetto dalle sue imprese collegate in termini di sistemi informativi e di rete che utilizza e in termini di servizi che fornisce.

Il citato articolo 6, paragrafo 2, prevede:

Per le imprese associate o collegate, i dati, inclusi quelli relativi agli effettivi, sono determinati sulla base dei conti e di altri dati dell'impresa oppure, se disponibili, sulla base dei conti consolidati dell'impresa o di conti consolidati in cui l'impresa è ripresa tramite consolidamento.

Sono, però, previste eccezioni all'esclusione delle piccole imprese dall'applicazione di quanto previsto dal d.lgs. 138/2024. In base ai commi 5 e 9 dell'articolo 3, infatti, **il decreto si applica, indipendentemente dalle loro dimensioni:**

- ai soggetti che sono identificati come soggetti critici ai sensi del decreto legislativo che recepisce la direttiva (UE) 2022/2557;
- ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico;
- ai prestatori di servizi fiduciari;
- ai gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;
- ai fornitori di servizi di registrazione dei nomi di dominio;
- ai soggetti identificati prima della data di entrata in vigore del presente decreto come operatore di servizi essenziali ai sensi del decreto legislativo 18 maggio 2018, n. 65 (cd. "decreto legislativo NIS");
- qualora il soggetto sia l'unico fornitore nazionale di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
- qualora una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
- qualora 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;
- qualora il soggetto sia critico in ragione della sua particolare importanza a livello nazionale o regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nel territorio dello Stato;

- qualora il soggetto sia considerato critico ai sensi del presente decreto quale elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti.

I soggetti di cui agli ultimi 6 punti dell'elenco di cui sopra sono individuati dall'Autorità nazionale competente NIS e questa notifica a tali soggetti la loro individuazione.

Il comma 10 dell'articolo 3, infine, dispone che il decreto **si applica, indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri:**

- 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;
- detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;
- effettua operazioni di sicurezza informatica del soggetto importante o essenziale;
- fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

Suddivisione in soggetti essenziali e soggetti importanti

Con riferimento alle imprese sopra indicate, la normativa prevede una loro suddivisione in soggetti essenziali e soggetti importanti in base alle dimensioni e servizi svolti. Nello specifico, in base a quanto indicato all'articolo 6, sono considerati essenziali:

- i soggetti di cui all'allegato I (Settori ad alta criticità) che superano i massimali per le medie imprese. Si tratta, quindi, di imprese che occupano 250 o più persone, il cui fatturato annuo supera i 50 milioni di EUR oppure il cui totale di bilancio annuo supera i 43 milioni di EUR;
- indipendentemente dalle loro dimensioni, i soggetti identificati come soggetti critici ai sensi del decreto legislativo che recepisce la direttiva (UE) 2022/2557;
- i fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di comunicazione elettronica accessibili al pubblico di cui all'articolo 3, comma 5, che si considerano medie imprese;
- indipendentemente dalle loro dimensioni, i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio di cui all'articolo 3, comma 5.

Fermo restando quanto sopra, **l'Autorità nazionale competente NIS individua i soggetti di cui all'articolo 3, commi 9 e 10, che, indipendentemente dalle loro dimensioni, sono considerati essenziali.**

Ai fini del presente decreto sono considerati soggetti importanti i soggetti di cui all'articolo 3 che non sono considerati essenziali ai sensi dei sopra riportati commi dell'articolo 6.

Passaggi e tempi per l'identificazione dei soggetti interessati dalla NIS 2

Come indicato al comma 1 dell'articolo 7 (*Identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti*) **dal 1° gennaio al 28 febbraio di ogni anno successivo alla data di entrata in vigore del presente decreto, i soggetti di cui all'articolo 3, si registrano o aggiornano la propria registrazione sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS.** Tali soggetti forniscono o aggiornano almeno le informazioni seguenti:

1. a) la ragione sociale; b) l'indirizzo e i recapiti aggiornati; c) la designazione di un punto di contatto; d) ove applicabile, i pertinenti settori, sottosettori e tipologie di soggetto di cui agli allegati I e II.

Entro il 31 marzo di ogni anno successivo alla data di entrata in vigore del presente decreto, come disposto al comma 2 dell'articolo 7, **l'Autorità nazionale competente NIS, redige l'elenco dei soggetti essenziali e dei soggetti importanti.**

Sarà, pertanto, necessario attendere ancora alcuni mesi per avere una precisa identificazione dei soggetti che saranno chiamati ad attuare le disposizioni della Direttiva NIS 2.

Il comma 3 dell'articolo 7 prevede, tramite la piattaforma digitale di cui al comma 1, **l'Autorità nazionale competente NIS comunica ai soggetti registrati** di cui al comma 2: a) **l'inserimento nell'elenco dei soggetti essenziali o importanti**; b) la permanenza nell'elenco dei soggetti essenziali o importanti; c) l'espunzione dall'elenco dei soggetti.

Il comma 4 dispone, **dal 15 aprile al 31 maggio** di ogni anno successivo alla data di entrata in vigore del presente decreto, tramite la piattaforma digitale di cui al comma 1, **i soggetti che hanno ricevuto la comunicazione** di cui al comma 3, lettere a) e b), **forniscono o aggiornano almeno le informazioni seguenti:** a) lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso o nella disponibilità del soggetto; b) ove applicabile, l'elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione del presente decreto; c) i responsabili di cui all'articolo 38, comma 5, indicando il ruolo presso il soggetto e i loro recapiti aggiornati; d) un sostituto del punto di contatto di cui al comma 1, lettera c) dell'articolo 7, indicando il ruolo presso il soggetto e i recapiti aggiornati.

Il comma 5 dell'articolo 7 dispone che 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, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, i fornitori di motori di ricerca online e i fornitori di piattaforme di social network, forniscano all'Autorità nazionale competente NIS,

secondo le modalità di cui al comma 4, anche: a) l'indirizzo della sede principale e delle altre sedi del soggetto nell'Unione europea; b) se non è stabilito nell'Unione europea, l'indirizzo della sede del suo rappresentante ai sensi dell'articolo 5, comma 3, unitamente ai dati di contatto aggiornati.

Il comma 7 dell'articolo 7 dispone che i soggetti che hanno ricevuto la comunicazione di cui al comma 3, lettere a) e b), **notificano all'Autorità nazionale competente NIS, tramite la piattaforma digitale di cui al comma 1, qualsiasi modifica delle informazioni trasmesse** ai sensi del presente articolo tempestivamente e, in ogni caso, entro quattordici giorni dalla data della modifica.

Obblighi in materia di gestione dei rischi

L'articolo 24, al comma 1, **impone ai soggetti essenziali e importanti di adottare misure tecniche,** operative e organizzative 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 per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

Tali misure:

a. assicurano un **livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti**, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;

b. sono **proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità**, compreso il loro impatto sociale ed economico.

Il comma 2 dell'articolo 24 dispone che le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono 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 (*Obblighi in materia di notifica di incidente*) e 26 (*Notifica volontaria di informazioni pertinenti*);

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;
h. politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;
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.

Il comma 3 dell'articolo 24 prevede, nel valutare quali misure di cui al comma 2, lettera d), siano adeguate, i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

Il comma 4 dell'articolo 24 prevede, qualora un soggetto rilevi di non essere conforme alle misure di cui al comma 2, esso adotta, senza indebito ritardo, tutte le misure appropriate e proporzionate correttive necessarie.

Obblighi in materia di notifica di incidente
Il comma 1 dell'articolo 25 dispone che i soggetti essenziali e i soggetti importanti **notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi, ossia quello che:**
a. ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
b. ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Il processo di notifica prevede tempistiche serrate. Come indicato al comma 5 dell'articolo 25, ai fini della notifica di cui al comma 1, i soggetti interessati trasmettono al CSIRT Italia:
a. senza ingiustificato ritardo, e comunque **entro 24 ore** da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b. senza ingiustificato ritardo, e comunque **entro 72 ore** da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni della pre-notifica e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
c. su richiesta del CSIRT Italia, una **relazione intermedia** sui pertinenti aggiornamenti della situazione;
d. una **relazione finale entro un mese** dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda: 1) una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto; 2) il tipo di minaccia o la causa originale che ha probabilmente innescato l'incidente; 3) le misure di attenuazione adottate e in corso; 4) ove noto, l'impatto transfrontaliero dell'incidente;
e. in caso di incidente in corso al momento della trasmissione della relazione finale, una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.
In deroga a quanto previsto dal comma 5, lettera b), un **prestatore di servizi fiduciari**, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, provvede alla notifica di cui alla medesima lettera, senza indebito ritardo e comunque **entro 24 ore** da quando sono venuti a conoscenza dell'incidente significativo.

Supporto del CSIRT ai soggetti colpiti da incidente

Il comma 7 dell'articolo 25 prevede che, senza ingiustificato ritardo e ove possibile entro 24 ore dal ricevimento della pre-notifica di cui al comma 5, lettera a), **il CSIRT Italia fornisca una risposta al soggetto notificante e, su richiesta, orientamenti o consulenza sull'attuazione di possibili misure tecniche di mitigazione.** Su richiesta del soggetto notificante, il CSIRT Italia fornisce, poi, ulteriore supporto tecnico.
Compito del CSIRT Italia è anche, ove si sospetti che l'incidente significativo abbia carattere criminale, fornire al soggetto notificante orientamenti sulla segnalazione dell'incidente significativo all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione.

Obbligo di notifica ai destinatari dei servizi.

L'obbligo di notifica per i soggetti essenziali ed importanti va oltre quello rivolto alle autorità e, come riportano i commi 9 e 10 dell'articolo 25, sentito **il CSIRT Italia, se ritenuto opportuno e qualora possibile, i soggetti essenziali e i soggetti importanti comunicano,** senza ingiustificato ritardo, ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi. Se ritenuto opportuno comunicano, inoltre, ai destinatari dei servizi che sono potenzialmente interessati da una minaccia informatica

significativa, **la natura di tale minaccia e le misure o azioni correttive o di mitigazione che questi possono adottare.**

Informazione al pubblico dell'incidente significativo

Come disposto dall'comma 11 dell'articolo 25, l'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di **Autorità nazionale competente NIS e di CSIRT Italia, può informare il pubblico riguardo all'incidente significativo per evitare ulteriori incidenti significativi o per gestire un incidente significativo in corso,** o qualora ritenga che la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico.

Notifica su base volontaria al CSIRT

Oltre l'obbligo di notifica di incidente di cui all'articolo 25, possono essere trasmesse, su base volontaria, notifiche al CSIRT Italia da parte dei: a) soggetti essenziali e soggetti importanti, per quanto riguarda gli incidenti che non hanno un impatto significativo, le minacce informatiche e i quasi-incidenti; b) soggetti diversi da quelli di cui alla lettera a), indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione del presente decreto, per quanto riguarda gli incidenti che hanno un impatto significativo sulla fornitura dei loro servizi, le minacce informatiche e i quasi-incidenti.

Fatte salve le esigenze di indagine, accertamento e perseguimento di reati, la notifica volontaria di cui sopra non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

Certificazioni e specifiche tecniche

Come disposto all'articolo 27 (*Uso di schemi di certificazione della cybersicurezza*) **l'Autorità nazionale competente NIS può imporre ai soggetti essenziali e ai soggetti importanti di utilizzare categorie di prodotti TIC, servizi TIC e processi TIC,** sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati. L'Autorità nazionale competente NIS promuove, altresì, l'utilizzo di servizi fiduciari qualificati da parte dei soggetti essenziali e dei soggetti importanti.

Come disposto all'articolo 28 (*Specifiche tecniche*) l'Autorità nazionale competente NIS, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, **promuove l'uso di specifiche tecniche europee e internazionali relative alla sicurezza dei sistemi informativi e di rete e può redigere e aggiornare un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica.** Tale elenco **non ha carattere vincolante o esaustivo** ed è pubblicato sul sito dell'Agenzia per la cybersicurezza nazionale.

Banca dati di registrazione dei nomi di dominio

Come disposto dall'articolo 29, per contribuire alla sicurezza, alla stabilità e alla resilienza dei sistemi di nomi di dominio, **i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio raccolgono e mantengono dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati.** Tale banca dati contiene le informazioni necessarie per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio presenti, registrati o censiti nel registro dei nomi di dominio di primo livello (*top level domain – TLD*).

I gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio per i domini di primo livello rendono pubblicamente disponibili, senza ingiustificato ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che non sono dati personali. Inoltre, su richiesta motivata dei soggetti legittimati, forniscono l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione europea in materia di protezione dei dati.

I soggetti che gestiscono i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio rispondono senza ingiustificato ritardo e, comunque, entro 72 ore dalla ricezione della richiesta di accesso.

Al fine di evitare una duplicazione della raccolta di dati di registrazione dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio individuano modalità e procedure di collaborazione per la raccolta e il mantenimento dei dati.

Gradualità degli obblighi e linee guida vincolanti

n base all'articolo 31 l'Autorità nazionale competente NIS stabilisce **obblighi proporzionati** tenuto conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità.

Termini, modalità, specifiche e tempi di implementazione degli obblighi potranno quindi differenziarsi in base anche alla tipologia di soggetto tenendo conto del grado di maturità iniziale nell'ambito della sicurezza informatica nonché all'individuazione del soggetto quale essenziale o importante.

L'Autorità nazionale competente NIS può emanare raccomandazioni e **linee guida vincolanti** per l'attuazione degli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente.

Come disposto dall'articolo 32 (Previsioni settoriali specifiche) tenuto conto degli impatti sociali e economici di un incidente significativo nella catena di approvvigionamento del settore della pubblica amministrazione, l'Autorità nazionale competente NIS **può imporre specifici obblighi proporzionati e graduali ai soggetti essenziali e ai soggetti importanti che forniscono servizi, anche digitali, alla pubblica amministrazione.**

Ruolo e responsabilità del management

In base all'articolo 23 gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti sono chiamati ad avere un ruolo attivo nella *compliance* alla normativa. Essi, infatti, **approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica** adottate ai sensi dell'articolo 24; **sovrintendono all'implementazione degli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente** di cui al Capo IV e di cui all'articolo 7 (*Identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti*) e sono considerati responsabili delle violazioni di cui al presente decreto. L'inosservanza degli obblighi diretti agli organi di amministrazione e direttivi può, infatti, comportare specifiche sanzioni, riportate nella sezione successiva.

Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti sono **informati tempestivamente degli incidenti e delle notifiche** di cui agli articoli 25 e 26.

Sono, inoltre, come disposto al comma 2 dell'articolo 23, **tenuti a seguire una formazione in materia di sicurezza informatica** e promuovono l'offerta periodica di una formazione coerente anche ai loro dipendenti.

Sanzioni per inosservanza della direttiva NIS 2

Il compito di monitorare la corretta applicazione delle disposizioni della Direttiva NIS 2 e di esercitare i poteri sanzionatori è stato attribuito, come disposto agli articoli da 34 a 38, all'Agenzia per la cybersicurezza quale Autorità competente NIS.

Le sanzioni sono **differenziate in base alla tipologia di soggetto (essenziale o importante) e di violazione.** In particolare, la violazione degli obblighi, previsti dal comma 8 dell'articolo 38 e sotto riportati, è sanzionata, come indicato al comma 9, **per i soggetti essenziali con sanzioni pecuniarie fino a un massimo di euro 10.000.000 o del 2% del totale del fatturato annuo** su scala mondiale per l'esercizio precedente del soggetto mentre, nel caso di **soggetti importanti, le sanzioni sono fino a un massimo di euro 7.000.000 o dell'1,4% del totale del fatturato annuo** su scala mondiale. Sono previsti dei minimi delle sanzioni pari, rispettivamente, a un ventesimo e un trentesimo del massimo edittale.

Le sanzioni di cui sopra sono relative alla violazione dei seguenti obblighi:

- mancata osservanza degli obblighi imposti dall'articolo 23 agli organi di amministrazione e direttivi;
- inosservanza degli obblighi relativi alla gestione del rischio per la sicurezza informatica e alla notifica di incidente di cui agli articoli 24 e 25;
- inottemperanza delle disposizioni adottate dall'Autorità nazionale competente NIS ai sensi dell'articolo 37, commi 3 e 4, e alle relative diffide.

Ai commi 10 e 11 dell'articolo 38 sono previste **sanzioni amministrative pecuniarie per violazioni meno gravi**, sotto riportate che, **per i soggetti essenziali sono fino a un massimo**

dello 0,1% del totale del fatturato annuo su scala mondiale per l'esercizio precedente mentre, **per i soggetti importanti, fino a un massimo dello 0,07% del totale del fatturato.** Rimangono validi i minimi edittali di cui sopra.

Le violazioni sono relative a:

a. mancata registrazione, comunicazione o aggiornamento delle informazioni sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS;

b. inosservanza delle modalità stabilite dall'Autorità nazionale competente NIS per la comunicazione delle informazioni ai sensi dell'articolo 7;

c. mancata comunicazione o aggiornamento dell'elenco delle attività e dei servizi nonché della loro categorizzazione ai sensi dell'articolo 30, comma 1;

d. mancata implementazione o attuazione degli obblighi relativi all'uso di schemi di certificazione, alla banca dei dati di registrazione dei nomi di dominio nonché alle previsioni settoriali specifiche di cui agli articoli 27, 29 e 32;

e. mancata collaborazione con l'Autorità nazionale competente NIS nello svolgimento delle attività e nell'esercizio dei poteri di monitoraggio, vigilanza ed esecuzione di cui al Capo V;

f. mancata collaborazione con il CSIRT Italia.

In caso di reiterazione delle violazioni di cui all'articolo 38, le sanzioni possono essere aumentate fino al triplo.

Infine, come indicato al comma 13 dell'articolo 38, in caso di mancata o tardiva registrazione sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS, di cui all'articolo 7, sono comunque contestate tutte le violazioni previste dai commi 8 e 10 del presente articolo, e si applica la sanzione prevista per la violazione più grave aumentata fino al triplo.

Sono, inoltre, disposte alcune sanzioni accessorie che prevedono, **in caso la diffida** da parte dell'Autorità nazionale competente NIS che richieda l'adempimento di determinate disposizioni (riferimento ai commi 6 e 7 dell'articolo 37) **venga ignorata** dal soggetto che la riceve, è possibile **sospendere temporaneamente**, come disposto dal comma 4 dell'articolo 38, **un certificato o un'autorizzazione relativi a servizi o attività pertinenti svolti dal soggetto essenziale.** Inoltre, nel medesimo caso, come indicato al comma 6 dell'articolo 38, può essere **disposta al management la sanzione della incapacità a svolgere funzioni dirigenziali** all'interno del medesimo soggetto.

Il comma 15 dell'articolo 38 prevede siano individuate modalità di applicazione, nell'ambito del procedimento sanzionatorio, di strumenti deflattivi del contenzioso.

Specifiche in fase di prima applicazione

In base all'articolo 42, in fase di prima applicazione, 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, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, i fornitori di motori di ricerca online e i fornitori di piattaforme di social network, che rientrano nell'ambito di applicazione del presente decreto, **si registrano sulla piattaforma digitale di cui all'articolo 7, comma 1 entro il 17 gennaio 2025.**

Sino al 31 dicembre 2025, il termine per l'adempimento degli obblighi di cui all'articolo 25 (*Obblighi in materia di notifica di incidente*) è **fissato in nove mesi** dalla ricezione della comunicazione di cui all'articolo 7, comma 3, lettere a) e b), che comunica l'inserimento o la permanenza nell'elenco dei soggetti essenziali o importanti, **e il termine per l'adempimento degli obblighi di cui agli articoli 23** (*Organi di amministrazione e direttivi*), **24** (*Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica*) e **29** (*Banca dei dati di registrazione dei nomi di domini*) **è fissato in diciotto mesi** dalla medesima comunicazione.
L'obbligo di cui all'articolo 30, comma 1 – che prevede dal 1° maggio al 30 giugno di ogni anno a partire dalla ricezione della prima comunicazione di cui all'articolo 7, comma 3, lettera a), i soggetti essenziali e i soggetti importanti comunicano e aggiornano, tramite la piattaforma digitale di cui all'articolo 7, comma 1, un 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 –**si applica a partire dal 1° gennaio 2026.**