LA GOVERNANCE DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – Decreto Legislativo n. 138 del 2024 – Capo V artt. 34-39 - Monitoraggio, vigilanza ed esecuzione

PNRR

Dossier

Articolo 34 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 34 delinea i principi fondamentali che regolano l'attività di vigilanza ed esecuzione affidata all'Autorità nazionale competente NIS, al fine di monitorare e garantire l'adempimento degli obblighi previsti in materia di sicurezza informatica da parte dei soggetti essenziali e importanti. L'Autorità svolge le proprie funzioni mediante il monitoraggio, l'analisi, le verifiche e le ispezioni, nonché attraverso l'adozione di misure di esecuzione, comprensive di sanzioni amministrative pecuniarie e accessorie, finalizzate a promuovere l'osservanza della normativa. Il testo prevede inoltre che l'Autorità adotti un approccio basato sul rischio, così da concentrare le proprie risorse sui casi di maggiore criticità e garantire un'efficace gestione delle attività di vigilanza. Essa è altresì chiamata a rispettare i principi di effettività, proporzionalità e dissuasività nell'esecuzione delle proprie competenze, tenendo in considerazione le specificità di ciascun caso e conformandosi ai criteri indicati dall'Articolo 31. La norma sottolinea l'indipendenza operativa dell'Autorità, soprattutto nei confronti degli enti della pubblica amministrazione sottoposti a vigilanza, e prescrive l'obbligo di motivare dettagliatamente ogni provvedimento adottato. La valutazione delle violazioni deve tenere conto di diversi elementi, tra cui la gravità e la durata della violazione, l'eventuale recidiva, il danno causato, la condotta intenzionale o negligente del trasgressore e il livello di collaborazione dimostrato, nonché l'adozione di eventuali misure preventive o mitigative. Particolare rilievo è attribuito alle violazioni considerate gravi, quali il mancato rimedio a incidenti significativi, la mancata notifica di tali incidenti, l'ostacolo alle attività di vigilanza e la fornitura di informazioni false o inesatte. L'articolo stabilisce che gli audit e le scansioni di sicurezza siano svolti da organismi indipendenti sulla base di valutazioni del rischio e prevede che i costi delle verifiche siano generalmente a carico del soggetto sottoposto ad audit, salvo diverse disposizioni motivate dall'Autorità. L'adozione di strumenti tecnologici è promossa tramite la previsione di interazioni prioritarie con i soggetti vigilati attraverso una piattaforma digitale dedicata, in linea con quanto disposto dall'Articolo 7, comma 1. Infine, il quadro regolatorio delle attività e dei poteri attribuiti all'Autorità sarà definito mediante un decreto del Presidente del Consiglio

dei Ministri, con l'obiettivo di garantire una coerenza applicativa e operativa nell'esercizio delle funzioni di vigilanza e nell'irrogazione delle relative sanzioni.

Articolo 35 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 35 disciplina l'attività di monitoraggio, analisi e supporto esercitata dall'Autorità nazionale competente NIS, con l'obiettivo di verificare l'adempimento degli obblighi imposti dal presente decreto e di promuovere l'efficace implementazione delle misure previste. Ai sensi del primo comma, l'Autorità verifica la correttezza e la conformità delle informazioni trasmesse dai soggetti registrati in relazione ai requisiti prescritti, funzionali all'inserimento nell'elenco di cui all'Articolo 7, comma 2, garantendo altresì la diffusione trasparente dei criteri che regolano l'ambito di applicazione della normativa e degli obblighi correlati. L'Autorità è altresì incaricata di monitorare l'attuazione degli obblighi previsti dal decreto per tutti i soggetti rientranti nell'ambito di applicazione di cui all'Articolo 3, implementando, ove necessario, specifici interventi di supporto. Per l'espletamento di tali compiti, l'Autorità può richiedere ai soggetti interessati una rendicontazione periodica, comprensiva di autovalutazioni e piani di implementazione, nonché ulteriori informazioni necessarie all'esercizio delle proprie funzioni istituzionali, specificando chiaramente le finalità della richiesta. Inoltre, è prevista la possibilità di richiedere l'esecuzione di audit e scansioni di sicurezza, mirati o periodici, soprattutto in caso di incidenti significativi o violazioni della normativa, basandosi su criteri obiettivi, equi e trasparenti, eventualmente in cooperazione con i soggetti interessati. In presenza di presunte violazioni, l'Autorità può altresì emanare raccomandazioni e avvertimenti. Il decreto prevede che l'Autorità indichi modalità e termini proporzionati per adempiere agli obblighi e riferire sullo stato di attuazione, assicurando che tali disposizioni siano ragionevoli rispetto al contesto di riferimento. L'analisi delle risultanze delle attività consente all'Autorità di stabilire le priorità negli interventi di supporto e di individuare linee guida per lo sviluppo della regolamentazione ai sensi dell'Articolo 31. Tuttavia, tali interventi sono subordinati alla condizione che non comportino oneri

sproporzionati o eccessivi. Infine, per lo svolgimento delle attività descritte, l'Autorità può avvalersi del supporto dei tavoli settoriali previsti dall'Articolo 11, comma 4, lettera f), rafforzando così il coordinamento tra i diversi attori coinvolti nella gestione della sicurezza informatica.

Articolo 36 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 36 stabilisce il quadro normativo per l'esercizio dei poteri di verifica e ispezione da parte dell'Autorità nazionale competente NIS nei confronti dei soggetti rientranti nell'ambito di applicazione del presente decreto. Tali poteri rappresentano uno strumento cruciale per garantire il rispetto degli obblighi normativi in materia di sicurezza informatica. L'Autorità può procedere a verifiche della documentazione e delle informazioni trasmesse dai soggetti ai sensi delle disposizioni normative, effettuare ispezioni sia in loco sia a distanza, includendo anche controlli casuali, e richiedere l'accesso a dati, documenti e altre informazioni rilevanti per lo svolgimento dei compiti istituzionali, previa dichiarazione della finalità e specificazione puntuale delle informazioni richieste. Tali attività consentono di garantire la conformità normativa e di accertare eventuali violazioni. Nei confronti dei soggetti qualificati come "importanti", l'esercizio dei poteri ispettivi è subordinato alla presenza di elementi di prova, indicazioni o informazioni che suggeriscano potenziali violazioni delle disposizioni del decreto, limitando così le ispezioni a casi in cui esistano motivi concreti e fondati per procedere. Questo approccio garantisce un equilibrio tra la necessità di vigilanza e il principio di proporzionalità, evitando un ricorso eccessivo a misure invasive in assenza di riscontri concreti di possibili irregolarità.

Articolo 37 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 37 disciplina l'esercizio dei poteri di esecuzione da parte dell'Autorità nazionale competente NIS, che si avvale dei risultati delle attività di monitoraggio, analisi e supporto di cui all'Articolo 35 e delle verifiche e ispezioni condotte ai sensi dell'Articolo 36. Nell'espletamento delle proprie funzioni, l'Autorità può richiedere ai soggetti l'accesso a dati, documenti e prove che attestino l'attuazione di politiche di sicurezza informatica e il rispetto degli obblighi previsti dal decreto, con particolare attenzione alla valutazione delle misure di gestione dei rischi per la sicurezza informatica e alla corretta trasmissione e notifica delle informazioni richieste. Tra le misure esecutive, l'Autorità può intimare ai soggetti l'esecuzione di audit di sicurezza, scansioni basate su criteri di valutazione del rischio, l'adozione di raccomandazioni derivanti dagli audit e il pieno adempimento agli obblighi normativi. Può inoltre ordinare di cessare comportamenti illeciti, porre rimedio a carenze e comunicare tempestivamente agli utenti eventuali incidenti o minacce informatiche, includendo la divulgazione al pubblico di violazioni significative. Le istruzioni impartite possono estendersi alla prevenzione e al rimedio degli incidenti, con l'adozione di istruzioni vincolanti finalizzate alla protezione della sicurezza informatica. L'Autorità può designare propri funzionari per supportare i soggetti nell'adempimento degli obblighi, prevedendo visite in loco o a distanza, e richiedere piena collaborazione da parte dei soggetti interessati. In caso di mancato adempimento, l'Autorità diffida i soggetti a conformarsi alle disposizioni, definendo modalità e termini proporzionati per l'attuazione degli obblighi e richiedendo rapporti sullo stato di avanzamento. Prima dell'adozione di provvedimenti esecutivi, l'Autorità notifica le conclusioni preliminari ai soggetti interessati, concedendo un termine minimo di quindici giorni per la presentazione di osservazioni, salvo i casi in cui la notifica pregiudichi interventi immediati per prevenire o rispondere a incidenti. Qualora siano adottati più provvedimenti legati alla medesima fattispecie, l'obbligo di notifica si applica esclusivamente al primo provvedimento. Questo articolo mira a bilanciare l'efficacia dell'azione amministrativa con il rispetto dei diritti dei soggetti vigilati, adottando un approccio proporzionato e basato sul rischio.

Articolo 38 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 38 disciplina i poteri sanzionatori dell'Autorità nazionale competente NIS, specificando i criteri, le modalità e le sanzioni applicabili per le violazioni degli obblighi previsti dal decreto. Le attività sanzionatorie si basano sugli esiti delle attività di monitoraggio, supporto, analisi, verifica, ispezione ed esecuzione, garantendo un approccio coerente e integrato. L'Autorità può specificare ulteriormente i criteri per la determinazione delle sanzioni, assicurando che queste siano effettive, proporzionate e dissuasive. La mancata ottemperanza alle diffide comporta la possibilità per l'Autorità di sospendere certificazioni o autorizzazioni, finché le misure necessarie non siano adottate, escludendo tuttavia questa misura per le pubbliche amministrazioni e altri soggetti specifici indicati. Sono previsti obblighi per le persone fisiche responsabili di soggetti essenziali o importanti, che possono essere ritenute responsabili per l'inadempimento delle disposizioni normative. In caso di violazioni persistenti, l'Autorità può applicare sanzioni accessorie, come l'incapacità temporanea a svolgere funzioni dirigenziali. Per i dipendenti pubblici, eventuali inadempimenti possono costituire motivo di responsabilità disciplinare, dirigenziale e contabile. Le violazioni degli obblighi relativi alla gestione del rischio, alla notifica di incidenti e agli adempimenti stabiliti dall'Autorità comportano l'irrogazione di sanzioni pecuniarie, il cui importo varia in base alla gravità della violazione e alla tipologia del soggetto interessato, con differenze tra soggetti essenziali, importanti e pubbliche amministrazioni. Sono previsti specifici minimi e massimi edittali, nonché un sistema di proporzionalità che tiene conto del fatturato annuo su scala mondiale. L'articolo introduce anche strumenti deflattivi del contenzioso, quali l'invito a conformarsi entro termini congrui o la possibilità di estinguere il procedimento attraverso il pagamento in misura ridotta. I proventi delle sanzioni sono destinati all'incremento delle risorse dell'Agenzia per la cybersicurezza nazionale, garantendo così il reinvestimento delle somme raccolte nel rafforzamento delle capacità di sicurezza cibernetica. Infine, l'articolo prevede specifiche disposizioni per la reiterazione delle violazioni, con l'applicazione di sanzioni aumentate in caso di recidiva e misure aggiuntive per la gestione delle mancanze continuative.

Articolo 39 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 39 disciplina il meccanismo di cooperazione e assistenza reciproca tra l'Autorità nazionale competente NIS e le autorità degli altri Stati membri, al fine di garantire una gestione coordinata ed efficace degli obblighi di sicurezza informatica transfrontalieri. L'assistenza reciproca si applica nei casi in cui un soggetto, rientrante sotto la giurisdizione nazionale o il cui sistema informativo è ubicato sul territorio nazionale, fornisca servizi in altri Stati membri, o viceversa. La cooperazione include notifiche e consultazioni mediante il Punto di contatto unico NIS riguardo a ispezioni, misure di esecuzione e sanzioni, la possibilità di richiedere attività ispettive o misure esecutive, e il supporto proporzionato alle risorse disponibili per garantire un'applicazione coerente e coordinata delle misure. Tale assistenza può riguardare richieste di informazioni, ispezioni in loco o a distanza, e audit sulla sicurezza mirati. L'Autorità può respingere una richiesta di assistenza qualora non sia competente, la richiesta non sia proporzionata o implichi attività o divulgazioni contrarie agli interessi essenziali di sicurezza nazionale, pubblica sicurezza o difesa dello Stato. In tali circostanze, l'Autorità consulta previamente le autorità competenti degli Stati membri interessati e, su richiesta, la Commissione europea e l'ENISA. È altresì prevista la possibilità di attività ispettive ed esecutive congiunte tra l'Autorità nazionale competente NIS e le autorità degli altri Stati membri, qualora opportuno e previo accordo. L'Autorità può esercitare i propri poteri nei confronti di soggetti che forniscono servizi in altri Stati membri su richiesta di cooperazione e, parallelamente, inoltrare richieste alle autorità di altri Stati membri per l'esercizio dei rispettivi poteri nei confronti di soggetti operanti sul territorio nazionale. L'articolo enfatizza la necessità di un approccio armonizzato e cooperativo a livello europeo, in linea con gli obiettivi della direttiva NIS 2, assicurando al contempo la tutela degli interessi nazionali sensibili.