EVERSHEDS SUTHERLAND

IL GDPR NELL'AMBITO GRC E COMPLIANCE INTEGRATA

Principi comuni, convergenze normative e best practice per una gestione efficiente

Roma, 25 novembre 2025

Avv. Massimo Maioletti

Partner - Head of Data Protection & Cybersecurity

ROPA

CISO

DPA

DMA

GDPR

CRA

ESG

GRC

DSA

AI

NIS2

DPIA

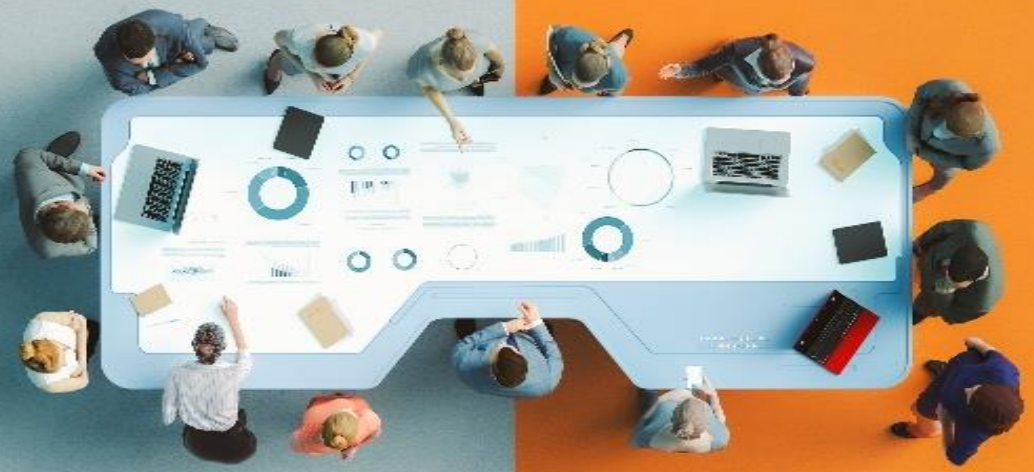
FRIA

DORA

DGA

Cosa si intende per GRC?

"Doing the right thing is the only way to do business"



DEFINIZIONE DI GRC

Governance, Risk and Compliance

GRC (Governance, Risk & Compliance) è un approccio integrato alla gestione aziendale che coordina tre pilastri fondamentali:

- **Governance**: sistema di regole, procedure e processi attraverso cui un'organizzazione è diretta e controllata. Sono chiaramente identificati i soggetti che prendono le decisioni e tutti conoscono il proprio ruolo e responsabilità e gli standard che ci si attende siano rispettati;
- **Risk Management**: Identificazione, valutazione e gestione dei rischi che potrebbero impedire il raggiungimento degli obiettivi aziendali;
- **Compliance**: Conformità alle leggi, regolamenti, standard e politiche interne applicabili.

Obiettivo del GRC: favorire trasparenza, coerenza e responsabilizzazione lungo l'intera catena operativa, ottimizzando performance, resilienza e uso delle risorse, riducendo rischi e costi.

Il concetto di GRC è stato introdotto dall'Open Compliance and Ethics Group (OCEG) nel 2002, per definire l'insieme integrato di capacità che consente a un'organizzazione di raggiungere la c.d. *Performance Principled* – ossia «*la capacità di conseguire in modo affidabile i propri obiettivi, affrontare l'incertezza e agire con integrità*».

NORMATIVE RILEVANTI PER IL MODELLO GRC

Panoramica delle principali normative che concorrono alla costruzione di un modello di GRC integrato

Quadro normativo di riferimento:

- GDPR (Regolamento UE 2016/679) - Protezione dei dati personali
- Statuto dei Lavoratori (Legge 300/1970)
- D.Lgs. 231/2001 - Responsabilità amministrativa degli enti
- AI Act (Regolamento UE 2024/1689) - Intelligenza artificiale
- Direttiva Whistleblowing (Direttiva UE 2019/1937)
- NIS 2 (Direttiva UE 2022/2555) - Sicurezza delle reti e dei sistemi informativi
- DORA (Regolamento UE 2022/2554) - Resilienza operativa digitale settore finanziario
- Cyber Resilience Act - Sicurezza dei prodotti digitali

Queste normative condividono principi comuni ed integrano requisiti e standard trasversali

È necessario un approccio integrato per l'adozione di un modello GRC robusto ed efficace.

PRINCIPI CHIAVE DI APPLICAZIONE TRASVERSALE

Principi normativi comuni per un modello GRC integrato

Risk-Based Approach
- Valutazione e prioritizzazione dei rischi
- Misure proporzionate al livello di rischio
- Monitoraggio continuo

Impostazione by Design e by Default
- Integrazione della compliance fin dalla progettazione
- Policy di sicurezza predefinite
- Principio di privacy/security by design

Selezione, gestione e controllo della catena di approvvigionamento
- Due diligence sui fornitori e partner
- Contratti con garanzie adeguate
- Audit e verifiche periodiche

Gestione degli incidenti
- Procedure di rilevamento degli incidenti e risposta
- Notifiche alle autorità competenti
- Registro degli incidenti e azioni correttive

Accountability
- Obbligo di dimostrare la conformità normativa
- Documentazione delle misure adottate
- Responsabilità diretta degli organi di governance

Il Digital Omnibus Package avrà un impatto sui modelli GRC?

CONVERGENZE NORMATIVE

Requisiti specifici comuni – Esempi

Adempimento	GDPR	NIS2	DORA	AI ACT	CRA
Gestione Data Breach/Incidenti di Sicurezza	Notifica entro 72h all'Autorità Garante (Art. 33-34)	Notifica incidenti significativi entro 72h (preallarme entro 24h) al CSIRT (Art. 23)	Notifica gravi incidenti ICT alle autorità competenti (Art.19)	Notifica incidenti gravi all'autorità di vigilanza del mercato immediatamente dopo aver accertato il nesso con il sistema di IA, e comunque entro 15 giorni dalla conoscenza (2 giorni se infrazione diffusa, 10 giorni in caso di decesso) (Art.73)	Notifica vulnerabilità attivamente sfruttata o incidente grave entro 72h (preallarme entro 24 h) al CSIRT ed all'ENISA.
Valutazioni dei rischi e Valutazioni d'Impatto	Risk Assessment e DPIA - Data Protection Impact Assessment (Art. 35)	Valutazione rischi posti alla sicurezza dei sistemi informatici e di rete (Art. 21)	Individuazione delle fonti di rischio relative alle TIC e valutazione delle minacce informatiche e vulnerabilità in materia di TIC (Art.8)	FRIA - Fundamental Rights Impact Assessment per AI ad alto rischio (Art. 27)	Valutazione dei rischi di cibersicurezza associati al prodotto con elementi digitali (Art.13)
Terze parti/outsourcing	Selezione, garanzie e clausole contrattuali per responsabili e subresponsabili del trattamento; audit (Art.28)	Requisiti di sicurezza nella supply chain; gestione rischio fornitori critici (art.24, c.1, lett.d) D.lgs 138/2024)	Governance del rischio ICT di terze parti; disposizioni contrattuali (artt.28 e 30)	Verifica che il sistema di IA sia conforme ai requisiti dell'AI Act; comprensione dei limiti e dei rischi del Sistema (art.13)	Controllo sulla conformità dei processi messi in atto dal fabbricante ai requisiti essenziali di cybersicurezza (art.6)

ACCOUNTABILITY E GOVERNANCE

Responsabilità degli organi di Governo

L'organo di amministrazione detiene la responsabilità ultima per garantire la conformità e la gestione dei rischi. Ciò implica: **definire e approvare politiche e procedure**, **allocare risorse adeguate**, **monitorare l'efficacia dei controlli** e **favorire una cultura aziendale orientata all'integrità, alla trasparenza e alla gestione proattiva del rischio.**

Per una Governance strutturata, è necessario:

1. Individuare e formalizzare ruoli e responsabilità

2. Assicurare il coordinamento tra funzioni aziendali, in particolare**:**

- DPO (Data Protection Officer)
- Legal/Compliance Officer
- HR
- CISO (Chief Information Security Officer)
- Organismo di Vigilanza 231
- Risk Manager
- Internal Audit

3. Adottare modelli organizzativi complementari e coordinati:

- Integrazione tra MOG 231, Privacy Framework, Policy Cybersecurity
- Procedure unificate e coerenti
- Reporting integrato al vertice aziendale

4. Garantire consapevolezza, cultura aziendale e formazione:

- Programmi di awareness per tutti i livelli
- Formazione specialistica per ruoli chiave

CASE STUDY

L'IT manager di una società nell'ambito del proprio programma di aggiornamento dei sistemi di sicurezza aziendali intende implementare autonomamente un **sistema di e-mail security anti-leakage** proposto da un fornitore esterno per proteggere informazioni aziendali riservate.

Il sistema sarà configurato per monitorare costantemente il traffico email dei dipendenti per **rilevare e-mail contenenti specifiche parole chiave eventualmente inviate verso indirizzi e-mail esterni alla Società**. In questi casi:

- Verrà generato un **alert per il Responsabile IT**, corredato da una **valutazione del rischio di esfiltrazione di informazioni sensibili**.
- L'IT informerà il **responsabile dell'area Legal**, che potrà decidere se **accedere alle e-mail** del dipendente coinvolto.
- Sulla base di quanto si apprenderà a seguito dell'accesso alle e-mail del dipendente, potranno essere adottati provvedimenti disciplinari di varia natura, inclusa la possibilità di licenziamento.

La Società **non dispone di policy o procedure interne** che regolino l'accesso alle e-mail dei dipendenti e **non ha informato il personale della possibilità e delle conseguenze di tale controllo e soprattutto non ha implementato un modello GRC**.

1. Quali sarebbero le principali criticità da considerare?

2. Quali sarebbero le principali funzioni aziendali che l'IT manager avrebbe dovuto coinvolgere?

CASE STUDY

Quali sono le principali criticità da considerare?

Overview delle principali criticità	
Criticità in ambito giuslavoristico (e possibile rilevanza anche sul piano penale)	**Monitoraggio lavoratori non conforme ad Art.4 Statuto dei Lavoratori** in caso di: • Mancanza di accordo sindacale/autorizzazione dell'Ispettorato del lavoro • Assenza di un'informativa sull'accesso ai sistemi informatici dati in uso ai dipendenti • Assenza di un'informativa relativa all'utilizzabilità die dati eventualmente raccolti a tutti i fini connessi al rapporto di lavoro **Potenziale violazione ad Art.8 Statuto dei Lavoratori**
Criticità in ambito privacy	**Trattamenti non conformi ai principi stabiliti dal GDPR** in caso di: • Mancato rispetto degli adempimenti giuslavoristici come condizione di liceità del trattamento • Mancata valutazione in termini di privacy by design e by default. • Mancato coinvolgimento del DPO/Privacy Officer. • Assenza di una procedura/policy interna sull'utilizzo degli strumenti informatici e posta elettronica. • Assenza di DPIA. • Mancanza di informativa ex art.13 GDPR. • Mancata valutazione del fornitore e mancata formalizzazione del suo ruolo come Responsabile ex art. 28.
Criticità Dlgs 231	**Possibile rilevanza dell'accesso ai contenuti della posta elettronica come fattispecie di reato informatico presupposto.***(Cass. Civ. Sez. Lav, R.G.N. 7632/2021 del 29.08.2025)

CASE STUDY

Quali sarebbero le principali funzioni aziendali che l'IT manager avrebbe dovuto coinvolgere?

- ✓ **Legal/HR**
- ✓ **Privacy officer/DPO**
- ✓ **Internal Audit**
- ✓ **CISO**
- ✓ **Odv**
- ✓ Nel caso in cui il tool integri sistemi di Intelligenza artificiale, l'eventuale **funzione IA**.

Chi, in assenza di un modello di gestione GRC, coordinerebbe le funzioni coinvolte e riporterebbe ai vertici aziendali?

Domande

Grazie per l’attenzione!

EVERSHEDS SUTHERLAND

IL GDPR NELL'AMBITO GRC E COMPLIANCE INTEGRATA

Avv. Massimo Maioletti
Partner - Head of Data Protection & Cybersecurity

massimomaioletti@eversheds-sutherland.it

eversheds-sutherland.it