DATA CENTER E NIS2: COME GARANTIRE LA SICUREZZA INFORMATICA E LA COMPLIANCE NORMATIVA

1 aprile 2025

AUTORI

Aurora Agostini
Partner

La crescente digitalizzazione delle infrastrutture critiche europee ha portato con sé un aumento esponenziale dei rischi cibernetici, rendendo necessario un quadro normativo più robusto e armonizzato. In questo contesto, la Direttiva NIS2 rappresenta un passo fondamentale nell'evoluzione della strategia europea di cybersicurezza, con significative implicazioni per gli operatori di servizi essenziali e, in particolare, per i gestori di data center.

Il presente contributo analizza l'impatto della Direttiva NIS2 sul settore dei data center in Italia, alla luce del recente recepimento nazionale, delineando il perimetro soggettivo di applicazione, gli obblighi di compliance e le sfide operative che i fornitori di infrastrutture digitali dovranno affrontare nei prossimi mesi.

IL CONTESTO NORMATIVO: LA DIRETTIVA NIS2

La Direttiva (UE) 2022/2555 ("**Direttiva NIS2**"), entrata in vigore il 16 gennaio 2023, ha sostituito la Direttiva NIS1 (2016/1148) con l'obiettivo di rafforzare la resilienza dei sistemi informatici e delle reti degli operatori attivi in settori considerati essenziali o importanti per il funzionamento dell'economia e della società europea.

Il recepimento in Italia è avvenuto con il decreto legislativo n. 138 del 4 settembre 2024, pubblicato in Gazzetta Ufficiale il 1° ottobre 2024 ed entrato in vigore il 16 ottobre 2024 (il "**Decreto NIS2**"). Il decreto amplia significativamente l'ambito soggettivo di applicazione, includendo anche le Pubbliche Amministrazioni locali e introducendo nuovi obblighi in materia di gestione dei rischi, sicurezza della *supply chain*, *business continuity* e *governance* della cybersicurezza.

Dal 1° dicembre 2024, le organizzazioni soggette agli obblighi NIS2 sono tenute a registrarsi presso l'Agenzia per la Cybersicurezza Nazionale (ACN), attraverso un'apposita piattaforma digitale. Il termine ultimo per completare la registrazione era fissato al 28 febbraio 2025; tale obbligo, è bene sottolinearlo, si rinnova di anno in anno, rappresentando non un adempimento una tantum ma un elemento strutturale del sistema di vigilanza.

La NIS2 impone un approccio sistemico e documentato alla gestione del rischio informatico, con l'obbligo di adottare misure tecniche e organizzative proporzionate, e prevede un regime sanzionatorio particolarmente severo, con sanzioni amministrative pecuniarie fino a 10 milioni di euro o al 2% del fatturato annuo globale, a seconda di quale sia l'importo maggiore. Vale la pena evidenziare che tale impianto sanzionatorio riprende la struttura già nota nel contesto del Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati o "**GDPR**"), confermando il progressivo allineamento degli approcci regolatori europei in materia di sicurezza e protezione dei dati.

IMPATTO SUI DATA CENTER: CHI È SOGGETTO ALLA NIS2

I fornitori di *data center*, intesi come soggetti che offrono servizi infrastrutturali per l'elaborazione, l'archiviazione e la trasmissione di dati digitali, rientrano espressamente tra i soggetti destinatari degli obblighi previsti dalla Direttiva NIS2 e dal Decreto NIS2. Più precisamente, essi sono qualificati come "**fornitori di servizi di infrastrutture digitali**" ai sensi dell'articolo 3, comma 1, lettera l), punto 8 del Decreto NIS2, e sono quindi inclusi nell'Allegato I tra le infrastrutture digitali, insieme ai fornitori di servizi *cloud*, ai *registrar* di nomi a dominio e ai gestori di punti di interscambio Internet (IXP).

La normativa distingue tra soggetti **essenziali** e soggetti **importanti**, classificazione fondata su criteri oggettivi come la natura dei servizi offerti, il settore di appartenenza e la dimensione aziendale. Per quanto concerne il criterio dimensionale, l'articolo 4 del Decreto NIS2 stabilisce una esclusione generale per le microimprese e le piccole imprese, così come definite dalla Raccomandazione 2003/361/CE della Commissione (ovvero imprese con meno di 50 dipendenti e un fatturato annuo o un totale di bilancio non superiore a 10 milioni di euro). Tale esclusione, tuttavia, non si applica qualora:

- le entità in questione forniscano servizi a soggetti essenziali o importanti con un ruolo critico nella catena del valore;

- le entità siano designate come gestori di servizi essenziali ai sensi del precedente D.Lgs. 65/2018;

- le entità operino come unici fornitori di servizi in uno Stato membro;

- una potenziale interruzione del servizio potrebbe avere un impatto sulla sicurezza pubblica, sull'incolumità pubblica o sulla salute pubblica;

- una potenziale interruzione del servizio potrebbe comportare rischi sistemici, in particolare nei settori in cui l'interruzione avrebbe un impatto transfrontaliero.

I *data center* sono pertanto da considerarsi, nella maggior parte dei casi, soggetti essenziali, soggetti a obblighi più stringenti in termini di *governance*, sicurezza e notifica, in virtù del loro ruolo critico nell'ecosistema digitale e dell'impatto potenziale di eventuali interruzioni di servizio.

Alla luce di tali criteri, è utile considerare alcune **situazioni-tipo** che aiutano a comprendere come si declina l'applicazione della NIS2 ai diversi modelli di *business* nel settore dei *data center*:

- un fornitore di servizi *cloud* su scala europea o globale, che gestisce infrastrutture in più Stati membri e offre servizi a soggetti pubblici e privati, rientra pienamente tra gli enti essenziali ai sensi della NIS2;

- una società nazionale o interregionale che offre servizi di *colocation*, *housing* o *hosting*, con più di 50 dipendenti o un fatturato annuo superiore a 10 milioni di euro, sarà tenuta ad applicare gli obblighi NIS2 come soggetto essenziale o importante, in base al livello di criticità dei servizi;

- un *data center* regionale di medie dimensioni, che ospita sistemi informativi di enti sanitari, amministrazioni pubbliche locali o infrastrutture energetiche, potrebbe ricadere nell'ambito applicativo della direttiva, anche se non opera su scala nazionale, in virtù della rilevanza funzionale dei servizi offerti.

Ai fini della valutazione, è fondamentale considerare non solo la natura del servizio offerto, ma anche il livello di interconnessione e dipendenza dell'ecosistema in cui il fornitore opera: come ben evidenziato dalla giurisprudenza della Corte di Giustizia dell'UE in materia di servizi digitali (C-434/15), l'elemento qualificante può risiedere non tanto nella dimensione autonoma del servizio, quanto nella sua **integrazione** in catene del valore più ampie. Pertanto, anche soggetti apparentemente secondari, ma integrati in filiere essenziali, possono essere qualificati come soggetti rilevanti ai fini della NIS2, con tutte le conseguenze in termini di obblighi di sicurezza e responsabilità.

OBBLIGHI DI *COMPLIANCE* PER I *DATA CENTER*

Il quadro delineato dalla Direttiva NIS2, come recepito nel Decreto NIS2, impone ai soggetti rientranti nell'ambito di applicazione – inclusi i gestori di *data center* qualificati come enti essenziali o importanti – l'adozione di un set articolato di misure tecnico-organizzative ispirate a un approccio basato sul rischio - "*risk-based approac*h" -, in linea con i principi già noti in ambito GDPR e cybersecurity framework europei.

Tali misure devono essere idonee a garantire un livello di sicurezza adeguato rispetto alla probabilità e gravità dei rischi per la sicurezza delle reti e dei sistemi informativi, anche tenendo conto della specificità dei servizi prestati, dell'interconnessione con altri soggetti della catena del valore e della rilevanza del ruolo infrastrutturale svolto.

Il decreto individua in particolare i seguenti obblighi principali:

- analisi e gestione dei rischi legati alla sicurezza dei sistemi e delle reti, da effettuarsi con cadenza periodica e documentabile;
- misure tecniche e procedurali di prevenzione e mitigazione degli attacchi, tra cui l'adozione di sistemi di segmentazione di rete, crittografia dei dati, autenticazione multifattoriale (MFA) e controllo degli accessi;
- procedure di gestione degli incidenti di sicurezza, con definizione di ruoli e responsabilità, escalation interne e registrazione degli eventi;
- piani di continuità operativa (BCP) e strategie di *disaster recovery* (DRP), volti a garantire la disponibilità e la resilienza dei servizi critici;
- obblighi di notifica degli incidenti significativi, da trasmettere entro 24 ore al CSIRT Italia e all'Agenzia per la Cybersicurezza Nazionale ("ACN") secondo le modalità stabilite dal Regolamento di esecuzione (UE) 2024/2690, già in vigore. Tale regolamento prevede: (i) una pre-notifica entro 24 ore dall'individuazione dell'incidente, (ii) una notifica completa entro 72 ore, e (iii) una relazione finale da trasmettere entro un mese.

L'effettiva *compliance* implica la definizione di una governance chiara in materia di cybersicurezza, l'attribuzione di responsabilità interne, l'aggiornamento dei contratti e dei flussi documentali e, non da ultimo, la capacità di dimostrare la diligenza organizzativa in caso di ispezioni da parte dell'ACN o contenziosi derivanti da violazioni o disservizi. Per i *data center* che operano in contesti regolamentati (es. finanziari o sanitari), è essenziale l'adozione di un approccio integrato che consideri anche gli ulteriori requisiti settoriali, come quelli previsti dal Regolamento (UE) 2022/2554 ("DORA") per il settore finanziario.

LA FIGURA DEL RESPONSABILE DELLA CYBERSICUREZZA E I POTERI DELL'ACN

Tra gli obblighi organizzativi introdotti dal Decreto NIS2, figura la designazione di un **responsabile per la sicurezza delle reti e dei sistemi informativi**, prevista dall'articolo 21, comma 2, lettera i) per i soggetti essenziali e dall'articolo 22, comma 2, lettera h) per i soggetti importanti. Tale figura, che in analogia con il DPO (*Data Protection Officer*) previsto dal GDPR deve disporre di competenze tecniche adeguate, autonomia operativa e risorse proporzionate alla dimensione e al livello di esposizione al rischio dell'organizzazione, può essere rappresentata da un professionista interno o esterno all'ente, purché siano garantite competenza, indipendenza e assenza di conflitti di interesse.

Questa figura – talvolta identificata anche come *Chief Information Security Officer* (CISO) o *Security Officer* – svolge una **funzione di coordinamento interno** e rappresenta il **punto di contatto verso l'esterno**, in particolare nei confronti delle autorità competenti per la gestione degli incidenti e per gli obblighi di notifica. Sebbene il Decreto NIS2 non prescriva requisiti formali di certificazione per questa figura, è ragionevole prevedere, in analogia con quanto accaduto per il DPO, lo sviluppo di standard professionali e percorsi formativi riconosciuti a livello nazionale, anche alla luce delle Linee Guida che l'ACN dovrebbe emanare nei prossimi mesi.

L'autorità nazionale competente per l'attuazione e il controllo della disciplina è l'ACN, alla quale il Decreto NIS2 affida un ampio spettro di poteri, tra cui:

- poteri di sorveglianza e ispezione;
- la valutazione della conformità degli enti soggetti agli obblighi NIS2;
- la gestione operativa del sistema di notifiche (in collaborazione con il CSIRT Italia);
- la possibilità di emettere raccomandazioni, prescrizioni vincolanti e misure correttive;
- l'irrogazione di sanzioni amministrative pecuniarie, che possono raggiungere fino a 10 milioni di euro o al 2% del fatturato mondiale annuo, se superiore.

In presenza di violazioni gravi o sistemiche, l'ACN può anche imporre misure specifiche, tra cui la sospensione temporanea dell'attività o la revoca dell'autorizzazione in caso di enti soggetti a regime concessorio o autorizzatorio. È significativo notare che, nel caso dei *data center* che forniscono servizi alla Pubblica Amministrazione, le violazioni potrebbero comportare anche l'esclusione dagli

appalti pubblici, in linea con quanto previsto dall'articolo 80 del D.Lgs. 36/2023 (Codice dei Contratti Pubblici).

PRIME INDICAZIONI OPERATIVE E PROSPETTIVE: DALLA *COMPLIANCE* ALLA *CYBER RESILIENCE*

In attesa di un consolidamento della prassi applicativa e dell'elaborazione giurisprudenziale – al momento ancora assente a livello nazionale – iniziano a emergere, sia in ambito dottrinale che nelle prime linee guida europee, alcune ***best practice*** operative di riferimento per i fornitori di infrastrutture digitali.

In primo luogo, il principio di *accountability* – mutuato dall'esperienza del GDPR e ripreso anche nel Regolamento di esecuzione (UE) 2024/2690 – impone agli operatori una documentazione rigorosa e strutturata delle misure di sicurezza adottate, non solo in chiave preventiva ma anche in funzione probatoria. L'adeguatezza delle misure va valutata in base al rischio, con un aggiornamento continuo rispetto all'evoluzione della minaccia e al contesto operativo di riferimento, secondo quanto già delineato dall'ENISA nel documento "NIS Investments" (novembre 2023) e dalle raccomandazioni preliminari dell'ACN sulla gestione del rischio cyber (marzo 2025).

Il quadro normativo derivante dalla NIS2 si inserisce in un contesto più ampio di riforme europee in materia di sicurezza digitale, con significative sinergie con altri framework normativi. In particolare, i data center che operano in ambito finanziario dovranno considerare anche gli obblighi derivanti dal DORA sui servizi ICT nel settore finanziario, mentre quelli che trattano dati personali dovranno integrare le misure NIS2 con quelle già adottate in ottemperanza all'articolo 32 del GDPR. I gestori di infrastrutture critiche dovranno inoltre considerare gli adempimenti derivanti dalla Direttiva (UE) 2022/2557 sulla resilienza dei soggetti critici (CER), recepita in Italia con il D.Lgs. 133/2024.

In quest'ottica, i fornitori di *data center* sono chiamati a rivedere in profondità:

- i contratti e gli SLA con i clienti, per includere esplicitamente gli obblighi derivanti dalla NIS2 (es. notifica incidenti, audit, responsabilità condivise);
- le policy interne, per formalizzare ruoli, responsabilità e processi di risposta agli incidenti;

- le procedure di due diligence sulla supply chain, in quanto la sicurezza dei fornitori rappresenta oggi un elemento centrale nella valutazione di conformità.

La NIS2 segna dunque un cambio di paradigma: la cybersicurezza non è più un adempimento meramente tecnico, ma diventa un *asset* strategico da integrare nella *governance* complessiva dell'organizzazione, e i *data center*, in quanto infrastrutture critiche abilitanti per la transizione digitale, devono assumere un ruolo proattivo e centrale nel garantire la resilienza sistemica.

In termini di governance, è altresì auspicabile un maggiore coinvolgimento degli organi amministrativi, che – in linea con quanto già avviene in settori regolamentati come quello finanziario – dovrebbero ricevere periodicamente reportistica sulla postura di sicurezza, approvare le strategie di mitigazione del rischio e assicurare risorse adeguate. Ma solo attraverso un lavoro congiunto e strutturato tra funzioni legali, compliance e IT security la conformità normativa potrà trasformarsi in vantaggio competitivo, rafforzando la fiducia degli stakeholder, l'affidabilità del servizio e la sostenibilità del modello di business in un contesto sempre più caratterizzato dalla centralità della sicurezza come fattore abilitante dell'innovazione digitale.

DATA CENTER FOCUS TEAM

Aurora Agostini

Partner

Elmira Shahbazi

Partner

Fabio Luongo

Partner

Giuseppe Di Vita

Counsel

Gabriel Zurlo Sconosciuto

Associate

Questo documento è fornito a scopo informativo generale e non intende fornire consulenza legale sui temi trattati. I destinatari di questo documento non possono fare affidamento sui suoi contenuti. LEXIA e/o i professionisti dello studio non possono essere ritenuti responsabili in alcun modo per i contenuti di questo documento, né sulla base di un incarico professionale né per qualsiasi altra ragione.