La protezione dei dati personali

nella

Direttiva NIS2

Carlo Brozzo

18 Settembre 2025

La Direttiva NIS 2 contiene diversi riferimenti espliciti alla protezione dei dati personali, sia nei considerando sia nel corpo del testo.

Considerando 121

Stabilisce la base giuridica per il trattamento dei dati in ambito cibersicurezza. Questo considerando chiarisce che il trattamento di dati personali da parte dei soggetti essenziali e importanti può essere considerato lecito ai sensi del GDPR.

Base giuridica per il trattamento

Il trattamento dei dati per la cibersicurezza deve rispettare norme giuridiche specifiche per garantire la protezione.

Importanza della cibersicurezza

Garantire la cibersicurezza è fondamentale per proteggere dati personali e infrastrutture critiche.

Obbligo legale e legittimo interesse come basi di liceità

Obbligo legale

Il trattamento è considerato necessario per adempiere a un obbligo legale a cui il titolare del trattamento (il soggetto essenziale o importante) è soggetto in virtù della direttiva stessa.

Legittimo interesse

Il trattamento può essere necessario anche per il perseguimento del legittimo interesse dei soggetti essenziali e importanti, nonché dei loro fornitori di servizi di sicurezza, a garantire la sicurezza dei propri sistemi

Categorie di dati trattati

I dati trattati includono indirizzi IP, URL, email e altre informazioni personali.

Questo principio è ribadito nel Regolamento delegato (UE) 2024/1366 per il settore dell'energia elettrica, il cui Considerando 33 riprende quasi testualmente le disposizioni del Considerando 121 della NIS 2, confermando la solidità di questo approccio normativo

Considerando 106: punto di ingresso unico per notifiche di incidenti

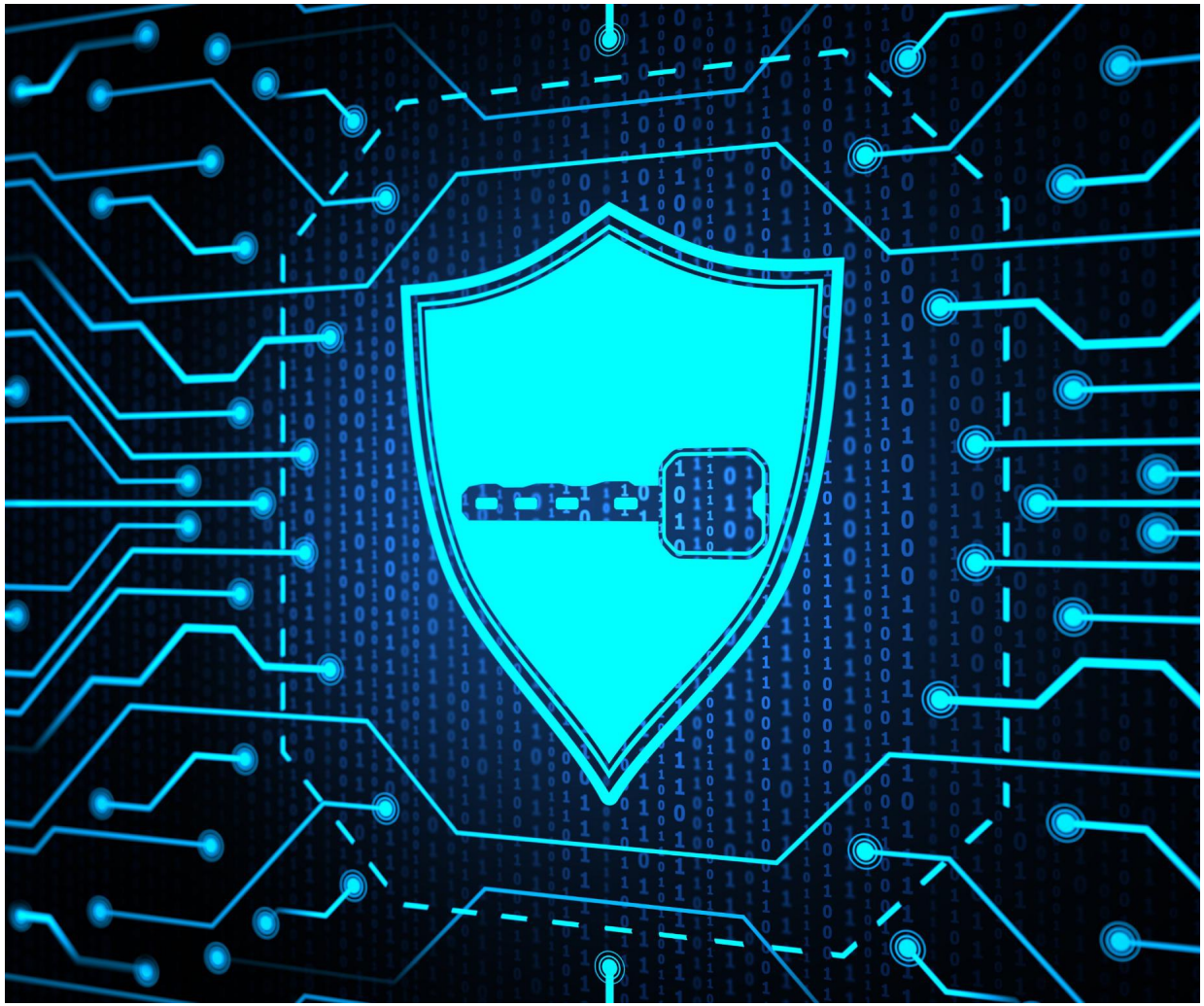
Incoraggia gli Stati membri a istituire un "punto di ingresso unico" per la notifica degli incidenti, al fine di ridurre gli oneri amministrativi per le imprese. Si suggerisce che tale punto unico possa essere utilizzato anche per le notifiche di violazioni di dati personali previste dal GDPR, fermo restando il rispetto delle disposizioni del GDPR stesso, in particolare quelle relative all'indipendenza delle autorità di controllo

Considerando 108: cooperazione tra autorità di cibersicurezza e protezione dei dati

Sottolinea che, poiché gli incidenti spesso compromettono dati personali, le autorità competenti ai sensi della NIS 2 "dovrebbero cooperare e scambiarsi informazioni su tutte le questioni pertinenti con le autorità di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE"

Articolo 35 Violazioni che comportano una violazione dei dati personali

L'articolo 35 della Direttiva NIS 2 è specificamente dedicato a disciplinare le situazioni in cui una violazione degli obblighi di cibersicurezza previsti dalla direttiva stessa si traduce anche in una violazione di dati personali (un "data breach") ai sensi del GDPR. Questo articolo svolge una funzione di coordinamento tra le autorità competenti per la cibersicurezza (autorità NIS) e le autorità di controllo per la protezione dei dati (Garante per la protezione dei dati personali).



Obbligo di informazione tra autorità (Art. 35, paragrafo 1)

Il primo paragrafo stabilisce un obbligo di comunicazione a carico delle autorità competenti NIS. Qualora, nell'esercizio delle loro funzioni di vigilanza ed esecuzione, vengano a conoscenza che la violazione degli obblighi previsti dagli **articoli 21 (Misure di gestione dei rischi di cibersicurezza)** e **23 (Obblighi di segnalazione)** da parte di un soggetto essenziale o importante possa comportare una violazione di dati personali, esse devono informare "senza indebito ritardo" le autorità di controllo competenti in materia di protezione dei dati

Principio del ne bis in idem e coordinamento sanzionatorio (Art. 35, paragrafo 2)

Il secondo paragrafo dell'articolo 35 introduce un'importante regola di coordinamento per evitare la duplicazione delle sanzioni pecuniarie per la medesima condotta.
Nello specifico, si prevede che se l'autorità di controllo per la protezione dei dati impone una sanzione amministrativa pecuniaria ai sensi dell'articolo 58, paragrafo 2, lettera i), del GDPR per una violazione di dati personali, l'autorità competente NIS non può imporre a sua volta una sanzione amministrativa pecuniaria ai sensi dell'articolo 34 della Direttiva NIS 2 per la stessa violazione

È fondamentale notare che questo divieto riguarda esclusivamente le sanzioni pecuniarie. L'autorità NIS conserva la facoltà di imporre altre misure correttive ed esecutive previste dalla direttiva, come:

- Emettere avvertimenti;
- Impartire istruzioni vincolanti;
- Ordinare di porre fine a una violazione;
- Ordinare di conformarsi agli obblighi della direttiva.

Riferimenti indiretti negli Articoli 21 e 23

Articolo 21 - Misure di gestione dei rischi di cibersicurezza: Questo articolo impone ai soggetti essenziali e importanti di adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza dei sistemi informatici e di rete. Tali misure includono, tra le altre, l'analisi dei rischi, la gestione degli incidenti, la sicurezza della catena di approvvigionamento e l'uso della crittografia. Poiché i sistemi informatici e di rete di questi soggetti trattano quasi inevitabilmente dati personali, le misure di sicurezza richieste dall'articolo 21 servono anche a proteggere tali dati, in linea con il principio di "integrità e riservatezza" sancito dall'articolo 5 del GDPR e con gli obblighi di sicurezza dell'articolo 32 del GDPR.

Articolo 23 - Obblighi di segnalazione: Questo articolo obbliga i soggetti a notificare senza indebito ritardo all'autorità competente o al CSIRT (Computer Security Incident Response Team) qualsiasi incidente che abbia un impatto significativo sulla fornitura dei loro servizi. Se un tale incidente comporta anche una violazione di dati personali, scatta il doppio obbligo di notifica: quello previsto dall'articolo 23 della NIS 2 verso l'autorità NIS/CSIRT e quello previsto dall'articolo 33 del GDPR verso l'autorità di protezione dei dati. L'articolo 35 della NIS 2, come visto, serve a coordinare la risposta delle rispettive autorità a seguito di tali eventi.