



La compliance integrata dei sistemi GDPR, AI Act e NIS 2

***A cura di
Roberto Scavizzi
avvocato, docente universitario e
compliance consultant***

Roma, 31 marzo 2025



Modello Integrato di Compliance: GDPR, NIS2 e AI Act

Il panorama regolatorio europeo in materia di ***protezione dei dati, cybersicurezza e intelligenza artificiale*** si articola oggi attorno a ***tre pilastri fondamentali*** che, pur nascendo da esigenze distinte, convergono verso ***un obiettivo comune***: la creazione di un ecosistema digitale europeo sicuro, affidabile e conforme ai diritti fondamentali.

Il Regolamento (UE) 2016/679 (GDPR), applicato dal 25 maggio 2018, la Direttiva (UE) 2022/2555 (NIS2), recepita in Italia con il D. Lgs. 138/2024 in vigore dal 16 ottobre 2024, e il Regolamento (UE) 2024/1689 (AI Act), con applicazione progressiva fino al 2 agosto 2026, costituiscono ***il 'triumvirato' normativo che ogni organizzazione operante in Europa è chiamata ad osservare.***



Il modello di compliance integrato

Questi tre regolamenti non sono silos separati.

Le ***tre strutture organizzative*** si sovrappongono, si integrano e, in alcuni punti, si rinforzano reciprocamente.

Comprendere le loro differenze strutturali — nei tipi di rischio trattati, nelle metodologie di valutazione, negli obblighi imposti e nelle strutture di governance richieste — ***è il primo passo per costruire un modello di compliance integrato*** che eviti duplicazioni, ottimizzi risorse e garantisca una copertura normativa completa



GDPR — Regolamento Generale sulla Protezione dei Dati

Il GDPR costituisce il fondamento della *privacy* nell'Unione Europea, disciplinando il trattamento dei dati personali da parte di titolari e responsabili del trattamento.

Il suo approccio è centrato sulla ***tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto al trattamento dei propri dati personali.***

I principi cardine **sono**: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; e responsabilizzazione (*accountability*).



GDPR: le tipologie di rischi

Il GDPR si concentra esclusivamente sui rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali.

Il concetto di ‘rischio’ **non** si esaurisce nella sola dimensione di sicurezza informatica — ossia nelle possibili violazioni o minacce tecniche — **ma** include, innanzitutto, ***ogni impatto negativo che un trattamento dei dati personali può avere sulla sfera personale, sociale ed economica dell'interessato.***



La valutazione dei rischi

- 1) **Metodologia di valutazione dei rischi 'ordinari' per tutti i trattamenti di dati**
- 2) **Valutazione d'Impatto sulla Protezione dei Dati (DPIA):** strumento centrale del GDPR per l'analisi preventiva del rischio elevato in relazione a specifici trattamenti di dati personali.

L'art. 35 del GDPR obbliga i titolari del trattamento a svolgere una DPIA quando un trattamento possa presentare **un rischio elevato**.

ES: Valutazione sistematica ed esaustiva di aspetti personali, inclusa la profilazione; Trattamento su larga scala di categorie particolari di dati (art. 9) o di dati relativi a condanne penali (art. 10) Monitoraggio sistematico e su vasta scala di aree accessibili al pubblico, etc



GDPR → obblighi principali

Obbligo	Riferimento normativo	Descrizione
Registro dei trattamenti	Art. 30	Documentazione di tutti i trattamenti svolti
Nomina DPO	Artt. 37-39	Obbligatoria per PA, amplissimo campo di applicazione per i privati
Privacy by design e by default	Art. 25	Integrazione della privacy fin dalla progettazione
DPIA	Art. 35	Valutazione d'impatto per trattamenti ad alto rischio
Notifica data breach	Artt. 33-34	Entro 72 ore all'Autorità di controllo; agli interessati se rischio elevato
Gestione dei diritti degli interessati	Artt. 15-22	Accesso, rettifica, cancellazione, portabilità, opposizione, limitazione
Designazione responsabili del trattamento	Art. 28	Contratto o altro atto giuridico con clausole specifiche



Organigramma *privacy*

La struttura organizzativa richiesta dal GDPR prevede i seguenti ruoli:

- ***Titolare del trattamento***: centro decisionale; determina finalità e mezzi del trattamento; è responsabile della conformità e deve dimostrare accountability
- ***Responsabile del trattamento (Processor)***: tratta dati per conto del titolare in base a istruzioni documentate
- ***Sub-responsabile del trattamento***: terze parti designate dal responsabile, vincolate alle stesse garanzie
- ***Autorizzati al trattamento***: dipendenti e collaboratori che operano sotto la diretta autorità del titolare o del responsabile
- ***Data Protection Officer (DPO)***: organo di staff indipendente; fornisce consulenza, monitora la conformità, funge da punto di contatto con il Garante; la sua nomina è obbligatoria in determinati casi



Le sanzioni

Il GDPR prevede **due livelli** di sanzione amministrativa:

- **Livello 1**: fino a 10 milioni di euro o il 2% del fatturato annuo mondiale, per violazioni organizzative e procedurali (es. mancata designazione del DPO, carenze nel registro dei trattamenti)
- **Livello 2**: fino a 20 milioni di euro o il 4% del fatturato annuo mondiale, per violazioni dei principi fondamentali, dei diritti degli interessati, dei trasferimenti internazionali illeciti



NIS2 — Direttiva sulla Sicurezza delle Reti e dei Sistemi Informativi

La **Direttiva NIS2** (Direttiva UE 2022/2555), recepita in Italia con il D. Lgs. 138/2024, abroga la precedente NIS1 (Direttiva UE 2016/1148) e introduce ***un quadro più ampio e stringente per la cybersicurezza delle reti e dei sistemi informativi.***

La NIS2 estende significativamente l'ambito di applicazione rispetto alla NIS1, coinvolgendo ***oltre 80 tipologie di soggetti***, raggruppate in 18 settori, di cui 11 altamente critici e 7 critici.

I soggetti sono classificati in due categorie: ***(i) essenziali*** e ***(ii) importanti***, con obblighi differenziati in ragione della loro criticità per l'economia e la società.



Focus della NIS 2

Il *focus* della NIS2 è principalmente sul ***rischio informatico (cyber risk)*** e sulla ***resilienza operativa*** delle ***infrastrutture critiche***.

A differenza di altre normative, la NIS 2 adotta un approccio '***all-hazards***' (multirischio) focalizzato sulla ***sicurezza di rete e dei sistemi informativi***, ***estendendosi anche alla sicurezza fisica di tali sistemi***.

Pertanto ***l'approccio è multi-rischio*** → le misure di sicurezza **devono** essere commisurate al rischio posto al sistema informativo e di rete.



Approccio multi-rischio

L'approccio è multi-rischio e, pertanto, le misure di sicurezza *devono essere commisurate al rischio relativo sistema informativo e di rete*, considerando almeno i seguenti ambiti:

- Politiche di analisi dei rischi e sicurezza dei sistemi informatici
- Gestione degli incidenti
- Continuità operativa e gestione delle crisi (BCP/BCM)
- Sicurezza della catena di approvvigionamento (*supply chain security*)
- Sicurezza nell'acquisizione, nello sviluppo e nella manutenzione dei sistemi
- Gestione e divulgazione delle vulnerabilità
- Pratiche di igiene informatica di base e formazione
- Politiche e procedure relative all'uso della crittografia
- Sicurezza delle risorse umane, politiche di controllo degli accessi e gestione degli *asset*
- Uso di soluzioni di autenticazione multi-fattore

A differenza del GDPR, la NIS2 non si concentra sui rischi per le persone fisiche derivanti dal trattamento dei loro dati personali, bensi sui **rischi sistemici per le infrastrutture e i servizi essenziali**.



Approccio proporzionato

La NIS2 adotta ***un approccio proporzionato e basato sul rischio (risk-based approach)***, richiedendo ai soggetti di adottare ***misure tecniche, operative e organizzative appropriate*** per gestire i rischi per la sicurezza delle reti e dei sistemi informativi.

Il ***processo di valutazione*** si articola come segue:

- ***Risk assessment continuativo***: identificazione, analisi e trattamento dei rischi *cyber* con *framework* quali ISO 27005, NIST CSF o il *Framework Nazionale per la Cybersicurezza (FNCS)* elaborato dall'ACN
- ***Business Continuity Planning (BCP)***: verifica della resilienza operativa e capacità di ripristino
- ***Supply chain risk assessment***: valutazione dei rischi connessi alla catena dei fornitori
- ***Notifica degli incidenti in tre fasi***: pre-notifica entro 24 ore, notifica entro 72 ore, relazione finale entro un mese



Gli obblighi

Obbligo	Descrizione
Registrazione presso ACN	Entro il 31 marzo 2025 per i soggetti già identificati
Misure di gestione del rischio cyber	Implementazione in almeno 10 ambiti con approccio multi-rischio
Notifica incidenti significativi	Pre-notifica (24h), notifica (72h), relazione finale (1 mese)
Formazione organi direttivi	I vertici aziendali devono seguire formazione specifica in materia di <i>cyber</i>
Responsabilità degli organi di gestione	Gli organi di vertice sono responsabili dell'implementazione delle misure e possono essere sanzionati
Sicurezza della supply chain	Valutazione e gestione dei rischi <i>cyber</i> dei fornitori
Divulgazione coordinata delle vulnerabilità (CVD)	Segnalazione responsabile delle vulnerabilità scoperte
Uso di crittografia e MFA	Implementazione di soluzioni di autenticazione robusta e cifratura



Livello istituzionale/nazionale

- ***ACN (Agenzia per la Cybersicurezza Nazionale)***: Autorità Nazionale Competente NIS e Punto di Contatto Unico NIS
- ***CSIRT Italia***: gestione operativa degli incidenti e coordinamento
- ***Ministero della Difesa***: Autorità Nazionale per la gestione delle crisi informatiche
- ***N. 9 Autorità di Settore ministeriali***: collaborano con ACN per la vigilanza nei rispettivi settori
- ***EU-CyCLONe***: rete europea per la gestione coordinata delle crisi transfrontaliere



Livello organizzativo aziendale

- ***Organi di gestione/CdA***: approvazione delle misure di sicurezza, responsabilità diretta, formazione obbligatoria
- ***CISO (Chief Information Security Officer)***: implementazione e supervisione delle misure di sicurezza cyber
- ***Responsabile della gestione degli incidenti***: coordinamento della notifica e della risposta
- ***Referenti per la sicurezza della supply chain***: gestione dei rischi connessi ai fornitori



Le sanzioni

Le sanzioni previste dalla NIS2 e recepite nel D. Lgs. 138/2024 sono:

- **Soggetti essenziali**: fino a 10.000.000 € o al 2% del fatturato mondiale annuo
- **Soggetti importanti**: fino a 7.000.000 € o all'1,4% del fatturato mondiale annuo

Possibile sospensione dall'esercizio delle funzioni manageriali per i responsabili in caso di gravi e reiterate violazioni



L'AI Act

Il Regolamento (UE) 2024/1689 (AI Act) costituisce ***il primo quadro normativo organico al mondo sull'intelligenza artificiale*** e introduce un approccio basato sul rischio per la regolamentazione dei sistemi di IA.

Il regolamento classifica ogni sistema di IA in **quattro categorie di rischio** e applica obblighi proporzionati alla categoria di appartenenza, bilanciando l'innovazione tecnologica con la tutela dei diritti fondamentali.

L'applicazione è progressiva: dal 2 agosto 2025 per le autorità nazionali competenti, dal 2 febbraio 2026 per i sistemi GPAI, dal 2 agosto 2026 per i sistemi ad alto rischio.



AI Act → le tipologie di 'rischio'

L'AI Act introduce **una tassonomia del rischio originale e specifica per i sistemi di IA**, che non trova equivalenti diretti nel GDPR o nella NIS2. Vediamola insieme:

1. **Rischio inaccettabile (vietato)**: sistemi che pongono una minaccia inaccettabile ai diritti fondamentali; sono completamente vietati (es. sistemi di *social scoring* governativo, manipolazione comportamentale subliminale, riconoscimento facciale in tempo reale in spazi pubblici a fini di *law enforcement*, con eccezioni tassative)
2. **Alto rischio**: sistemi impiegati in settori sensibili (infrastrutture critiche, istruzione, occupazione, accesso a servizi essenziali, applicazione della legge, gestione della migrazione, amministrazione della giustizia, biometria); non vietati ma soggetti a obblighi stringenti di conformità *ex ante*
3. **Rischio limitato**: sistemi soggetti a obblighi di trasparenza (es. *chatbot* ove l'utente deve essere informato che sta interagendo con un sistema automatico)
4. **Rischio minimo o nullo**: applicazioni di IA a basso impatto (es. filtri *antispam*, videogiochi con IA), per le quali non sono previsti obblighi specifici, salvo il rispetto dei principi etici.



AI Act → le tipologie di ‘rischio’

I rischi specifici contemplati dall’AI Act includono:

- danni alla salute e alla sicurezza fisica
- violazioni dei diritti fondamentali
- bias algoritmici
- mancanza di trasparenza e di spiegabilità
- assenza di supervisione umana
- vulnerabilità informatiche nei sistemi di IA
- impatti sui diritti dei lavoratori
- discriminazioni automatizzate

Etc.



Metodologia di Valutazione del Rischio [1/2]

Conformity Assessment (Valutazione di Conformità) per sistemi ad alto rischio:

- **deve** essere eseguita prima dell'immissione sul mercato o della messa in servizio;
- **verifica** la sussistenza di tutti i requisiti obbligatori. Nello specifico si verifica il sistema di gestione del rischio, la qualità dei dati di addestramento, la documentazione tecnica, la trasparenza e la fornitura di informazioni agli utenti, la supervisione umana, l'accuratezza/robustezza/*cybersecurity*;
- **può** essere condotta internamente (auto-valutazione) o tramite organismi notificati (*third-party assessment*) per alcune categorie specifiche;
- **richiede** marcatura CE e la **registrazione** nel database europeo dei sistemi ad alto rischio.



Metodologia di valutazione del rischio [2/2]

FRIA (*Fundamental Rights Impact Assessment*). Si tratta di una **valutazione d'Impatto sui diritti fondamentali** che:

- **è stata introdotta dall'art. 27 dell'AI Act**. Essa è obbligatoria per specifici *deployer* (es. enti pubblici) che utilizzano sistemi ad alto rischio;
- **ha un ambito di applicazione più ampio della DPIA**. Detta metodologia valuta l'impatto del sistema di IA su tutti i diritti fondamentali della persona, non solo dal punto di vista privacy;
- **non sostituisce la DPIA del GDPR**. Invero le due valutazioni coesistono e si integrano;
- **include le seguenti attività**: descrizione del sistema, popolazione interessata, periodo di utilizzo, valutazione dei rischi per diritti specifici, misure di mitigazione e piano di monitoraggio *post-deployment*.



Sistema di gestione del rischio (art. 9 AI Act)

Si tratta di un ***processo iterativo continuo*** durante tutto il ciclo di vita del sistema di IA.

Di seguito le fasi che caratterizzano detto processo.

- a. identificazione dei rischi noti e ragionevolmente prevedibili***
- b. analisi dei rischi***
- c. stima e valutazione***
- d. adozione delle misure di gestione***
- e. monitoraggio***
- f. azioni correttive e miglioramento***

La norma impone **una determinata documentazione tecnica e l'approntamento di registri automatici (*logs*) obbligatori per la tracciabilità delle attività poste in essere con il sistema di IA.**



Obblighi per i Fornitori (*Providers*) di sistemi ad alto rischio:

Obbligo	AI Act	Descrizione
Sistema di gestione del rischio	Art. 9	Processo continuo durante tutto il ciclo di vita
Qualità dei dati	Art. 10	<i>Dataset</i> di addestramento adeguati, rappresentativi, privi di <i>bias</i>
Documentazione tecnica	Art. 11	Documento completo prima dell'immissione sul mercato
Registro automatico degli eventi (<i>logs</i>)	Art. 12	Tracciabilità delle operazioni del sistema
Trasparenza e istruzioni d'uso	Art. 13	Informazioni chiare per i <i>deployer</i>
Supervisione umana	Art. 14	Misure per consentire intervento umano
Accuratezza, robustezza, <i>cybersecurity</i>	Art. 15	<i>Standard</i> tecnici da rispettare
Sistema di gestione della qualità	Art. 17	QMS documentato e approvato
Valutazione di conformità e marcatura CE	Artt. 43 e 48	Prima dell'immissione sul mercato
Registrazione nel <i>database</i> europeo	Art. 49	Obbligatoria per sistemi ad alto rischio
Notifica incidenti gravi	Art. 73	Senza ingiustificato ritardo alle autorità competenti



Obblighi per gli Utilizzatori (*Deployer*) di sistemi ad alto rischio

- Utilizzo conforme alle istruzioni d'uso del fornitore
- Sorveglianza umana affidata a persone con competenze adeguate
- Controllo sulla pertinenza e rappresentatività dei dati di *input*
- Monitoraggio del funzionamento e segnalazioni al fornitore ed alle autorità
- Conservazione dei *log* automatici per almeno 6 mesi
- Informazione preventiva dei lavoratori
- FRIA (per enti pubblici e assimilati)



I tre livelli della *governance*

La struttura di *governance* prevista dall'AI Act opera su **tre livelli**:

- *Livello europeo*
- *Livello nazionale*
- *Livello organizzativo aziendale*



Livello europeo

- **AI Office (Ufficio per l'IA)** → istituito all'interno della Commissione Europea. Esso supervisiona i modelli GPAI e le modalità di attuazione dell'AI Act negli Stati membri.
- **Comitato Europeo per l'IA** → composto da rappresentanti degli Stati membri. Ha funzione consultiva e di coordinamento.
- **Gruppo di Esperti Scientifici** → composto da esperti indipendenti per fornire un supporto tecnico-scientifico.
- **Forum Consultivo** → rappresentanza diversificata di *stakeholder* commerciali e non commerciali.



Livello nazionale

- **Le Autorità di Vigilanza del Mercato** → vigilano sulla conformità dei sistemi di IA immessi sul mercato; possono avviare indagini e imporre sanzioni
- **Le Autorità di Notifica** → esse designano e controllano gli Organismi Notificati
- **Gli Organismi notificati (*Notified Bodies*)** → terze parti indipendenti per la valutazione di conformità dei sistemi ad alto rischio

In Italia il quadro istituzionale è ancora in definizione.

Mentre l'ACN è indicata come autorità di vigilanza del mercato, l'AGCM mantiene le sue competenze per la tutela del mercato e dei consumatori anche in relazione all'utilizzo dei sistemi di intelligenza artificiale (vedi casi di istruttoria nei confronti di Meta AI di WhatsApp).



Livello organizzativo aziendale

- ***AI Governance Officer*** / Responsabile AI → ad essi spetta la supervisione del ciclo di vita dei sistemi di IA e della conformità all'AI Act
- **Team tecnico AI** → si cura della manutenzione del sistema di gestione del rischio, della documentazione tecnica e dei log
- **DPO** → il suo ruolo comprende anche la supervisione delle interazioni AI-GDPR, DPIA e FRIA applicate in coordinazione tra loro.
- ***Compliance officer*** → si occupa dell'armonizzazione organizzativo giuridica dei sistemi, dei processi e delle funzioni



Le sanzioni

Le sanzioni previste dall'art. 99 del Regolamento (UE) 2024/1689:

- **Violazioni di sistemi vietati (rischio inaccettabile)** → fino a 35.000.000 € o il 7% del fatturato annuo mondiale
- **Violazioni degli obblighi per sistemi ad alto rischio** → fino a 15.000.000 € o il 3% del fatturato annuo mondiale
- **Informazioni false o fuorvianti a organismi notificati o autorità** → fino a 7.500.000 € o l'1% del fatturato annuo mondiale



Analisi Comparativa

Le differenze 'chiave'



Tipologie di rischio a confronto

Dimensione	GDPR	NIS2	AI Act
Oggetto del rischio	Diritti e libertà delle persone fisiche nei trattamenti di dati personali	Sicurezza reti, sistemi informativi e servizi essenziali	Sicurezza, diritti fondamentali, impatti sociali dei sistemi di IA
Natura del danno	Personale (<i>privacy</i> , discriminazione, danno reputazionale, perdita controllo dati)	Sistemico/infrastrutturale (interruzione servizi, instabilità economica, sicurezza nazionale)	Pluridimensionale (salute, sicurezza fisica, bias, discriminazione algoritmica, mancanza trasparenza)
Soggetto a rischio	Persone fisiche (interessati)	Sistemi e reti di organizzazioni critiche	Persone fisiche, società, mercato
Orizzonte temporale	Pre-trattamento (DPIA) + continuo	Continuo (<i>risk assessment</i>) + <i>post</i> -incidente	Pre-immissione mercato (conformità) + continuo (ciclo di vita)
Rischio residuo	Consultazione preventiva Garante se non mitigabile	Adozione misure proporzionate; notifica incidenti	Documentazione e supervisione umana come guardrail

Metodologie di valutazione del rischio a confronto

Aspetto	GDPR (DPIA)	NIS2 (<i>Risk Assessment cyber</i>)	AI Act (<i>Conformity Assessment + FRIA</i>)
Strumento principale	DPIA (<i>Data Protection Impact Assessment</i>)	<i>Risk Assessment</i> multi-rischio continuo	Conformity Assessment + FRIA
Quando si esegue	Prima del trattamento; aggiornamento continuo	Continuativamente; aggiornamento periodico	Prima dell'immissione sul mercato; <i>post-market monitoring</i>
Chi la esegue	Titolare (con supporto DPO)	Soggetto essenziale/importante (con CISO)	Provider (con AI <i>Governance Officer</i> ; terzo per alcuni casi)
Ambito	Rischi per dati personali	Rischi <i>cyber</i> per reti e sistemi	Rischi per salute, sicurezza, diritti fondamentali da sistemi IA
Obbligatorietà	Condizionata (art. 35 GDPR: trattamenti ad alto rischio)	Generale per tutti i soggetti in ambito	Generale per sistemi ad alto rischio; FRIA per deployer pubblici
Output	<i>Report DPIA</i> ; misure di mitigazione; eventuale consultazione Garante	Registro rischi; piano di trattamento; BCP	Documentazione tecnica; marcatura CE; database europeo; <i>FRIA report</i>
Framework di riferimento	Linee guida EDPB (WP248); ISO 29134	ISO 27005; NIST CSF; FNCS (ACN)	<i>Standard</i> armonizzati CEN/CENELEC; ISO/IEC 42001
Convergenza possibile	DPIA ampliabile a processi IA	<i>Risk assessment</i> integrabile con GDPR e AI Act	FRIA può inglobare elementi DPIA

Obblighi e incombenze a confronto

Obbligo/Incombenza	GDPR	NIS2	AI Act
Registro/Documentazione	<i>Registro dei trattamenti</i> (RoPA)	Registro rischi, piani BCP, report incidenti	Documentazione tecnica, logs, registri conformità
Notifica incidenti	<i>Data breach</i> entro 72h al Garante; agli interessati se rischio elevato	Pre-notifica 24h + notifica 72h + relazione finale 1 mese all'ACN/CSIRT	Notifica incidenti gravi art. 73 (senza ingiustificato ritardo)
Valutazione preventiva	DPIA (se rischio elevato)	<i>Risk assessment</i> continuo	<i>Conformity assessment</i> ; FRIA
Supervisione esterna	Garante per la <i>privacy</i> ; eventuale <i>audit</i>	ACN, CSIRT, Autorità di settore; audit e ispezioni	Autorità di Vigilanza del Mercato, Organismi Notificati; <i>AI Office</i>
Formazione obbligatoria	Non esplicitamente prevista come obbligo formale	Organi di gestione obbligati a seguire formazione <i>cyber</i>	Supervisione umana da parte di persone competenti
Trasparenza verso terzi	Informativa agli interessati; diritti di accesso, portabilità, cancellazione	Divulgazione coordinata delle vulnerabilità (CVD)	Avviso agli utenti finali per sistemi rischio limitato; istruzioni d'uso per sistemi alto rischio
Accountability	Titolare dimostra conformità; DPO come garante interno	Organi di gestione responsabili; CISO operativo	<i>Provider</i> responsabile ciclo di vita; <i>deployer</i> responsabile utilizzo
Sanzioni massime	20M€ o 4% fatturato	10M€ o 2% fatturato (essenziali)	35M€ o 7% fatturato (sistemi vietati)

Strutture organizzative (organigrammi) a confronto

Livello	GDPR	NIS2	AI Act
Figura apicale aziendale	Titolare del trattamento (CdA/CEO)	Organo di gestione (responsabile)	Provider/Deployer (CdA/CEO)
Figura tecnica operativa	Responsabile del trattamento / <i>Team privacy</i>	CISO (<i>Chief Information Security Officer</i>)	<i>AI Governance Officer / AI Engineer</i>
Figura di supervisione interna	DPO (obbligatorio in certi casi; organo di staff)	Nessuna figura analoga al DPO; ruolo distribuito	Non prevista figura dedicata obbligatoria; DPO esteso
Autorità nazionale di vigilanza	Garante <i>Privacy</i> (GPDP)	ACN + 9 Autorità di settore	Autorità di Vigilanza del Mercato (in definizione in IT)
Autorità europea	EDPB	ENISA; EU-CyCLONe	<i>AI Office</i> ; Comitato Europeo per l'IA
Terze parti obbligatorie	Organismi di certificazione (facoltativi)	Nessuna terza parte obbligatoria (<i>audit</i> su richiesta ACN)	Organismi Notificati (per alcune categorie alto rischio)



I punti di incontro e di sovrapposizione dei tre Regolamenti



La condivisione di alcuni principi

I tre regolamenti condividono ***un insieme di principi fondamentali che costituiscono il terreno fertile per un approccio integrato:***

- **Accountability** → ogni organizzazione deve dimostrare attivamente la propria conformità, non limitarsi ad affermarla
- **Privacy/Security/Safety by Design** → le misure di tutela devono essere integrate fin dalla fase progettuale dei processi, sistemi e prodotti
- **Proporzionalità al rischio** → gli obblighi sono calibrati sull'entità e la natura del rischio, non sull'organizzazione in senso assoluto
- **Trasparenza** → verso gli interessati (GDPR), verso le autorità competenti (NIS2), verso gli utenti e il pubblico (AI Act)



Aree di sovrapposizione critica [1/2]

La notifica degli incidenti

Quando un *data breach* (GDPR) deriva da un attacco cibernetico su infrastruttura critica (NIS2) che coinvolge un sistema di IA ad alto rischio (AI Act), si innescano **tre diversi obblighi di notifica con tempistiche e destinatari parzialmente differenti**:

- **GDPR** → entro 72h al Garante (Artt. 33-34)
- **NIS2** → pre-notifica entro 24h + notifica entro 72h + relazione finale entro 1 mese all'ACN/CSIRT
- **AI Act** → notifica incidenti gravi art. 73 all'Autorità di Vigilanza del Mercato (senza ingiustificato ritardo; 15 giorni per morte/lesioni gravi)



Aree di sovrapposizione critica [2/2]

La DPIA e la FRIA

La **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)** e la **Valutazione d'Impatto sui Diritti Fondamentali (FRIA)** hanno *metodologie analoghe ma ambiti distinti*.

Quando un sistema di IA tratta dati personali, entrambe le valutazioni sono richieste. Tuttavia, gli orientamenti emergenti suggeriscono la possibilità di una valutazione integrata che soddisfi entrambi i requisiti, evitando duplicazioni.



Aree di sovrapposizione critica [1/2]

La sicurezza dei sistemi

I requisiti di *cybersecurity* prescritti dall'art. 15 dell'AI Act (per sistemi ad alto rischio) spesso si sovrappongono con le misure di sicurezza richieste dalla NIS2 per le organizzazioni che rientrano nel medesimo campo di applicazione.

Per le organizzazioni che sono tenute ad applicare le dette normative, i **controlli possono essere progettati per soddisfare simultaneamente i requisiti delle predette prescrizioni.**



Aree di sovrapposizione critica [1/2]

Il ruolo del DPO

Le incombenze del DPO e del *compliance officer*, tradizionalmente centrate per il primo sulla protezione dei dati personali e per il secondo su progettazione e monitoraggio integrato dei sistemi cogenti e volontari, si stanno espandendo al fine di avere figure in grado di eseguire gli obblighi e determinate attività previste dalla NIS2 (interfaccia con il CISO) e dall'AI Act (es: coordinamento DPIA/FRIA, supervisione dell'AI governance).



Il Modello integrato di *compliance*

Un modello integrato di compliance per GDPR, NIS2 e AI Act potrebbe essere progettato su **quattro principi metodologici di base**:

- **Unicità del registro dei rischi** → un unico strumento che cataloga tutti i rischi — di privacy, cyber e algoritmici — in un registro consolidato, evitando silos informativi e duplicazioni documentali
- **Policy trasversali** → invece di politiche separate per ciascuna normativa, adottare policy unificate che coprano contemporaneamente i requisiti di tutte e tre le normative (es. una politica di gestione degli incidenti che soddisfi GDPR art. 33, NIS2 art. 23 e AI Act art. 73)
- **Struttura organizzativa convergente** → definire ruoli e responsabilità in modo che le figure chiave (DPO, CISO, *AI Governance Officer*, *compliance officer*) collaborino in modo strutturato, evitando sovrapposizioni e lacune
- **Audit trail unificato** → mantenere un'unica base documentale di evidenze di conformità che supporti simultaneamente tutti gli audit (*privacy audit*, *cyber audit*, *AI conformity assessment*)



GRAZIE PER L'ATTENZIONE