

LA GOVERNANCE DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – Decreto Legislativo n. 138 del 2024 – Capo VI artt. 40-44 – Disposizione finali e transitorie



PNRR

Dossier

Articolo 40 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 40 regola l'attuazione delle disposizioni contenute nel decreto attraverso una serie di decreti del Presidente del Consiglio dei Ministri e determinazioni dell'Agenzia per la cybersicurezza nazionale, adottati in collaborazione con altre autorità e soggetti istituzionali. Tali atti disciplinano aspetti operativi, tecnici e normativi finalizzati a garantire un'applicazione coerente ed efficace delle misure previste. Il primo comma prevede che, su proposta dell'Agenzia per la cybersicurezza nazionale e previo parere di organi come il Tavolo per l'attuazione della disciplina NIS e il Comitato interministeriale per la cybersicurezza, siano definiti criteri e modalità per l'applicazione della clausola di salvaguardia, la gestione delle sanzioni amministrative e l'organizzazione degli strumenti deflattivi del contenzioso. Inoltre, i decreti possono individuare ulteriori categorie di soggetti cui si applica il decreto, stabilire modalità di raccordo tra autorità e disciplinare la collaborazione tra l'Agenzia e le Autorità di settore NIS. Le determinazioni dell'Agenzia per la cybersicurezza nazionale specificano, tra le altre cose, l'elenco dei soggetti essenziali e importanti, i procedimenti relativi alla designazione dei rappresentanti e la politica nazionale per la divulgazione coordinata delle vulnerabilità. Sono altresì disciplinati obblighi relativi alla condivisione di informazioni di sicurezza informatica e all'utilizzo di prodotti e servizi certificati, nonché criteri per la categorizzazione delle attività multisettoriali e settoriali e la determinazione delle sanzioni amministrative. Il decreto introduce termini stringenti per l'adozione di tali atti: i principali decreti e determinazioni devono essere emanati entro trenta giorni dall'entrata in vigore del decreto, mentre ulteriori atti devono essere adottati entro sei mesi o diciotto mesi a seconda della complessità. La revisione periodica dei decreti (ogni tre anni) e delle determinazioni (ogni due anni) garantisce un costante aggiornamento del quadro normativo in linea con l'evoluzione tecnologica e delle minacce cibernetiche. Infine, il testo prevede che specifici decreti e atti, come quelli relativi alle notifiche degli incidenti e alla sicurezza nazionale, siano esclusi dall'accesso pubblico, a tutela degli interessi essenziali di sicurezza dello Stato. L'articolo mira a stabilire un solido impianto normativo e procedurale, rafforzando la collaborazione interistituzionale e garantendo un'attuazione armonizzata delle misure di cybersicurezza a livello nazionale.

Articolo 41 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 41 regola il regime transitorio e le abrogazioni necessarie per l'entrata in vigore del nuovo decreto, stabilendo il quadro normativo che garantisce una transizione ordinata verso l'attuazione delle nuove disposizioni. Le norme del presente decreto trovano applicazione a partire dal 18 ottobre 2024, data dalla quale il decreto legislativo 18 maggio 2018, n. 65, sarà abrogato, fatta eccezione per gli articoli 7, comma 8, e 8, comma 10, che rimarranno in vigore fino al 1° gennaio 2025. I Capi IV e V del medesimo decreto continueranno ad applicarsi ai soli soggetti indicati all'articolo 3, comma 9, lettera a), fino all'adozione dei provvedimenti attuativi previsti dall'Articolo 40. Il Codice delle comunicazioni elettroniche (decreto legislativo 1° agosto 2003, n. 259) subisce modifiche significative, con l'abrogazione dell'articolo 2, comma 1, lettera h), dell'articolo 30, comma 26, e degli articoli 40 e 41. Tuttavia, i provvedimenti attuativi relativi agli articoli 40 e 41 del Codice delle comunicazioni elettroniche continueranno a trovare applicazione, purché non in contrasto con la legge e le disposizioni del nuovo decreto, fino all'adozione delle determinazioni previste all'Articolo 40, comma 5, lettera l). Questo articolo assicura una transizione normativa armonizzata, garantendo la continuità operativa e l'applicabilità delle disposizioni previgenti fino all'adozione completa delle nuove misure. L'articolo rappresenta un passaggio fondamentale per il consolidamento del quadro normativo in materia di sicurezza cibernetica, assicurando il rispetto degli obblighi europei e nazionali. Inoltre, l'armonizzazione delle normative tra il decreto legislativo 2018 e il nuovo decreto permette una gestione coordinata delle competenze e delle responsabilità tra i vari soggetti coinvolti. L'articolo 41 enfatizza il ruolo strategico dei provvedimenti attuativi, che garantiranno l'implementazione progressiva delle nuove disposizioni e delle relative sanzioni, assicurando una regolamentazione coerente e trasparente in materia di cybersicurezza.

Articolo 42 del Decreto Legislativo 4 settembre 2024, n. 138

L'articolo 42 definisce le disposizioni transitorie per la fase di prima applicazione del decreto, stabilendo termini e modalità per l'adempimento degli obblighi da parte dei soggetti interessati. Entro il 17 gennaio 2025, una serie di fornitori di servizi, inclusi quelli di sistema dei nomi di dominio, cloud computing, data center, reti di distribuzione dei contenuti, servizi gestiti, mercati online, motori di ricerca e piattaforme di social network, devono registrarsi sulla piattaforma digitale predisposta ai sensi dell'articolo 7, comma 1. Tale piattaforma costituisce un elemento chiave per l'attuazione e la gestione del nuovo quadro normativo. Fino al 31 dicembre 2025, il Tavolo per l'attuazione della disciplina NIS si riunirà con cadenza almeno bimestrale per garantire un monitoraggio costante dell'implementazione della normativa e favorire il coordinamento tra i diversi attori coinvolti. Durante lo stesso periodo, i termini per l'adempimento degli obblighi previsti dagli articoli 23, 24, 25 e 29 sono fissati rispettivamente in nove e diciotto mesi dalla ricezione della comunicazione relativa alla designazione come soggetti essenziali o importanti, con la possibilità per l'Autorità nazionale competente NIS di definire modalità e specifiche per assicurare la conformità. L'obbligo di categorizzazione delle attività e dei servizi di cui all'articolo 30, comma 1, entrerà in vigore a partire dal 1° gennaio 2026, fornendo un periodo transitorio per consentire ai soggetti interessati di prepararsi adeguatamente. La registrazione sulla piattaforma digitale è consentita sin dalla pubblicazione della stessa, consentendo ai soggetti essenziali e importanti di avviare tempestivamente le procedure richieste. Queste disposizioni transitorie riflettono un approccio graduale all'attuazione della normativa, garantendo che i soggetti interessati abbiano tempi adeguati per conformarsi agli obblighi previsti e che le istituzioni competenti dispongano di strumenti efficaci per supervisionare la transizione verso il nuovo regime normativo. L'articolo evidenzia l'importanza del coordinamento istituzionale e della pianificazione progressiva per assicurare un'implementazione uniforme e coerente del decreto.

Articolo 43 del Decreto Legislativo 4 settembre 2024, n. 138

L'articolo 43 introduce modifiche normative volte a garantire la coerenza del quadro normativo nazionale con le disposizioni del presente decreto, nonché con l'architettura

nazionale di cybersicurezza e i compiti dell'Agenzia per la cybersicurezza nazionale. In particolare, le modifiche riguardano il decreto-legge 14 giugno 2021, n. 82, e il decreto-legge 21 settembre 2019, n. 105, adattandone le disposizioni per riflettere l'attuazione della direttiva (UE) 2022/2555 (NIS 2). Nel decreto-legge n. 82/2021, viene aggiornata la definizione di "decreto legislativo NIS" (art. 1, comma 1, lettera d), per includere il recepimento della direttiva NIS 2, e vengono riformulate le competenze dell'Agenzia per la cybersicurezza nazionale. Quest'ultima è designata come Autorità nazionale competente NIS, Punto di contatto unico NIS e Autorità nazionale per la gestione delle crisi informatiche, nonché come CSIRT Italia, centralizzando così le responsabilità in materia di cybersicurezza. Sono altresì abrogate alcune disposizioni superflue o non più pertinenti, come il comma 3 dell'articolo 7 e l'intero articolo 15, per eliminare eventuali sovrapposizioni normative. Nel decreto-legge n. 105/2019, viene abrogato il comma 3-bis dell'articolo 1, mentre il comma 8 viene riformulato per chiarire che la notifica di incidente da parte dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica soddisfa anche gli obblighi di notifica previsti dall'articolo 25 del presente decreto. Inoltre, viene introdotto il nuovo comma 8-bis, che estende agli stessi soggetti alcuni obblighi e poteri ispettivi e sanzionatori applicabili ai soggetti essenziali, con riferimento ai sistemi informativi e di rete non inclusi nell'elenco specifico previsto dal decreto. Questo rafforza l'armonizzazione tra le misure di cybersicurezza applicabili al perimetro nazionale e quelle stabilite dal decreto legislativo NIS. Le modifiche apportate garantiscono un'implementazione coordinata della direttiva NIS 2, promuovendo un approccio centralizzato e razionale alla gestione della sicurezza cibernetica, con particolare enfasi sulla chiarezza delle competenze, sull'unità operativa e sulla coerenza normativa. L'articolo evidenzia inoltre l'impegno a evitare duplicazioni negli obblighi di notifica, semplificando i processi per i soggetti interessati, e ad assicurare che le misure di cybersicurezza siano applicate in modo proporzionato e graduale.

Articolo 44 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 44 disciplina gli aspetti finanziari relativi all'attuazione del decreto, con particolare riferimento alle spese ICT delle pubbliche amministrazioni e alla copertura

degli oneri derivanti dalle disposizioni normative. Le spese ICT sostenute dalle pubbliche amministrazioni per l'adeguamento dei sistemi informativi al presente decreto, incluse quelle relative agli articoli 10, 11, 13 e 15, devono essere coerenti con il Piano triennale per l'informatica nella pubblica amministrazione, come previsto dalla legge 28 dicembre 2015, n. 208. Tale coerenza garantisce un approccio pianificato e strategico nell'utilizzo delle risorse per il miglioramento dell'infrastruttura digitale. Per la copertura degli oneri derivanti dalle disposizioni del decreto, pari a 409.424 euro per l'anno 2024 e 5.925.695 euro annui a partire dal 2025, si prevede il ricorso a due fonti principali di finanziamento. La prima, attraverso una riduzione corrispondente del Fondo per il recepimento della normativa europea, prevede un utilizzo graduale dei fondi: 409.424 euro per il 2024, 2.625.695 euro per il 2025, 2.707.695 euro per il 2026 e 3.100.695 euro annui a decorrere dal 2027. La seconda fonte, pari a 3.300.000 euro per il 2025, 3.218.000 euro per il 2026 e 2.825.000 euro annui a decorrere dal 2027, deriva dalle risorse liberate dall'abrogazione delle disposizioni indicate all'Articolo 41, comma 2. L'articolo stabilisce inoltre che, salvo quanto espressamente previsto per la copertura degli oneri, dall'attuazione del decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni competenti sono tenute a operare nell'ambito delle risorse umane, strumentali e finanziarie già disponibili, evitando così l'introduzione di spese aggiuntive non coperte. Questo approccio garantisce la sostenibilità economica del decreto, promuovendo al contempo l'efficienza e l'ottimizzazione delle risorse pubbliche. L'articolo 44 rappresenta un pilastro fondamentale per l'attuazione finanziaria del decreto, assicurando che le spese necessarie siano pianificate e coperte attraverso un utilizzo oculato delle risorse disponibili, senza gravare ulteriormente sui conti pubblici.

