WORKSHOP GARR 2024

NET MAKERS

NIS2 e GDPR

Cybersicurezza e protezione dei dati personali

Roberto Puccinelli

Consiglio Nazionale delle Ricerche

Overview

NIS2:

- Obiettivi
- Novità
- Contenuti
- Soggetti
- Roadmap

GDPR:

- Obiettivi
- Soggetti
- Contenuti

Ecosistemi

Complementarietà e intersezioni

Verso un approccio integrato

Ambiti di Applicazione: NIS2 vs GDPR

Aree di intervento:

- **NIS2**: Focus sulla sicurezza dei sistemi informatici, protezione delle reti e sistemi ICT essenziali per la società. Mira a garantire resilienza e continuità operativa contro cyber minacce.
- **GDPR**: Focus sulla protezione dei dati personali, regolamentazione del trattamento e tutela dei diritti e delle libertà degli individui. Garantisce la privacy e il controllo sui dati.

Differenze chiave:

- **NIS2**: Tutela della sicurezza nazionale ed europea della minacce cyber.
- **GDPR**: Tutela dei diritti e delle libertà degli interessati.

NIS2 Network and Information Security

Normativa europea **adottata nel 2022 per rafforzare la sicurezza informatica nell'Unione Europea**.

Sostituisce la precedente Direttiva NIS del 2016, ampliando **l'ambito di applicazione** e introducendo **nuovi requisiti per le organizzazioni e gli Stati membri**.

Perché?

- Evoluzione delle minacce cibernetiche
- Evoluzione della superficie di attacco (5G, l'Intelligenza Artificiale, Internet delle Cose, …)
- Estensione ambito di applicazione della NIS ad ulteriori settori critici
- Disomogeneità di applicazione negli stati membri
- Necessità di miglioramento della gestione del rischio e della cooperazione
- Sanzioni più severe e coerenti con GDPR

Obiettivi

MIGLIORARE LA RESILIENZA E LA RISPOSTA AGLI INCIDENTI CYBER DELLE INFRASTRUTTURE CRITICHE E DEGLI OPERATORI DI SERVIZI ESSENZIALI.

AUMENTARE LA COOPERAZIONE TRA STATI MEMBRI PER UNA RISPOSTA COORDINATA AGLI INCIDENTI DI SICUREZZA.

GARANTIRE STANDARD DI SICUREZZA.

Soggetti essenziali e importanti

•**Soggetti essenziali**: Organizzazioni strategiche per la sicurezza e il funzionamento dell'economia e della società, il cui malfunzionamento avrebbe un impatto critico. Includono settori come l'energia, i trasporti, la sanità, le infrastrutture digitali, le finanze e la pubblica amministrazione.

•**Soggetti importanti**: Attori di rilevanza per la sicurezza dei sistemi digitali, il cui impatto è significativo, ma non critico. Comprendono settori come le telecomunicazioni, i servizi postali, la gestione dei rifiuti, la produzione alimentare e le industrie chimiche.

La direttiva impone requisiti di sicurezza specifici, come l'adozione di misure tecniche e organizzative e la segnalazione degli incidenti, con livelli di conformità e sanzioni variabili in base alla categoria.

Regolamento di esecuzione

La Commissione Europea ha pubblicato il **Regolamento di esecuzione (UE) 2024/2690** il 17 ottobre 2024, che mira a stabilire i requisiti tecnici e metodologici delle misure di gestione dei rischi cyber (NIS2 articolo 21, paragrafo 2) e a specificare ulteriormente i casi in cui un incidente dovrebbe essere considerato significativo (NIS2 articolo 23, paragrafo 3).

Operativo dal 7 novembre 2024

Novità

•**Ampliamento dei settori e dei soggetti**: La NIS 2 estende il campo di applicazione, includendo nuovi settori critici come i fornitori di servizi digitali, le infrastrutture sanitarie, la gestione dei rifiuti e i servizi di pubblica amministrazione. Introduce anche la distinzione tra **soggetti essenziali** e **soggetti importanti** per graduare i requisiti di sicurezza.

•**Rafforzamento dei requisiti di sicurezza**: Richiede misure di sicurezza più stringenti per tutti i soggetti, inclusi la gestione del rischio, la notifica degli incidenti e l'adozione di controlli specifici.

•**Miglioramento della governance e delle sanzioni**: Introduce un maggiore coordinamento tra gli Stati membri e prevede sanzioni più severe per le violazioni della direttiva.

•**Segnalazione degli incidenti e tempestività**: Standardizza le procedure e i tempi per la segnalazione degli incidenti, per una risposta più rapida e coordinata a livello europeo.

Roadmap NIS2

- 27 dicembre 2022: **Pubblicazione della direttiva NIS2**
- 17 ottobre 2024: **Recepimento della direttiva da parte degli Stati Membri**
- 7 novembre 2024: **Entrata in vigore del Regolamento di Esecuzione (UE) 2024/2690**
- A partire da Novembre 2024: **Implementazione delle misure da parte dei Soggetti Pertinenti**
- Dal 2025: **Monitoraggio continuo e valutazione dell'applicazione**

Revisione Periodica: Ogni 3 anni

- Obiettivo: Adattare le misure in base all'evoluzione delle minacce e delle tecnologie.

Scadenze per gli Stati Membri

- **17 ottobre 2024**: Termine entro il quale gli Stati membri devono recepire la Direttiva NIS2 nelle rispettive legislazioni nazionali.

- **17 aprile 2025**: Entro questa data, gli Stati membri devono comunicare alla Commissione Europea l'elenco dei soggetti essenziali e importanti identificati secondo i criteri della direttiva.

Calendario per i soggetti essenziali ed importanti

- **1 gennaio - 28 febbraio 2025**: registrazione su apposita piattaforma digitale ACN.
- **17 gennaio 2025**: Scadenza anticipata per la registrazione sulla piattaforma ACN per specifiche categorie di fornitori (servizi DNS, gestori TLD, registrar, data center, cloud provider, etc.)
- **31 marzo 2025**: ACN completerà la redazione dell'elenco ufficiale dei soggetti essenziali e importanti in base alle registrazioni ricevute.
- **1 aprile - 15 aprile 2025**: ACN invierà una comunicazione ufficiale di inserimento nell'elenco ai soggetti registrati.
- **1 gennaio 2026**: Termine entro il quale i soggetti identificati devono adeguarsi agli obblighi relativi alla notifica degli incidenti (articolo 25) e aggiornare annualmente le informazioni richieste dalla piattaforma ACN (articolo 30).
- **Ottobre 2026**: Scadenza per l'adeguamento agli obblighi riguardanti gli organi di amministrazione e direttivi (articolo 23), la gestione dei rischi e l'implementazione delle misure di sicurezza (articolo 24) e la banca dati dei nomi a dominio (articolo 29).

Organismi di cooperazione e coordinamento

EU Cyber Crises Liaison Organisation Network (EU-CyCLONe): Questo nuovo organismo ha il compito di coordinare la risposta a incidenti informatici significativi tra gli Stati membri, garantendo una gestione rapida e coordinata delle crisi. EU-CyCLONe facilita il supporto operativo e consente agli Stati di collaborare su decisioni strategiche in tempo reale.

Network of National CSIRTs (Computer Security Incident Response Teams): Sebbene già presente nella NIS 1, la NIS 2 rafforza il ruolo dei CSIRTs nazionali come punto di riferimento per la segnalazione e la gestione di incidenti a livello di ciascun Paese. I CSIRTs collaborano tra loro per assicurare una risposta coordinata e uno scambio di informazioni efficace.

Gruppo di Cooperazione: Previsto anche nella NIS 1, il Gruppo di Cooperazione è ulteriormente potenziato dalla NIS 2. Include rappresentanti degli Stati membri, della Commissione Europea e dell'ENISA (l'Agenzia dell'UE per la cybersicurezza), con l'obiettivo di promuovere lo scambio di informazioni, sviluppare buone pratiche e linee guida e migliorare la resilienza collettiva.

Obiettivi:

- rafforzare l'ecosistema di cybersicurezza e renderlo più coeso,
- fornire risposte tempestive e coordinate in caso di minacce o incidenti significativi,
- migliorare la resilienza complessiva dell'Unione Europea.

D.Lgs. 4 settembre 2024, n. 138 - Recepimento Direttiva NIS2

1.Obiettivo: Rafforzare la sicurezza informatica delle infrastrutture critiche nazionali per garantire un livello elevato e comune di cybersecurity nell'UE.

2.Ambiti di Applicazione: Include settori essenziali (energia, trasporti, sanità, finanziario, pubblico) e importanti (digitale, forniture IT, servizi sociali).

3.Agenzia per la Cybersicurezza Nazionale (ACN): Designata come Autorità competente per la sicurezza informatica e **Punto di contatto unico** per l'applicazione della Direttiva NIS2; responsabile dell'attuazione e della vigilanza.

4.Obblighi per gli Operatori Essenziali e Importanti:

1. **Gestione del Rischio**: Implementazione di misure tecniche e organizzative adeguate.
2. **Notifica degli Incidenti**: Segnalazione degli incidenti di sicurezza significativi entro tempi stabiliti.
3. **Conformità e Verifiche**: Soggetti a controlli periodici da parte dell'ACN.

5.Registro dei Soggetti Coinvolti: Creazione di un registro nazionale per monitorare i soggetti obbligati.

6.Sanzioni: Previste sanzioni amministrative e pecuniarie per mancata conformità, fino al 2% del fatturato annuo globale.

Entrata in Vigore: 16 ottobre 2024.

GDPR

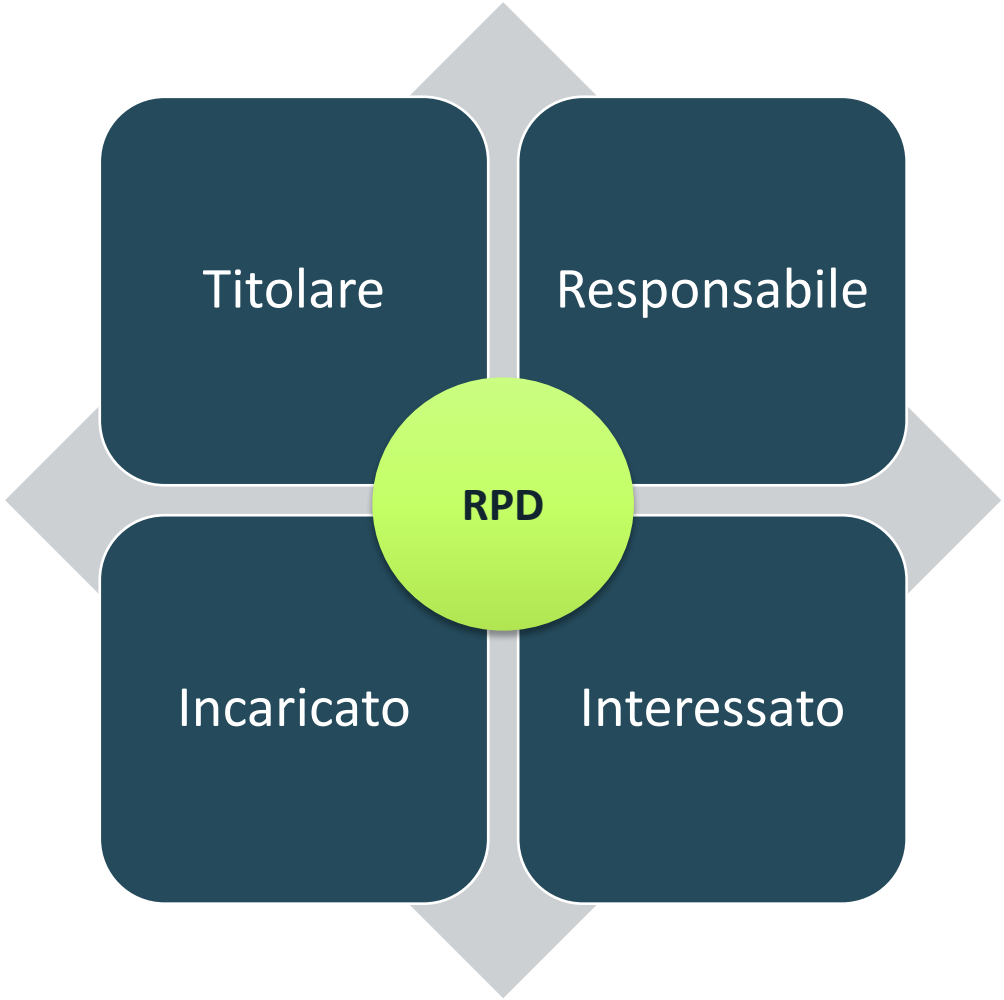
Obiettivo: Rafforzare e unificare la protezione dei dati personali dei cittadini dell'Unione Europea, garantendo maggiore controllo sugli stessi e migliorando la fiducia nel trattamento dei dati.

Motivazioni principali:

- **Tutela dei Diritti**: Salvaguardare i diritti e le libertà fondamentali dei cittadini, proteggendo la loro privacy in un'era digitale.
- **Uniformità Normativa**: Superare le differenze tra le normative dei vari Stati membri, creando un quadro giuridico unico e omogeneo.
- **Risposta alla Tecnologia**: Affrontare le sfide poste dai nuovi sviluppi tecnologici (big data, IA, cloud) e dalle crescenti attività online.
- **Fiducia e Sicurezza**: Rafforzare la fiducia dei consumatori e delle aziende nel mercato digitale, incentivando pratiche di trattamento dei dati trasparenti e sicure.

Principi Chiave: Liceità, correttezza e trasparenza; minimizzazione dei dati; limitazione della conservazione; responsabilità e sicurezza.

Soggetti dei trattamenti



Contenuti

- Diritti dell'interessato
- Doveri del Titolare e del Responsabile
- Autorità di controllo indipendenti
- Definizione del Responsabile per la Protezione dei dati
- Cooperazione e coerenza
- Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
- Mezzi di ricorso, responsabilità e sanzioni
- Disposizioni per settori specifici

Garante per la Protezione dei Dati Personali

Ruolo: Autorità indipendente istituita per vigilare sul rispetto delle normative sulla protezione dei dati personali in Italia.

Principali Compiti:

- **Tutela dei Diritti dei Cittadini**: Assicura il rispetto del diritto alla privacy e alla protezione dei dati personali.
- **Controllo e Vigilanza**: Verifica la conformità delle aziende, enti pubblici e organizzazioni alle normative (GDPR e Codice Privacy).
- **Interventi e Sanzioni**: Può emettere provvedimenti correttivi, ordinanze e sanzioni in caso di violazioni.
- **Linee Guida e Consulenza**: Fornisce indicazioni e orientamenti per garantire un'adeguata protezione dei dati.

Obiettivo: Promuovere la cultura della protezione dei dati, garantendo sicurezza e trasparenza nei trattamenti per la tutela dei diritti dei cittadini.

European Data Protection Board

Descrizione: L'EDPB è un organismo indipendente dell'UE istituito dal GDPR (Regolamento (UE) 2016/679) per garantire l'applicazione coerente della normativa sulla protezione dei dati nei Paesi membri.

Composizione: Include i rappresentanti delle autorità di protezione dei dati di ciascun Paese dell'UE e il Garante europeo della protezione dei dati (EDPS).

Principali Funzioni:

- **Linee Guida e Raccomandazioni**: Emette orientamenti per un'applicazione uniforme del GDPR.
- **Consulenza alla Commissione Europea**: Fornisce pareri e suggerimenti in ambito di protezione dei dati.
- **Coordinamento e Risoluzione delle Controversie**: Facilita la cooperazione tra autorità e risolve i conflitti transfrontalieri.

Obiettivo: Assicurare una protezione dei dati uniforme e di alto livello nell'UE, promuovendo i diritti fondamentali alla privacy e alla protezione dei dati personali.

Ecosistemi

Privacy — **Sicurezza**

Europeo

- **EPDB** — edpb — European Data Protection Board
- **Garante Europeo**
- **ENISA** — enisa — European Union Agency for Cybersecurity
- **Gruppo coordinamento**
- **EU-CyCLONe** — CyCLONe — European Cyber Crises Liaison Organisation Network — Powered by ENISA
- **CSIRT network** — CSIRTs Network

Nazionale

- **Autorità Garanti Nazionali**
- **P.ti contatto nazionali**
- **CSIRT Nazionali**

Locale

- **Titolari e RPD**
- **Soggetti e CISO**

- **CSIRT sub-nazionali**

Intersezioni e Complementarietà

Obiettivi Comuni: Entrambe le normative mirano a proteggere l'integrità, la riservatezza e la disponibilità dei sistemi e dei dati.

Sovrapposizioni: La sicurezza informatica (NIS2) e la privacy (GDPR) si intersecano nella protezione dei dati personali contro accessi non autorizzati e cyber attacchi.

Norme Complementari: La sicurezza informatica garantisce la protezione dell'infrastruttura, mentre il GDPR assicura che i dati personali siano trattati in modo sicuro e conforme.

Titolari e Soggetti essenziali ed importanti

Ambito	Titolare	Soggetto essenziale o importante
Misure tecniche e organizzative	A tutela dei dati personali	A tutela della sicurezza dei sistemi e delle reti informatiche
Violazioni	Notifica al Garante	Notifica a ANC (autorità competente per l'Italia e gestore del CSIRT nazionale)
Valutazione del rischio	Valutazione del rischio e Valutazione di impatto per i trattamenti	Valutazione del rischio per i dati le infrastrutture informatiche
Approccio risk based	Adozione di misure di sicurezza in funzione della probabilità e gravità dei rischi	Adozione di misure di sicurezza in funzione della probabilità e gravità dei rischi
Sistema sanzionatorio	Sanzioni proporzionali alla gravità della violazione	Sanzioni proporzionali alla gravità della violazione
Approccio by-design by default	Applicato ai trattamenti	Applicato ai dati e alle infrastrutture informatiche
Obblighi di sorveglianza	Monitoraggio continuo dei trattamenti	Monitoraggio continuo della sicurezza dei dati e delle infrastrutture informatiche
Sensibilizzazione e formazione	In merito alla sicurezza dei trattamenti	In merito alla sicurezza dei dati e delle infrastrutture informatiche
Audit interni ed esterni	Verifiche periodiche degli adempimenti e della sicurezza dei trattamenti	Verifiche periodiche della sicurezza dei dati e delle infrastrutture informatiche

Verso un approccio integrato

- Comunicazione tra CISO e RDP
- Iniziative di formazione congiunte
- Collaborazione nelle attività di audit
- Coinvolgimento di CISO E RPD nella realizzazione di nuovi sistemi
- Ecosistema integrato

Grazie per l'attenzione

Per le domande: wooclap.com
e codice WSGARR24