

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

NIS2: dalla registrazione alla conformità effettiva

Si avvicina il termine per l'adozione delle misure di sicurezza di base: cosa deve essere realmente operativo nelle organizzazioni interessate.

Pagina 3

AI Act: dal 2 agosto nuovi obblighi diventano applicabili

Trasparenza, pratiche vietate, alfabetizzazione sull'IA e nuove scadenze per i sistemi ad alto rischio.

Pagina 4

Intelligenza artificiale e Modello 231: nuovi reati presupposto dal 30 settembre

Nuovi reati presupposto collegano l'uso dell'IA alla responsabilità 231: cosa cambia per imprese e Modelli organizzativi.

Pagina 5

Anticorruzione e Modello 231: nuove regole europee rafforzano la prevenzione

La nuova disciplina europea e l'evoluzione della responsabilità e delle sanzioni applicabili agli enti.

Pagina 6

RENTRI: dal 16 settembre il FIR diventa digitale

Una nuova fase per la tracciabilità dei rifiuti: strumenti, responsabilità e coordinamento della filiera.

Pagina 7

Data breach: 1,7 milioni di euro di sanzione per carenze nella sicurezza

Il recente caso Wind Tre mostra quanto persone, credenziali, accessi e controlli siano determinanti nella protezione dei dati.

Pagina 8



IL TEAM DI COMPLIANCE SRL

NOEMI IZZO

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

Presentiamo **Noemi Izzo**, laureata in **Diritto dell'impresa nazionale e internazionale**, entrata a far parte di COMPLIANCE SRL nel 2024.

La sua formazione giuridica rappresenta un importante elemento di complementarità all'interno del team. Nel gruppo di lavoro, il suo approccio è infatti caratterizzato da una particolare attenzione alla **lettura normativa e giurisprudenziale**, che completa le competenze più aziendalistiche ed economiche, nonché quelle orientate all'audit e all'analisi dei rischi.

Nel corso della sua esperienza ha approfondito diversi ambiti della **compliance aziendale**, con particolare attenzione alla protezione dei dati personali (**GDPR**), alla responsabilità degli enti ai sensi del **D.Lgs. 231/2001**, all'**antiriciclaggio** e, più in generale, alla predisposizione e applicazione di regolamenti, policy e sistemi interni di prevenzione e controllo.

Un percorso che le ha permesso di confrontarsi con realtà e problematiche differenti, cercando sempre di coniugare il dato normativo con le **esigenze concrete delle organizzazioni**.

In questi anni ha inoltre affiancato più volte i colleghi con maggiore esperienza nelle attività di formazione in aula presso le aziende clienti, acquisendo esperienza anche nel confronto diretto con i partecipanti.

Nonostante la giovane età, l'esperienza maturata le sta consentendo di assumere progressivamente **maggiore autonomia e responsabilità**, contribuendo oggi anche all'affiancamento dei nuovi collaboratori e alla condivisione del metodo di lavoro del team.



Il terzo numero di Focus Compliance arriva in un periodo particolarmente ricco di novità e scadenze per le imprese.

In questo numero torniamo innanzitutto su due temi che stanno entrando in una fase sempre più concreta: la Direttiva NIS2, con l'avvicinarsi del termine per l'adozione delle misure di sicurezza di base, e l'AI Act, dopo la nuova tappa del suo percorso applicativo raggiunta il 2 agosto.

Affrontiamo inoltre la recente evoluzione europea in materia di anticorruzione e responsabilità degli enti, le novità operative introdotte dal RENTRI e un recente provvedimento del Garante Privacy relativo a un importante data breach, utile per riflettere concretamente sulla sicurezza dei sistemi, sulla gestione degli accessi e sul ruolo delle persone. Temi diversi, accomunati da un principio che cerchiamo di mantenere al centro anche della nostra attività quotidiana: la compliance non può limitarsi alla predisposizione di documenti, ma deve tradursi in misure, responsabilità e comportamenti concretamente applicati all'interno delle organizzazioni.

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

Daniel Zisa
Founder – COMPLIANCE SRL

NIS2: dalla registrazione alla conformità effettiva

Per le organizzazioni rientranti nell'ambito della **Direttiva NIS2**, il percorso di adeguamento entra ora in una fase particolarmente importante.

Nei mesi scorsi molte imprese hanno concentrato l'attenzione sugli adempimenti verso l'**Agenzia per la Cybersicurezza Nazionale (ACN)**: registrazione sulla piattaforma, aggiornamento delle informazioni, individuazione dei referenti e gestione delle successive comunicazioni. Essere correttamente registrati, tuttavia, **non significa essere conformi alla NIS2**.

Per i soggetti inseriti nell'elenco NIS nella prima fase di applicazione del 2025 si avvicina infatti il termine per l'adozione delle **misure di sicurezza di base definite da ACN**. Il termine è fissato in 18 mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti NIS e, per la platea individuata nel 2025, ricade generalmente nel mese di **ottobre 2026**. L'attenzione deve quindi spostarsi dagli adempimenti prevalentemente formali alla verifica di ciò che è stato **effettivamente implementato nell'organizzazione**.

La conformità alla NIS2 non coincide con l'adozione di un singolo documento o con l'acquisto di nuove soluzioni informatiche. Richiede un sistema coordinato di misure tecniche, operative e organizzative che comprende, tra gli altri aspetti, **valutazione e gestione dei rischi, gestione degli incidenti, continuità operativa, sicurezza della catena di fornitura, gestione degli accessi, protezione dei sistemi e formazione del personale**.

Un ruolo centrale è inoltre attribuito agli **organi di amministrazione e direttivi**, chiamati ad approvare le modalità di implementazione delle misure di gestione dei rischi, sovrintendere l'attuazione e partecipare a specifiche attività formative.

A poche settimane dalla scadenza, diventa quindi importante verificare non soltanto se la documentazione prevista sia stata predisposta, ma soprattutto se **procedure, responsabilità e misure di sicurezza siano realmente applicate, documentate e conosciute dalle persone coinvolte**.

Cosa verificare in azienda

- **Valutazione dei rischi:** verificare che i rischi per la sicurezza dei sistemi informativi e di rete siano stati individuati, valutati e documentati.
- **Misure di sicurezza:** verificare lo stato di implementazione delle misure di base previste da ACN per i soggetti importanti o essenziali.
- **Gestione degli incidenti:** accertare che siano definiti ruoli e procedure interne per individuare, gestire e notificare gli incidenti significativi.
- **Continuità operativa:** verificare backup, ripristino, gestione delle crisi e continuità delle attività maggiormente rilevanti.
- **Fornitori:** individuare i fornitori critici e verificare i rischi di cybersicurezza connessi alla catena di approvvigionamento.
- **Formazione e governance:** verificare che personale, responsabili e organi amministrativi siano adeguatamente coinvolti e formati.
- **Evidenze:** assicurarsi che valutazioni, controlli, attività svolte e decisioni assunte siano adeguatamente documentati.

AI ACT: dal 2 Agosto nuovi obblighi diventano applicabili

Il **2 agosto 2026** ha segnato un nuovo passaggio importante nell'applicazione dell'AI Act, il Regolamento europeo che disciplina lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale.

Dopo l'entrata in vigore dei primi obblighi nel 2025, il quadro normativo entra ora in una fase più concreta, con l'applicazione di nuovi **obblighi di trasparenza** e l'avvio dei relativi poteri di controllo da parte delle autorità competenti.

In particolare, quando un sistema di intelligenza artificiale interagisce direttamente con una persona, quest'ultima deve essere informata che sta interagendo con un'IA, salvo che ciò risulti già evidente. Specifiche regole riguardano inoltre i **contenuti generati o manipolati artificialmente**, i deepfake e l'utilizzo di sistemi di riconoscimento delle emozioni o categorizzazione biometrica.

Parallelamente, continuano ad applicarsi i **divieti relativi alle pratiche di IA considerate inaccettabili** e gli obblighi in materia di **alfabetizzazione sull'intelligenza artificiale**, che richiedono alle organizzazioni di adottare misure affinché le persone che utilizzano sistemi di

IA dispongano di conoscenze adeguate rispetto al proprio ruolo, al contesto di utilizzo e ai rischi connessi.

Le recenti modifiche alla disciplina europea hanno invece concesso più tempo per l'applicazione degli obblighi relativi ai **sistemi di IA ad alto rischio**: per quelli rientranti nelle categorie dell'Allegato III, tra cui determinati utilizzi in ambito HR, istruzione, biometria e servizi essenziali, la nuova data è il **2 dicembre 2027**; per i sistemi ad alto rischio integrati in prodotti regolamentati, il termine è il **2 agosto 2028**.

Le nuove scadenze non devono però essere interpretate come una sospensione generale dell'AI Act. Per le imprese rimane importante conoscere **quali strumenti di IA vengono effettivamente utilizzati**, per quali finalità, con quali dati e da quali persone.

Il percorso di adeguamento dovrebbe quindi partire dalla mappatura degli strumenti utilizzati e proseguire con la definizione di **regole interne, responsabilità, controlli e attività formative proporzionate ai rischi**.

Cosa verificare in azienda

- **Mappatura degli strumenti:** verificare quali sistemi e applicazioni di IA sono utilizzati dalle diverse funzioni aziendali, compresi gli strumenti introdotti autonomamente dai lavoratori.
- **Trasparenza:** individuare eventuali utilizzi per i quali sia necessario informare clienti, utenti, lavoratori o altri soggetti dell'interazione con un sistema di IA o della natura artificiale di determinati contenuti.
- **Pratiche vietate:** verificare che gli strumenti utilizzati non rientrino nelle pratiche espressamente vietate dall'AI Act.
- **Regole interne:** definire quali strumenti possono essere utilizzati, per quali finalità e quali informazioni possono essere inserite nei sistemi di IA.
- **Formazione:** adottare misure di alfabetizzazione sull'IA coerenti con il ruolo delle persone coinvolte e con le modalità concrete di utilizzo degli strumenti.
- **Sistemi ad alto rischio:** verificare se l'organizzazione utilizza sistemi che potrebbero rientrare nelle categorie ad alto rischio, così da programmare per tempo le successive attività di adeguamento.

Intelligenza artificiale e Modello 231: nuovi reati presupposto dal 30 settembre

L'intelligenza artificiale entra espressamente nel sistema della responsabilità amministrativa degli enti prevista dal D.Lgs. 231/2001.

Dal **30 settembre 2026** è infatti in vigore una nuova disciplina che introduce nel catalogo dei reati presupposto alcune fattispecie collegate all'utilizzo dei sistemi di intelligenza artificiale.

La novità riguarda in particolare i sistemi di IA ad alto rischio. La nuova normativa prevede conseguenze penali nei casi più gravi in cui **vengano omesse le misure di sicurezza** o la necessaria sorveglianza umana, oppure venga alterato il funzionamento del sistema, creando un concreto pericolo per le persone o per la sicurezza.

Un aspetto particolarmente importante per le imprese è che la disciplina non riguarda soltanto chi sviluppa o produce sistemi di intelligenza artificiale, ma può interessare **anche chi li utilizza** professionalmente nell'ambito della propria attività.

Nel nuovo articolo del D.Lgs. 231/2001 rientra inoltre il reato relativo alla diffusione illecita di contenuti generati o modificati attraverso l'intelligenza artificiale, come nel caso dei cosiddetti deepfake.

Per le imprese le conseguenze possono essere rilevanti, con sanzioni pecuniarie e, in determinati casi, sanzioni interdittive.

Questo non significa che ogni azienda che utilizza strumenti di IA debba automaticamente modificare il proprio Modello 231. Diventa però **importante sapere quali strumenti vengono utilizzati**, per quali finalità e con quali rischi, verificando se le nuove fattispecie possano essere concretamente applicabili alla propria organizzazione.

Per le società dotate di un Modello 231, la novità rappresenta quindi un'occasione per integrare la mappatura degli strumenti di IA nel risk assessment aziendale e valutare se procedure, controlli e responsabilità già previste siano ancora adeguati.

Cosa verificare in azienda

- **Mappatura dell'IA:** individuare quali sistemi di intelligenza artificiale sono effettivamente utilizzati e per quali attività.
- **Classificazione del rischio:** verificare se tra gli strumenti utilizzati siano presenti sistemi classificabili come IA ad alto rischio ai sensi dell'AI Act.
- **Sorveglianza umana:** verificare che siano definite responsabilità e modalità di controllo umano sull'utilizzo dei sistemi rilevanti.
- **Regole interne:** disciplinare l'utilizzo dell'IA e la produzione o diffusione di contenuti generati o modificati artificialmente.
- **Modello 231:** valutare l'impatto del nuovo art. 25-bis sul risk assessment e sui protocolli aziendali esistenti.
- **Organismo di Vigilanza:** assicurare adeguati flussi informativi sull'introduzione e sull'utilizzo di sistemi di IA potenzialmente rilevanti ai fini 231.

Anticorruzione e modello 231: nuove regole europee rafforzano la prevenzione

Nel 2026 l'Unione Europea ha introdotto una nuova disciplina in materia di **lotta alla corruzione**, destinata a incidere anche sui sistemi nazionali di responsabilità degli enti.

La nuova Direttiva europea rafforza il quadro comune per la prevenzione e il contrasto dei fenomeni corruttivi, intervenendo sulla definizione dei reati, sulla responsabilità delle persone giuridiche e sul sistema delle sanzioni.

Uno degli elementi più significativi riguarda proprio le **sanzioni applicabili agli enti**, per le quali la disciplina europea introduce parametri collegati anche al fatturato mondiale dell'impresa. Il sistema italiano previsto dal **D.Lgs. 231/2001** è invece attualmente basato sul meccanismo delle quote.

La Direttiva dovrà essere recepita dagli Stati membri e **non modifica quindi immediatamente il sistema sanzionatorio previsto dal D.Lgs. 231/2001**.

Rappresenta però un'indicazione importante sull'evoluzione della normativa europea e sulla crescente attenzione verso

l'effettività dei sistemi aziendali di prevenzione della corruzione.

Per le imprese il tema non riguarda soltanto i rapporti diretti con la Pubblica Amministrazione. I rischi possono emergere anche nella gestione di **consulenti e intermediari, omaggi e spese di rappresentanza, sponsorizzazioni, selezione dei fornitori, autorizzazione dei pagamenti e gestione dei flussi finanziari**.

In questo contesto, il Modello 231 rappresenta uno degli strumenti attraverso cui l'organizzazione può strutturare responsabilità, procedure e controlli finalizzati alla prevenzione dei comportamenti illeciti.

L'evoluzione normativa costituisce quindi un'occasione per verificare che **risk assessment, protocolli e controlli anticorruzione siano ancora adeguati rispetto all'organizzazione e alle attività concretamente svolte**, evitando che il Modello rimanga un documento formalmente adottato ma non pienamente applicato.

Cosa verificare in azienda

- **Valutazione dei rischi:** verificare che la mappatura 231 consideri adeguatamente i processi maggiormente esposti ai rischi corruttivi.
- **Rapporti con soggetti terzi:** valutare i controlli previsti nella selezione e gestione di consulenti, intermediari, fornitori e altri partner commerciali.
- **Flussi finanziari:** verificare autorizzazioni, tracciabilità e segregazione delle responsabilità nei processi di pagamento.
- **Codice Etico e protocolli:** accertare che regole e procedure anticorruzione siano aggiornate e concretamente applicate.
- **Whistleblowing:** verificare che il sistema di segnalazione sia operativo e adeguatamente conosciuto dai destinatari.
- **Formazione:** assicurare una formazione coerente con i rischi e maggiormente mirata alle funzioni aziendali più esposte.

RENTRI: dal 16 settembre il FIR diventa digitale

Dal **16 settembre 2026** è entrata in una nuova fase la digitalizzazione della tracciabilità dei rifiuti: per i soggetti iscritti al **RENTRI**, il Formulario di identificazione del rifiuto (FIR) deve essere gestito in formato digitale.

Fino al 15 settembre era infatti previsto un periodo transitorio durante il quale gli operatori iscritti potevano continuare a scegliere tra **FIR cartaceo e FIR digitale**. Con la conclusione di questa fase, il formulario digitale diventa la modalità ordinaria per gli iscritti al Registro.

Il cambiamento non riguarda soltanto il formato del documento. Il **FIR digitale (xFIR)** accompagna elettronicamente la movimentazione del rifiuto e coinvolge i diversi soggetti della filiera: produttore o detentore, trasportatore e destinatario.

Per le imprese diventa quindi importante verificare che siano state definite le modalità operative per **compilare, sottoscrivere e gestire il formulario digitale** e che le persone incaricate dispongano degli strumenti e delle abilitazioni necessarie.

Il processo può essere gestito attraverso i servizi messi a disposizione direttamente dal RENTRI, compresa l'applicazione dedicata, oppure attraverso sistemi gestionali interoperabili con la piattaforma.

Particolare attenzione deve essere dedicata anche al **coordinamento con trasportatori e impianti destinatari**. Il formulario accompagna infatti l'intera movimentazione e richiede che i diversi soggetti coinvolti siano in grado di gestire correttamente le rispettive fasi.

La disciplina prevede inoltre specifiche modalità operative da utilizzare in caso di

indisponibilità o temporaneo degrado dei servizi RENTRI, recentemente aggiornate dal Ministero proprio in vista della piena operatività del sistema digitale.



Cosa verificare in azienda

- **Applicabilità:** verificare se l'impresa è iscritta al RENTRI e per quali attività e unità locali trova applicazione la gestione digitale del FIR.
- **Strumenti utilizzati:** individuare se il formulario viene gestito attraverso i servizi RENTRI oppure mediante un software gestionale interoperabile.
- **Persone incaricate:** verificare che siano individuati e abilitati i soggetti che devono compilare e sottoscrivere il FIR per conto dell'impresa.
- **Coordinamento della filiera:** accertare che trasportatori e destinatari siano organizzati per gestire correttamente il formulario digitale.
- **Procedure interne:** aggiornare le modalità operative aziendali e conoscere le procedure da utilizzare in caso di indisponibilità dei servizi RENTRI.

Data breach: 1,7 milioni di euro di sanzione per carenze nella sicurezza

Un recente provvedimento del **Garante per la protezione dei dati personali** richiama l'attenzione delle imprese sull'importanza delle misure di sicurezza adottate per proteggere dati, sistemi e credenziali di accesso.

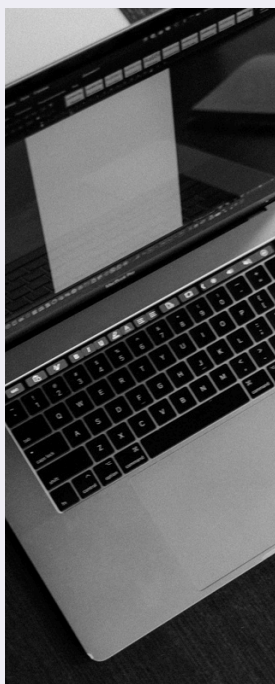
Il caso riguarda **Wind Tre**, destinataria di una sanzione di oltre **1,7 milioni di euro** a seguito di due data breach che hanno comportato accessi abusivi ai sistemi aziendali e coinvolto i dati personali di oltre **365.000 clienti**. Per più di 41.000 interessati risultavano coinvolte anche informazioni relative ai metodi di pagamento.

Particolarmente interessante è la modalità con cui si sono verificati gli attacchi. Gli autori, **fingendosi tecnici dell'assistenza**, hanno contattato operatori di alcuni punti vendita convincendoli a consentire l'accesso remoto ai dispositivi e riuscendo così a ottenere i fattori necessari per accedere ai sistemi.

L'istruttoria del Garante ha evidenziato anche criticità nella **gestione delle credenziali e dei certificati digitali** e ha rilevato che le verifiche di sicurezza precedentemente effettuate non avevano individuato alcune vulnerabilità che sarebbero potute emergere attraverso controlli più approfonditi.

Il caso dimostra come la sicurezza delle informazioni non dipenda esclusivamente dall'adozione di strumenti tecnologici. Anche **procedure, gestione degli accessi e consapevolezza delle persone** rappresentano elementi essenziali per ridurre il rischio di incidenti.

Per le organizzazioni diventa quindi importante adottare un approccio che combini misure tecniche e organizzative, verificando periodicamente l'efficacia dei controlli e prestando particolare attenzione alle modalità con cui vengono gestite **credenziali, accessi remoti e richieste di assistenza tecnica**.



Cosa verificare in azienda

- **Credenziali e accessi:** verificare le modalità di assegnazione, conservazione, aggiornamento e revoca delle credenziali aziendali.
- **Accessi remoti:** definire procedure chiare per autorizzare interventi di assistenza e collegamenti da remoto ai sistemi aziendali.
- **Social engineering:** sensibilizzare il personale rispetto a telefonate, e-mail o richieste apparentemente provenienti da tecnici, fornitori o soggetti conosciuti.
- **Verifiche di sicurezza:** effettuare controlli periodici sull'effettiva efficacia delle misure tecniche e organizzative adottate.
- **Gestione degli incidenti:** assicurarsi che il personale sappia a chi segnalare rapidamente anomalie, accessi sospetti o possibili violazioni dei dati.
- **Data breach:** verificare che siano definite responsabilità e procedure per valutare e, quando necessario, notificare tempestivamente eventuali violazioni dei dati personali.

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.