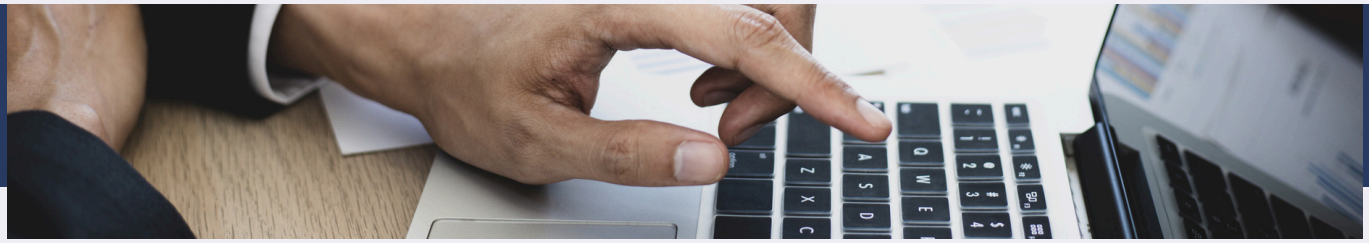
NUMERO 02 – GIUGNO 2026 NEWSLETTER TRIMESTRALE

FOCUS COMPLIANCE

AGGIORNAMENTI NORMATIVI E INDICAZIONI OPERATIVE PER LA GESTIONE DEI RISCHI AZIENDALI



Nota informativa

La presente newsletter viene trasmessa esclusivamente a imprese e organizzazioni che collaborano con COMPLIANCE SRL o che hanno richiesto di ricevere questo servizio informativo.

La comunicazione non ha finalità promozionali o di marketing, ma esclusivamente tecniche e informative, con l'obiettivo di condividere aggiornamenti normativi e indicazioni operative utili per le aziende.

Per tali ragioni la presente comunicazione rientra nelle attività informative rivolte a soggetti professionali e non richiede un consenso esplicito, fermo restando che chiunque non desideri più riceverla potrà richiederne in qualsiasi momento la cancellazione.

In questo numero

Compliance®
Smart Solutions

IL TEAM DI COMPLIANCE SRL
GIANLUCA ALDEGHERI

In questo secondo numero di **Focus Compliance** proseguiamo nella presentazione dei professionisti che ogni giorno contribuiscono alle attività di consulenza e supporto alle organizzazioni clienti.

Presentiamo **Gianluca Aldegheri**, laureato magistrale in ambito economico-aziendale, entrato a far parte di COMPLIANCE SRL nel 2023, quando aveva già scelto di affiancare il percorso universitario all'attività professionale. Un'esperienza che gli ha consentito di maturare competenze sul campo già prima del conseguimento della laurea magistrale, sviluppando fin da subito un approccio concreto e orientato alle esigenze delle imprese.

Sin dai primi mesi ha dimostrato **curiosità, capacità di apprendimento e voglia di mettersi in gioco**, qualità che gli hanno permesso di crescere rapidamente fino a gestire con autonomia numerosi progetti di consulenza.

Nel corso dell'ultimi anni ha approfondito i principali ambiti della compliance aziendale, partecipando a progetti relativi alla protezione dei dati personali (**GDPR**), alla Direttiva **NIS2**, ai sistemi di gestione e agli standard internazionali in materia di sicurezza delle informazioni e **organizzazione d'impresa**. Ha inoltre maturato esperienza nelle attività di **audit**, **assessment** e verifica documentale, collaborando con aziende appartenenti a settori tra loro molto diversi.

La crescita di Gianluca è stata accompagnata anche da una progressiva assunzione di **responsabilità** all'interno del team. Nel corso del 2025 ha iniziato a coordinare e affiancare i colleghi più giovani, contribuendo all'organizzazione delle attività e condividendo le competenze maturate nei diversi progetti di consulenza.

Ciò che maggiormente lo contraddistingue è l'approccio con cui affronta ogni progetto: **disponibilità all'ascolto, spirito collaborativo e capacità di instaurare un dialogo costruttivo con il cliente**. In un settore come quello della compliance, dove gli adempimenti possono essere percepiti come meri obblighi burocratici, riuscire a trasmetterne il valore organizzativo rappresenta una competenza fondamentale.

La crescita di Gianluca riflette uno dei principi che caratterizzano COMPLIANCE SRL: investire sulle persone, valorizzarne le competenze e accompagnarle in un percorso di sviluppo continuo, affinché possano offrire alle organizzazioni un supporto sempre più qualificato e orientato alla prevenzione dei rischi.

In questo numero affronteremo alcuni temi di particolare attualità, tra cui l'applicazione dell'AI Act nelle organizzazioni, le nuove indicazioni del Garante Privacy sulla gestione della posta elettronica aziendale, la trasparenza salariale, la gestione dei fornitori, il ruolo della formazione in ambito cybersecurity e Modello 231 e l'importanza del Codice Etico aziendale.

Con l'auspicio che anche questo secondo numero possa rappresentare uno strumento utile per le vostre attività, vi auguriamo buona lettura.

Daniel Zisa
Founder – COMPLIANCE SRL

Intelligenza artificiale e AI Act: da tema innovativo a tema di Compliance

L'intelligenza artificiale è ormai entrata nella quotidianità di molte organizzazioni. Strumenti come ChatGPT, Microsoft Copilot e altre soluzioni basate su IA vengono sempre più frequentemente utilizzati per attività di ricerca, redazione di documenti, analisi dei dati e automazione dei processi aziendali.

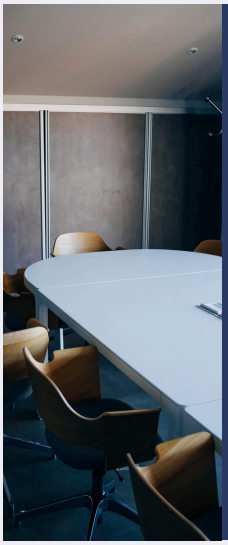
Parallelamente alla diffusione di queste tecnologie, l'Unione Europea ha introdotto il primo **quadro normativo** organico dedicato all'intelligenza artificiale: il cosiddetto **AI Act**, che mira a garantire uno sviluppo e un utilizzo dei sistemi di IA **sicuro, trasparente e rispettoso dei diritti fondamentali.**

Per molte aziende il tema non riguarda più soltanto l'innovazione tecnologica, ma diventa un vero e proprio argomento di **compliance aziendale**. L'utilizzo di strumenti di intelligenza artificiale può infatti comportare implicazioni in materia di protezione dei dati personali, sicurezza delle informazioni, proprietà intellettuale, gestione dei processi decisionali e responsabilità organizzativa.

L'intelligenza artificiale rappresenta senza dubbio un'opportunità per migliorare efficienza e produttività, ma richiede anche nuove forme di controllo e consapevolezza da parte delle organizzazioni che intendono utilizzarla in modo responsabile, per evitare, anche inconsapevolmente, di incorrere in reati.

Particolare attenzione deve essere prestata ai dati inseriti all'interno di tali strumenti. Informazioni aziendali riservate, dati personali o documentazione interna potrebbero infatti essere trattati da piattaforme esterne senza che gli utenti siano pienamente consapevoli delle conseguenze. Diventa così fondamentale limitare l'uso di dati sensibili allo stretto necessario e, se necessario, **anonimizzare** i dati inseriti quando possibile.

Per questo motivo sempre più aziende stanno iniziando a disciplinare l'utilizzo dell'IA attraverso **policy interne, attività di formazione o alfabetizzazione e specifiche procedure operative**, con l'obiettivo di garantire un utilizzo consapevole e coerente con il proprio sistema di governance.



Cosa verificare in azienda

- Verificare se dipendenti e collaboratori utilizzano strumenti di intelligenza artificiale nello svolgimento delle attività lavorative.
- Valutare quali dati aziendali o personali vengono inseriti nei sistemi di IA.
- Verificare se i sistemi di IA siano sicuri e affidabili nel loro utilizzo.
- Definire regole interne per l'utilizzo degli strumenti di intelligenza artificiale.
- Pianificare attività di formazione e sensibilizzazione sul corretto utilizzo dell'IA.
- Individuare figure o funzioni aziendali incaricate di monitorare l'utilizzo delle nuove tecnologie.

GDPR e gestione della mail aziendale: nuove indicazioni del Garante Privacy

La gestione degli strumenti informatici aziendali, e in particolare della **posta elettronica** assegnata ai dipendenti, rappresenta un tema rilevante per le imprese sia sotto il profilo organizzativo sia in materia di protezione dei dati personali.

Con un recente **provvedimento del marzo 2026**, il Garante per la protezione dei dati personali è tornato a occuparsi della gestione delle caselle e-mail aziendali individuali e dei documenti conservati nei dispositivi aziendali, con particolare attenzione alla fase di **cessazione del rapporto di lavoro** e all'esercizio del diritto di accesso da parte dell'ex dipendente.

Il Garante ha chiarito che le comunicazioni contenute in una casella e-mail aziendale individuale possono contenere dati personali riferiti al lavoratore anche quando riguardano l'attività professionale. Di conseguenza, non è possibile escludere automaticamente dall'**accesso le e-mail** solo perché considerate di natura lavorativa o aziendale.

Questo non significa che l'azienda debba consegnare indistintamente tutti i contenuti presenti nella casella di posta. Eventuali limitazioni devono però essere fondate su ragioni specifiche, documentate e verificabili, ad esempio per tutelare diritti di terzi, segreti aziendali o informazioni effettivamente riservate.

Il provvedimento richiama inoltre l'attenzione sulla conservazione delle e-mail aziendali. La posta elettronica **non dovrebbe trasformarsi in un archivio permanente dell'impresa**, poiché una conservazione eccessiva di messaggi, allegati e documenti può risultare non coerente con i principi di minimizzazione e limitazione della conservazione previsti dal GDPR.

Per le aziende diventa quindi importante adottare regole chiare sull'utilizzo della posta elettronica, sulla conservazione dei messaggi e sulle modalità da seguire in caso di cessazione del rapporto di lavoro.

Una corretta regolamentazione interna consente di ridurre il rischio di contestazioni, tutelare il patrimonio informativo aziendale e garantire, al tempo stesso, il rispetto dei diritti dei lavoratori.

Cosa verificare in azienda

- Verificare la presenza di una policy aggiornata sull'utilizzo di posta elettronica, PC aziendali e strumenti informatici.
- Definire regole chiare per la gestione delle e-mail in caso di cessazione del rapporto di lavoro.
- Prevedere procedure interne per la gestione delle richieste di accesso ai dati personali da parte di dipendenti ed ex dipendenti.
- Evitare che la posta elettronica diventi l'archivio principale e permanente della documentazione aziendale.
- Verificare i tempi di conservazione di e-mail, backup e metadati.
- Aggiornare informative privacy, regolamenti interni e istruzioni operative rivolte al personale.

Trasparenza salariale: nuovi obblighi per le aziende

La parità retributiva tra uomini e donne rappresenta da tempo un principio fondamentale dell'ordinamento europeo. Con la recente introduzione delle **nuove disposizioni in materia di trasparenza salariale**, le aziende sono chiamate a prestare maggiore attenzione ai propri processi di selezione, alle politiche retributive e ai criteri utilizzati per la gestione del personale.

La normativa mira a rafforzare la trasparenza nelle decisioni che riguardano retribuzioni e progressioni economiche, consentendo ai lavoratori di comprendere meglio i criteri adottati dall'organizzazione e **riducendo il rischio di disparità non giustificate**.

Tra le principali novità vi è l'**obbligo di fornire ai candidati informazioni** sulla retribuzione iniziale prevista o sulla relativa fascia retributiva già nelle fasi iniziali del processo di selezione.

Parallelamente, ai datori di lavoro viene preclusa la possibilità di richiedere informazioni sulle retribuzioni percepite nei precedenti rapporti di lavoro.

Per le organizzazioni di maggiori dimensioni assumono inoltre particolare rilievo gli obblighi informativi legati alle richieste dei lavoratori e alla **disponibilità di dati aggregati** relativi ai livelli retributivi.

La trasparenza salariale non deve essere vista esclusivamente come un nuovo adempimento normativo, ma anche come un'**opportunità per verificare la coerenza dei sistemi di inquadramento**, delle politiche HR e dei criteri utilizzati per la determinazione delle retribuzioni.

Un approccio preventivo consente alle aziende di prepararsi correttamente ai nuovi obblighi, riducendo il rischio di contestazioni e rafforzando la trasparenza interna.

Cosa verificare in azienda

- Verificare che annunci di lavoro e processi di selezione riportino la la fascia retributiva prevista.
- Accertare che durante i colloqui non vengano richieste informazioni sulle precedenti retribuzioni dei candidati.
- Verificare se l'azienda supera le soglie dimensionali previste dalla normativa e valutare i relativi adempimenti.
- Valutare la presenza di criteri oggettivi e documentati per determinare retribuzioni e progressioni economiche.
- Aggiornare, ove necessario, procedure HR, policy interne, job description e sistemi di classificazione del personale.
- Sensibilizzare le funzioni HR e i responsabili coinvolti nei processi di selezione e gestione del personale.

Fornitori critici: perchè la loro gestione è diventata un obbligo di compliance

Negli ultimi anni numerose violazioni informatiche, interruzioni di servizio o criticità operative non sono state causate direttamente dall'azienda interessata, ma da **fornitori esterni** coinvolti in attività rilevanti: servizi informatici, cloud, software, manutenzioni, logistica, produzione, gestione documentale o trattamento di dati aziendali e personali.

Per questo motivo le più recenti normative in materia di **protezione dei dati personali, cybersecurity e continuità operativa** attribuiscono crescente importanza alla gestione della catena di fornitura.

Il **GDPR** richiede di selezionare responsabili del trattamento che offrano garanzie sufficienti in materia di sicurezza, mentre la **Direttiva NIS2** impone ai soggetti interessati di valutare anche i rischi derivanti dai fornitori ICT e dai servizi digitali utilizzati.

La gestione dei fornitori non dovrebbe quindi limitarsi alla stipula del contratto o della nomina privacy, ma comprendere una **valutazione preventiva** del rischio, **verifiche periodiche** e un **monitoraggio** continuo dei servizi maggiormente rilevanti per l'operatività aziendale.

Ogni organizzazione dovrebbe riuscire a individuare con chiarezza quali fornitori sono realmente essenziali per la **continuità delle attività**, quali soggetti hanno **accesso a dati**, sistemi o informazioni aziendali, e quali servizi potrebbero incidere su processi critici in caso di interruzione.

La capacità di conoscere e presidiare la propria catena di fornitura rappresenta oggi uno degli elementi fondamentali di un sistema di compliance e gestione dei rischi realmente efficace.

Cosa verificare in azienda

- Identificare i fornitori che svolgono attività critiche per il business o trattano dati aziendali e personali.
- Verificare la presenza di accordi contrattuali e nomine privacy aggiornate ove necessarie.
- Valutare le misure di sicurezza adottate dai fornitori più rilevanti.
- Monitorare periodicamente i fornitori strategici e i relativi livelli di servizio.
- Definire modalità di gestione delle criticità e delle interruzioni di servizio.
- Verificare la presenza di eventuali subfornitori coinvolti nell'erogazione dei servizi più critici.

Cybersecurity e modello 231: la formazione come misura di prevenzione

Gli attacchi informatici rappresentano oggi una delle principali minacce per le organizzazioni. **Ransomware, phishing, furto di credenziali, accessi abusivi e compromissione** dei sistemi informatici possono generare conseguenze economiche, operative e reputazionali particolarmente rilevanti.

Negli ultimi anni la sicurezza informatica è diventata un tema sempre più centrale non solo per le funzioni IT, ma anche per il management e per i sistemi di controllo aziendale.

La crescente digitalizzazione dei processi e l'incremento dei **reati informatici** rendono infatti necessario adottare un approccio strutturato alla gestione dei rischi cyber.

In questo contesto assume particolare importanza il rapporto tra cybersecurity, formazione del personale e Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001.

Molti incidenti informatici non derivano infatti da vulnerabilità tecnologiche, ma da **comportamenti inconsapevoli** degli utenti.

Apertura di allegati malevoli, utilizzo di password deboli, condivisione impropria di informazioni o mancato rispetto delle procedure aziendali rappresentano alcuni dei comportamenti più ricorrenti che possono esporre l'organizzazione a rischi e incidenti informatici.

Per questo motivo la **formazione** del personale rappresenta una delle misure di prevenzione più efficaci. Un lavoratore **consapevole** dei principali rischi informatici è infatti in grado di riconoscere più facilmente comportamenti sospetti e contribuire attivamente alla sicurezza dell'organizzazione.

La formazione assume inoltre un ruolo sempre più rilevante nell'ambito dei **Modelli 231**, in particolare per quanto riguarda la prevenzione dei reati informatici e la diffusione di una cultura aziendale orientata alla sicurezza e alla **gestione responsabile delle informazioni**.

Investire nella formazione significa non solo migliorare il livello di sicurezza dell'organizzazione, ma anche rafforzare l'efficacia dei sistemi di controllo interno e delle misure di compliance già adottate.

Cosa verificare in azienda

- Verificare se la formazione sulla cybersecurity è prevista all'interno dei programmi formativi aziendali.
- Valutare la presenza di contenuti dedicati a phishing, gestione delle password, utilizzo sicuro della posta elettronica e protezione delle informazioni.
- Verificare il coordinamento tra misure di sicurezza informatica, procedure aziendali e Modello Organizzativo 231.
- Pianificare attività periodiche di sensibilizzazione e aggiornamento del personale.
- Coinvolgere dirigenti, responsabili e figure chiave nei percorsi di formazione sulla sicurezza informatica.

Codice etico aziendale: non solo un documento, ma uno strumento di Governance

Quando si parla di **Codice Etico**, molte organizzazioni tendono ancora a considerarlo un documento formale da predisporre per adempiere a specifici obblighi normativi o per completare un sistema documentale aziendale.

In realtà, un Codice Etico efficace rappresenta molto di più: costituisce uno strumento attraverso il quale l'azienda **definisce e comunica i propri valori, i principi** di comportamento attesi e **le regole** che devono guidare le decisioni quotidiane di amministratori, dipendenti, collaboratori e partner commerciali.

Il Codice Etico assume un ruolo particolarmente importante all'interno dei sistemi di compliance e dei Modelli di Organizzazione, Gestione e Controllo adottati ai sensi del D.Lgs. 231/2001, contribuendo a diffondere una **cultura aziendale orientata all'integrità, alla trasparenza e alla responsabilità.**

Un documento realmente efficace non dovrebbe limitarsi a richiamare principi generali, ma fornire indicazioni concrete sui **comportamenti attesi**, sulla gestione dei conflitti di interesse, sulla tutela delle informazioni aziendali, sui rapporti con clienti, fornitori, pubbliche amministrazioni e altri stakeholder.

Affinché il Codice Etico possa svolgere la propria funzione, è inoltre fondamentale che sia **adeguatamente comunicato** all'interno dell'organizzazione e che i suoi contenuti siano conosciuti e compresi da tutti i destinatari.

In un contesto caratterizzato da una crescente attenzione verso i temi della compliance, della sostenibilità e della responsabilità sociale d'impresa, il Codice Etico rappresenta quindi un importante strumento di governance e un elemento distintivo della cultura organizzativa aziendale.

Cosa verificare in azienda

- Verificare la presenza di un Codice Etico formalmente adottato e aggiornato.
- Accertare che i contenuti siano coerenti con l'attività svolta e con i principali rischi aziendali.
- Verificare la diffusione del documento a dipendenti, collaboratori e soggetti terzi rilevanti.
- Integrare il Codice Etico con procedure aziendali, Modello 231 e sistemi di controllo interno.
- Prevedere attività di formazione e sensibilizzazione sui principi contenuti nel documento.
- Verificare periodicamente l'attualità dei contenuti e la necessità di eventuali aggiornamenti.

CONTATTI

info@compliance-srl.it
daniel.zisa@compliance-srl.it

www.compliance-srl.it

Nel prossimo numero

Nei prossimi numeri di **Focus Compliance** continueremo a condividere aggiornamenti normativi e indicazioni operative sui principali temi di compliance aziendale.

Proseguirà inoltre la presentazione dei professionisti e collaboratori che fanno parte del **team di COMPLIANCE SRL**, con l'obiettivo di far conoscere le competenze e le esperienze che contribuiscono quotidianamente ai progetti sviluppati per le organizzazioni clienti.

Compliance®
Smart Solutions