INSIGHT | 24 marzo 2025

Direttiva NIS 2 e D.Lgs. 138/2024: obblighi in materia di cybersicurezza e profili di compliance

Il **Decreto Legislativo 4 settembre 2024 n. 138**, che traspone la Direttiva (UE) 2022/2555 (Direttiva NIS 2), relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, introduce novità rilevanti, che potrebbero avere dei riflessi in tema di responsabilità amministrativa degli enti, in particolare per quanto riguarda la disciplina del D.Lgs. 231/2001.

L'ambito di applicazione soggettivo

In linea con l'ampliamento del novero dei soggetti obbligati dettato dalla Direttiva NIS 2, l'articolo 3 del D.Lgs. 138/2024 perimetra l'ambito applicativo del Decreto suddividendo gli enti in quattro categorie, meglio dettagliate nei relativi allegati:

- **Allegato I**: soggetti dei **settori ad alta criticità** come energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC e spazio, **purché superino** ***"i massimali per le piccole imprese"*** dettati dall'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE;
- **Allegato II**: soggetti dei **settori critici** come servizi postali e di corriere, gestione dei rifiuti, fabbricazione, produzione e distribuzione di sostanze chimiche, produzione, trasformazione e distribuzione di alimenti, fabbricazione di dispositivi medici, computer, apparecchiature elettriche, macchinari, autoveicoli e altri mezzi di trasporto, fornitori di servizi digitali e organizzazioni di ricerca, **purché superino** ***"i massimali per le piccole imprese"*** dettati dall'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE;
- **Allegato III: pubbliche amministrazioni centrali, regionali e locali, e altri soggetti pubblici** come enti di regolazione, enti produttori di servizi economici, enti a struttura associativa, enti produttori di servizi assistenziali, ricreativi e culturali, enti e istituzioni di ricerca, e istituti zooprofilattici sperimentali;
- **Allegato IV**: ulteriori tipologie di soggetti come fornitori di servizi di trasporto pubblico locale, istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, e società in house, partecipate e a controllo pubblico.

Sono tuttavia individuate altre categorie di soggetti obbligati **a prescindere dai requisiti dimensionali**, come i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, i prestatori di servizi fiduciari, i gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio, i fornitori di servizi di registrazione dei nomi di dominio, o il soggetto che si trovi ad essere l'unico fornitore nazionale di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali.

In ogni caso l'Agenzia per la Cybersicurezza Nazionale (ACN), definita come "*Autorità nazionale competente NIS*" e competente per la supervisione e l'implementazione delle misure di sicurezza

richieste dal Decreto, può individuare **ulteriori soggetti obbligati** nei settori interessati, sempre a prescindere dalle dimensioni.

Nel novero dei soggetti obbligati così identificati, l'articolo 6 del Decreto opera un'ulteriore distinzione tra soggetti **essenziali** (perché superano determinati criteri dimensionali o svolgono determinate attività rilevanti) e soggetti **importanti** (tutti i soggetti rientranti negli Allegati da I a IV, non considerati essenziali), al fine di **graduare gli obblighi gravanti sulle due categorie**, lasciando sempre all'ACN la facoltà di identificare altri soggetti essenziali, indipendentemente dalle loro dimensioni.

Periodicamente, i soggetti rientranti nell'ambito di applicazione del Decreto hanno pertanto l'obbligo di **registrarsi o aggiornare la propria registrazione** sull'apposita piattaforma digitale gestita dall'ACN, proprio al fine di permettere a quest'ultima di redigere l'elenco dei soggetti essenziali e importanti ai sensi della Direttiva NIS 2.

Le modalità di registrazione sono disciplinate dalla determinazione del Direttore generale dell'ACN "*recante termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimenti di designazione dei rappresentanti NIS nell'Unione*".

In particolare, entro il 28 febbraio 2025, i soggetti di cui all'art. 3 devono registrarsi sulla piattaforma ed effettuare l'autovalutazione come soggetto essenziale, importante o fuori ambito.

Entro aprile 2025, invece, l'ACN comunicherà a tutti i soggetti registrati se fanno parte o meno dell'elenco dei soggetti NIS 2.

Obblighi a carico dei soggetti essenziali e dei soggetti importanti

Il capo IV del Decreto stabilisce gli "*obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente*" gravanti sui soggetti essenziali e dei soggetti importanti. In particolare, tali obblighi riguardano, *inter alia*:

- **l'adozione di misure di gestione dei rischi per la sicurezza informatica:** i soggetti essenziali e importanti devono adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza dei sistemi informativi e di rete che utilizzano nelle loro attività o nella fornitura dei loro servizi. Tali misure devono garantire un livello di sicurezza adeguato ai rischi esistenti, tenendo conto delle conoscenze più aggiornate e dello stato dell'arte in materia. Le **misure minime**, elencate dall'articolo 24, devono includere, a titolo esemplificativo, politiche di sicurezza, gestione delle vulnerabilità, controllo degli accessi, sicurezza della *supply chain*, e l'uso della crittografia;
- **la notifica degli incidenti:** i soggetti essenziali e importanti devono notificare senza ingiustificato ritardo al CSIRT Italia (*Computer Security Incident Response Team* istituito presso l'ACN) ogni incidente che abbia un impatto significativo sulla fornitura dei loro servizi;
- **l'uso di schemi di certificazione della cybersicurezza:** l'ACN può imporre ai soggetti essenziali e importanti di utilizzare prodotti, servizi e processi TIC certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza;
- **la comunicazione e l'aggiornamento delle informazioni** sull'apposita piattaforma digitale;
- in capo agli **organi di amministrazione e direttivi**, l'approvazione delle modalità di implementazione delle misure di gestione dei rischi, il monitoraggio dell'implementazione degli obblighi e la formazione in materia di sicurezza informatica;
- in capo ai **gestori di nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio**, la pubblicazione dei dati di registrazione dei nomi di dominio che non sono dati personali e l'accesso a specifici dati di registrazione su richiesta motivata.

La violazione degli obblighi dettati dal Decreto determina la possibile irrogazione di **sanzioni amministrative** da parte dell'ACN, differenziate a seconda della categorizzazione del soggetto come essenziale o importante.

Profili di compliance in relazione al D.Lgs. 231/2001

La disciplina dettata dall'art. 24 Decreto 138/2024 individua le **misure minime di sicurezza informatica** volte a "*proteggere i sistemi informativi e di rete nonché il loro ambiente fisico*

da incidenti", quali:

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;*
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.*"

La mancata adozione delle misure e degli obblighi previsti dal Decreto comporta l'applicazione di **sanzioni amministrative pecuniarie** che sono determinate tenendo conto di diversi criteri, tra cui la gravità e la durata della violazione, eventuali precedenti violazioni, danni causati, intenzionalità o negligenza, misure adottate per prevenire o mitigare il danno, adesione a codici di condotta o meccanismi di certificazione, e il livello di collaborazione con l'Autorità nazionale competente.

Ad esempio, in caso in mancata osservanza degli obblighi relativi alla gestione del rischio per la sicurezza informatica e alla notifica di incidente (articoli 23, 24 e 25), per i soggetti essenziali (escluse le pubbliche amministrazioni), sanzioni fino a 10.000.000 di euro o il 2% del fatturato annuo mondiale dell'esercizio precedente (se superiore), con un minimo di un ventesimo del massimo edittale; per i soggetti importanti (escluse le pubbliche amministrazioni), sanzioni fino a 7.000.000 di euro o l'1,4% del fatturato annuo mondiale dell'esercizio precedente (se superiore), con un minimo di un trentesimo del massimo edittale.

Le misure minime di sicurezza informatica sono dunque presidi a **tutela dei sistemi informatici** delle società, tanto da incidenti fortuiti, quanto da potenziali attacchi informatici.

Il Decreto è dunque focalizzato solo sui reati informatici **subiti** a danno della società, e non su quelli commessi nell'interesse o a vantaggio della stessa: non vi è dunque alcuna menzione del D.Lgs. 231/2001.

Tuttavia, le misure minime previste dal Decreto potrebbero costituire delle linee guida anche per **prevenire la commissione di reati informatici nell'interesse o a vantaggio della società**, evitando la responsabilità dell'ente ai sensi dell'art. 24 *bis* D.Lgs. 231/2001.

Tali misure potrebbero dunque assumere **rilevanza anche ai fini della normativa di cui al D.Lgs. 231/2001**, e dunque nella redazione dei **Modelli di Organizzazione, Gestione e Controllo** di qualsiasi società.

In sede di adozione o aggiornamento del Modello, tutte le società – o quantomeno quelle più esposte al rischio di commissione di reati informatici – potrebbero quindi fare riferimento **proprio alle misure minime identificate dall'art. 24** e degli obblighi stabiliti nel medesimo Decreto per predisporre specifiche procedure di prevenzione dei rischi informatici, come:

- **adozione di procedure di *cybersecurity* e *incident response plan***, compresi piani di gestione delle crisi informatiche, con indicazioni chiare quanto a doveri e responsabilità delle funzioni coinvolte;
- **definizione di procedure per la segnalazione di incidenti informatici** e gestione delle vulnerabilità;
- **implementazione di un sistema di gestione della sicurezza informatica** (**ISMS**) conforme agli standard internazionali, nonché di un sistema di **monitoraggio** e **auditing periodico**;
- **nomina di un responsabile della sicurezza del-**

le informazioni (**CISO**) e creazione di un team interno per la gestione della sicurezza informatica;

- **formazione obbligatoria del personale su sicurezza informatica e protezione dei dati,** con sessioni di aggiornamento periodiche;
- **adozione di misure disciplinari interne** per i dipendenti che non rispettano le politiche di cybersecurity aziendali.

Contatti

Nicolò Pelanda
nicolo.pelanda@lcalex.it

Giulia Marrazza
giulia.marrazza@lcalex.it

Chiara Sarzi Sartori
chiara.sarzi@lcalex.it