people in compliance

by compliancedesign.it

GRC talks

Cyber attack e data breach: prepararsi all'evento per gestire la crisi

ritratti e organizzazioni

Etica e buona reputazione per generare fiducia e credibilità

Chief Compliance Officer
Leonardo

aree e settori

Tutela e gestione dei dati, un valore strategico per l'azienda

Elisa Romano,
Head of Data Protection & Information Security di Lamborghini

il punto

Una compliance semplice e integrata a sostegno dei process owner

Lorenzo Rinaldi,
Chief Risk Officer e Vice President Risk Governance & Compliance di Aeroporti di Roma

CONFINDUSTRIA ASSOIMMOBILIARE

AITRA
ASSOCIAZIONE ITALIANA TRASPARENZA E ANTICORRUZIONE

compliance design

aml integrity design

Al via la prima edizione di
aml integrity design

l'iniziativa di **AITRA** e **compliancedesign.it**
in partnership con **Confindustria Assoimmobiliare**

che nasce con l'obiettivo di **favorire il dialogo** tra operatori del settore bancario e finanziario, autorità di vigilanza e tutti gli stakeholder coinvolti **nel processo di diffusione della cultura del contrasto al riciclaggio** di denaro e al finanziamento del terrorismo.

save the date

Roma, 18 giugno 2024
ore 14:30 - 18:30

Confindustria Assoimmobiliare
Via IV Novembre, 114

PROGRAMMA E RELATORI
PRESTO DISPONIBILE

REGISTRATI

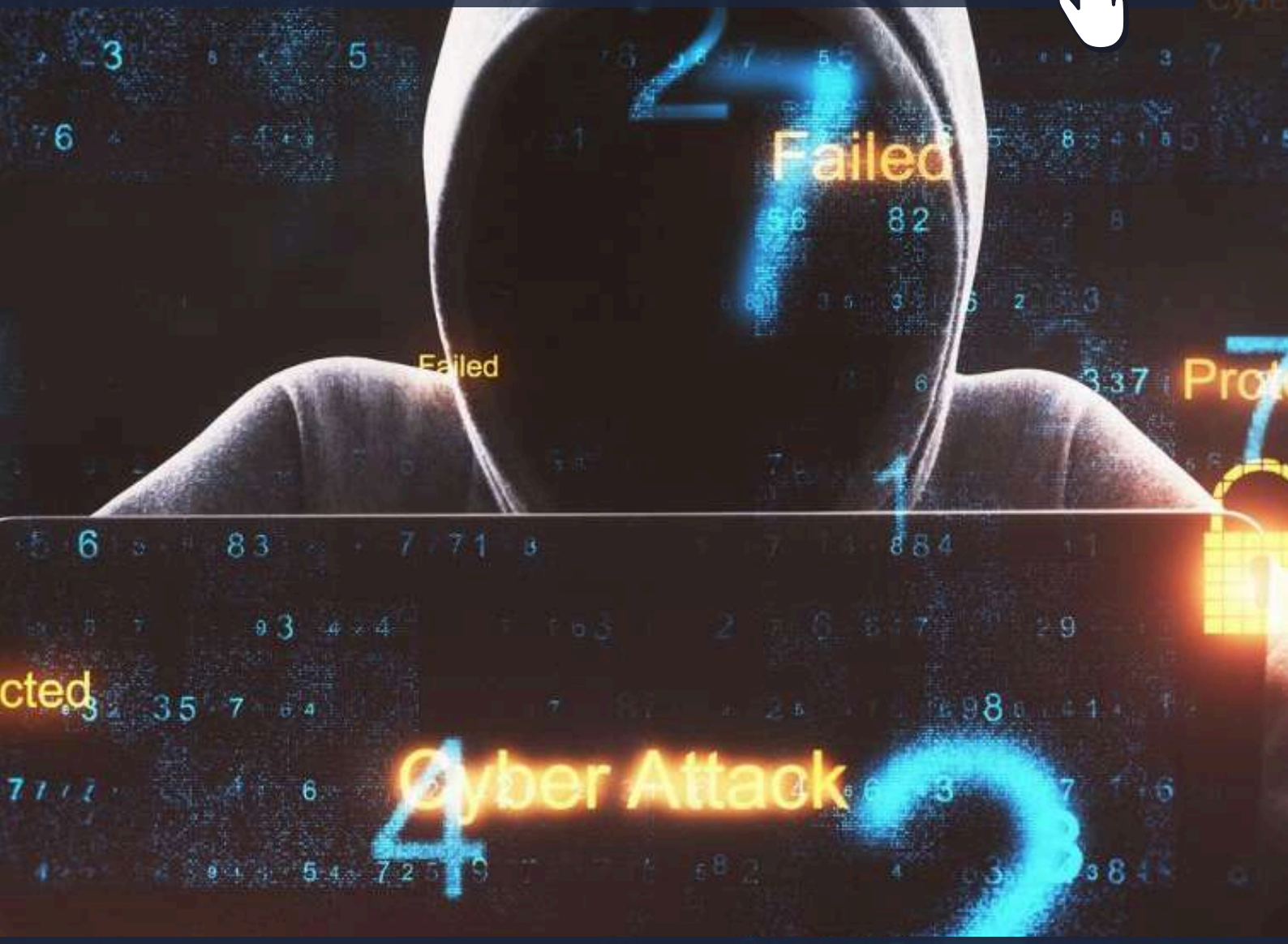
eventi@compliancedesign.it

Partner ANDAF

GRC talks

Cyber attack e data breach: prepararsi all'evento per gestire la crisi

WATCH VIDEO



compliance design | PARTNER EY

Si è tenuto lo scorso 23 aprile un nuovo appuntamento del ciclo GRC talks sviluppato in collaborazione con EY Forensic & Integrity Services

Il talk dal titolo "*Cyber attack e data breach: prepararsi all'evento per gestire la crisi*" ha visto la partecipazione di **Davide Ajello** (*Data Protection Officer Telepass*), **Eliana Carusi** (*Country Business Risk & Compliance Manager IKEA Italia Retail*), **Jean Paule Castagno** (*Partner White Collar Crime Orrick*), **Luca Marzegalli** (*Partner Cyber EY Forensic & Integrity Services*), **Pietro Pisanelli** (*Head of Compliance & Risk Management Vodafone*) e la moderazione di **Luigi Neirotti** (*Senior Legal Counsel EY*).

WATCH VIDEO

compliance design | PARTNER EY

Nel mondo sempre più

interconnesso e digitalizzato in cui viviamo, gli attacchi informatici rappresentano una minaccia sempre più concreta per le aziende di ogni settore. La necessità di prepararsi adeguatamente a gestire le crisi generate da tali eventi è diventata cruciale, come è emerso nel recente talk "*Cyber attack e data breach: prepararsi all'evento per gestire la crisi*", organizzato da ***compliancedesign.it*** in collaborazione con ***EY Forensic & Integrity Services***.

La sintesi dell'incontro è chiara: non è più una questione di se, ma di quando un'azienda subirà un attacco informatico. Prevenire è sicuramente importante, ma è altrettanto essenziale uscire dalla comfort zone della difesa per essere pronti a reagire in modo efficace quando la crisi si presenta.

Gestire una crisi richiede una prospettiva preventiva e strategica. È fondamentale anticipare e prepararsi a reagire in modo tempestivo e coordinato, altrimenti ci si trova ad affrontare la situazione in modo disorganizzato, con conseguenze potenzialmente devastanti per l'azienda. La corretta risposta e la corretta reazione, nell'immediatezza della scoperta, è buona parte della risoluzione del problema.

Uno degli esempi più evidenti di questa necessità è rappresentato dai ransomware, che hanno colpito numerose organizzazioni in tutto il mondo. Le conseguenze di tali attacchi possono variare notevolmente: da pochi giorni di inattività aziendale a lunghi periodi, e da nessuna perdita di dati a danni irreparabili. Nella maggior parte dei casi, il risultato dipende dalle azioni intraprese dall'azienda prima dell'attacco.

Se in passato la cybersecurity si concentrava principalmente sulla prevenzione, con l'implementazione di firewall, segmentazione di rete e password complesse, oggi la gestione degli incidenti richiede approcci e competenze nuove, ancora difficili da trovare sul mercato.

La rapidità delle decisioni è altresì fondamentale, non solo dal punto di vista tecnico, ma anche strategico-legale, e tende a coinvolgere un numero sempre più ampio di funzioni aziendali, a partire da IT, compliance, audit e legale, per affrontare la situazione in modo completo e coordinato.

Le conseguenze di un attacco informatico, infatti, possono essere devastanti sotto diversi aspetti. Oltre ai danni pecuniari ed economici, ci sono quelli reputazionali e sanzionatori, che possono avere conseguenze a lungo termine per l'azienda.

Dal punto di vista penale, le società che subiscono un attacco si trovano poi in una situazione giuridica particolare: da un lato sono vittime del cyber attack, ma

Davidee Ajello
Data Protection Officer Telepass

Jean Paule Castagno
Partner White Collar Crime Orrick

Eliana Carusi
Country Business Risk
& Compliance Manager IKEA Italia Retail

Non è più una questione di se, ma di quando un'azienda subirà un attacco informatico. Prevenire è sicuramente importante, ma è altrettanto essenziale uscire dalla comfort zone della difesa per essere pronti a reagire in modo efficace quando la crisi si presenta

Luigi Neirotti
Partner EY Forensic & Integrity Services

Luca Marzegalli
Partner Cyber EY Forensic & Integrity Services

Pietro Pisanelli
Head of Compliance & Risk Management Vodafone

Le indagini investigative in chiave difensiva *(in campo cyber)* assumono un ruolo centrale nel nuovo contesto, influenzando significativamente la responsabilità giuridica dell'azienda.

contemporaneamente devono dimostrare di essere vittime innocenti. Ciò significa aver adottato tutte le precauzioni necessarie per evitare, anche solo colposamente, di favorire l'evento infausto. Il mancato o incompleto sistema di regolamentazione interna potrebbe essere interpretato come un contributo all'agevolazione del reato commesso da terzi soggetti.

Cambia il paradigma.
Le indagini investigative in chiave difensiva (in campo cyber) assumono un ruolo centrale nel nuovo contesto, influenzando significativamente la responsabilità giuridica dell'azienda. Ciò implica la capacità di descrivere e delineare chiaramente i diversi aspetti dell'evento: il contesto tecnologico, l'attacco subito e i danni connessi, documentare eventuali attività di esfiltrazione e la tempestività della scoperta, oltre a illustrare i presidi tecnici e organizzativi adottati per reagire. Quindi non solo quelli preventivi in base all'ordinaria gestione della situazione, ma anche quelli che sono stati adottati prevedendo che un attacco potesse in qualche modo avvenire.

La reazione agli attacchi informatici rappresenta la nuova frontiera per la difesa aziendale. È necessario adottare un approccio olistico e prepararsi adeguatamente per affrontare le nuove complesse sfide.

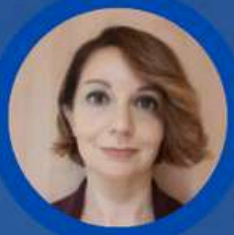
COMPLIANCE E SOSTENIBILITÀ DI FILIERA, SUPPLY CHAIN DUE DILIGENCE

GRC talks

MARTEDÌ 28 MAGGIO

ONLINE ORE 14:30

CLICCA E REGISTRATI



Daria Angelini
Compliance Director
Webuild

Antonio Buonafine
Head of Governance &
Compliance Arvedi Group

Nicoletta Pia di Cagno
Compliance Director
Versace

Getano Vittoria
Director Legal, Global
Business Counsel/ESG,
Nordic Regional Counsel
McDonald's

MODERA
Marianna Lamolinara
Partner Forensic &
Integrity Services EY

eventi@compliancedesign.it

compliance design | EY

Elena Napolitano (Leonardo)

Etica e buona reputazione per generare fiducia e credibilità

di Matteo Rizzi

Nel cuore dell'industria

aerospaziale e della difesa, Leonardo rappresenta una punta di diamante nel panorama italiano, con una presenza che si estende ben oltre i confini nazionali. Tuttavia, dietro il successo tecnologico ed economico si nasconde una realtà complessa, in cui la gestione della reputazione e l'etica aziendale giocano un ruolo fondamentale.

compliancedesign.it ha intervistato **Elena Napolitano**, *Chief Compliance Officer di Leonardo*, per approfondire il percorso della società nel delicato equilibrio tra progresso economico e responsabilità sociale, scoprendo come l'azienda abbia affrontato le sfide della prevenzione dei rischi di conformità legale e reputazionali nel corso degli anni e quali strategie adotti attualmente per mantenere la fiducia degli stakeholder.

La funzione opera con una ramificazione nei 27 siti di Leonardo e con oltre 160 risorse dislocati sul territorio nazionale, e con un dialogo constante con le strutture di Compliance delle oltre 60 Società Controllate (italiane ed estere) da Leonardo, verso cui svolge un'attività di indirizzo, supervisione e monitoraggio.

Leonardo rappresenta una risorsa per il nostro Paese, con un enorme potenziale per generare sviluppo e crescita economica. Ma l'azienda opera anche in un settore sensibile in cui la reputazione gioca sempre più un ruolo fondamentale. Qual è l'approccio di Leonardo?

È proprio così. Il settore Aerospazio, Difesa e Sicurezza riveste un'importanza strategica per ogni sistema-Paese, ponendo le condizioni per la sua sicurezza e stabilità, e fornendo un sensibile contributo al progresso scientifico e alla ricerca di nuove tecnologie. In tale contesto, in modo particolare, la buona reputazione rappresenta per le aziende del settore un vero e proprio asset, una leva strategica per generare fiducia e credibilità di fronte a stakeholder, partner commerciali e clientela. Questa è una tematica che, in Leonardo, ha acquisito un'importanza sempre crescente negli ultimi decenni, traducendosi in un impegno costante a prevenire i rischi di pratiche illecite a qualsiasi livello lavorativo e in ogni ambito geografico.

Tale impegno si è tradotto, in primis, nella diffusione e promozione di valori e principi etici (contenuti in documenti quali la Carta dei Valori, il Codice Anticorruzione, il Codice Etico, la Policy Human Rights o il Codice di Condotta per i fornitori), accompagnato dalla creazione di un robusto sistema procedurale e dall'effettiva attuazione di processi di controllo, in linea con i requisiti fissati dalle normative applicabili e con le migliori pratiche internazionali.

Sul fronte organizzativo, la funzione di Compliance - costituita per la prima volta nel Gruppo quasi vent'anni fa, con un ampliamento progressivo delle proprie attività – ad oggi è posta a diretto riporto dell'Amministratore Delegato a dimostrazione dell'impegno tone from the top del Gruppo Leonardo a fare dei principi di integrità, etica e legalità dei driver fondamentali del proprio modo di fare business.

La funzione opera capillarmente, con una ramificazione nei 27 siti di Leonardo e con oltre 160 risorse dislocati sul territorio nazionale, e con un dialogo constante con le strutture di Compliance delle oltre 60 Società Controllate (italiane ed estere) da Leonardo, verso cui svolge un'attività di indirizzo, supervisione e monitoraggio.

La credibilità etica di un'azienda fa la differenza nei rapporti che gli stakeholder vogliono avere con quell'azienda. Leonardo ha lavorato molto per rafforzare il proprio modello di conduzione responsabile del business e costruire una reputazione che oggi possiamo definire solida.

Governance, compliance, etica e trasparenza sembrano essere concetti sempre più interconnessi e interdipendenti. Come si traducono nella pratica?

L'etica è il primo tra i valori menzionati nella Carta dei Valori di Leonardo, il documento di riferimento per i modelli organizzativi e le procedure adottate all'interno del Gruppo, al cui rispetto sono improntati i rapporti con tutti i propri stakeholder, interni ed esterni. La credibilità etica di un'azienda fa la differenza nei rapporti che gli stakeholder vogliono avere con quell'azienda.

Leonardo ha lavorato molto per rafforzare il proprio modello di conduzione responsabile del business e costruire una reputazione che oggi possiamo definire solida. Lo ha fatto disegnando un sistema organizzativo fortemente orientato a prevenire l'illegalità,

Accanto a misure organizzative e dispositive efficaci, Leonardo ha investito ed investe molto sulla cultura dell'integrità, promossa attraverso attività di formazione, sensibilizzazione e valorizzazione del tema all'interno della propria catena del valore, con attenzione specifica ai propri dipendenti e alle controparti

ma anche promuovendo un approccio sinergico tra tutte le funzioni aziendali coinvolte a vario titolo in tale attività di prevenzione (tra queste, compliance, legale, interna audit, sostenibilità, finance) e creando un forte sistema di monitoraggio e controllo di tutti i relativi processi.

Proprio questo approccio sinergico è stato un fattore chiave per il raggiungimento di importanti obiettivi per l'Azienda negli ultimi anni. Tra questi è il conseguimento, per la prima volta nel 2018 (con successivi rinnovi di anno in anno), della certificazione UNI ISO 37001:2016, Anti-Bribery Management Systems, che stabilisce i requisiti per un sistema di gestione anticorruzione efficace all'interno dell'organizzazione, e della certificazione AEO-F (Authorised Economic Operator Full), che attribuisce una "patente" di affidabilità e di solvibilità valida in tutto il territorio doganale comunitario a cui sono collegati una serie di vantaggi e semplificazioni.

Ancora, nel 2020 Transparency International ha inserito Leonardo nel livello più alto (fascia A, prima di sei) del Defence Companies Index on *Anti-Corruption and Corporate Transparency*, con una scalata del ranking rispetto all'ultima rilevazione del 2015. L'indice valuta le informazioni pubbliche di 134 società del settore di 38 Paesi in tutto il mondo con riferimento a 10 aree di rischio chiave. Nell'area relativa ad "Agenti, Intermediari e Joint Ventures", Leonardo è stata l'unica società del settore Aerospazio e Difesa a posizionarsi in fascia A.

Ma, accanto a misure organizzative e dispositive efficaci, Leonardo ha investito ed investe molto sulla cultura dell'integrità, promossa attraverso attività di formazione, sensibilizzazione e valorizzazione del tema all'interno della propria catena del valore, con attenzione specifica ai propri dipendenti e alle controparti (nel 2023 sono state erogate 38 mila ore di formazione sui temi di Compliance ai dipendenti del Gruppo Leonardo e sono state coinvolte più di 100 controparti in percorsi formativi concepiti ad hoc).

Il bilanciamento tra business e rischio è spesso un compito arduo. Quali sono gli elementi chiave che Leonardo considera per ottenere un risultato win-win?

Per affrontare in modo efficace questa sfida è fondamentale, innanzitutto, un impegno tone from the top del Vertice aziendale che promuova una cultura dell'etica ed orienti ad essa tutte le scelte strategiche e le attività operative dell'azienda. Una cultura che riconosca la Compliance non come un ostacolo al business, ma come un ostacolo alle scorciatoie del business ed uno strumento per creare valore.

Occorre che il processo decisionale, sia strategico che operativo, sia fondato su un approccio di Enterprise Risk Management tale da assicurare l'analisi ed il corretto bilanciamento tra i rischi e le opportunità connessi alle singole iniziative, dall'anticorruzione ai diritti umani.

FUNZIONE DI COMPLIANCE E LEGALE SEPARATE CON RIPORTO DIRETTO AL CEO

L'evoluzione della compliance all'interno delle grandi aziende è un riflesso della crescente consapevolezza dei rischi connessi al mancato rispetto delle norme - esterne ed interne – che regolano l'attività dell'Azienda e della necessità di prevenire le potenziali minacce che potrebbero metterla a rischio. Un esempio tangibile di questo processo di trasformazione è l'approccio adottato da Leonardo, che ha posto la compliance al centro della propria strategia aziendale. "Mentre il legale assiste nelle negoziazioni e nei momenti critici, la compliance si concentra sulla prevenzione di qualsiasi rischio di conformità legale e reputazionale", spiega **Elena Napolitano**, Chief Compliance Officer di Leonardo a ***compliancedesign.it***. "La compliance è di supporto continuo al business nell'identificare i potenziali rischi e prevenirli".

L'evoluzione della funzione compliance in Leonardo è stata graduale ma significativa. Nata nel 2007 in una delle società del gruppo, ha subito un progressivo processo di ampliamento organico fino a diventare una funzione trasversale a tutte le società del gruppo stesso.

Questo sviluppo è stato supportato, nel tempo, dalla creazione di Leonardo One Company, che ha riunito sotto di sé tutte le attività aziendali e, successivamente, dalla configurazione della compliance come una funzione a diretto riporto del CEO.

La compliance in Leonardo si estende a una serie di attività che, oltre al presidio delle tematiche etiche e di integrità aziendale, include l'aggiornamento del "Modello 231/2001", il presidio sul sistema anticorruzione della società, una gestione rigorosa degli intermediari commerciali, la supervisione del rispetto delle normative internazionali sul commercio di materiali civili e militari, nonché un sistema di controllo sulle partnership commerciali.

"Guardando al futuro, le sfide permangono: identificare e mitigare i rischi in un mercato in continua evoluzione", indica Napolitano. "A livello globale stiamo affrontando cambiamenti significativi, come il mutamento del mercato della difesa e l'emergere di nuove minacce, nei confronti delle quali bisogna trovarsi preparati anche attraverso l'uso di strumenti tecnologici innovativi in ambito cybersecurity e intelligenza artificiale.

Occorre che il processo decisionale, sia strategico che operativo, sia fondato su un approccio di Enterprise Risk Management tale da assicurare l'analisi ed il corretto bilanciamento tra i rischi e le opportunità connessi alle singole iniziative, dall'anticorruzione ai diritti umani.

Tale approccio si traduce, nel day by day, in un dialogo costante tra la funzione di Compliance e le strutture di business, normato dalle procedure aziendali e strutturato attraverso attività condivise di due diligence e risk analysis (ad esempio, al fine di valutare l'opportunità di incaricare un determinato intermediario commerciale, o il livello di sensibilità di una transazione commerciale). In tal modo le funzioni di business non sono, quindi, "oggetti" della compliance, ma "componenti" della compliance.

In che misura l'AI, la tecnologia e le regtech influenzano le attività quotidiane e le dinamiche dei manager che supervisionano le aree di rischio?

L'impiego di strumenti tecnologici così potenti come l'AI presenta enormi potenzialità ma, al contempo, anche rischi di cui non conosciamo ancora bene i contorni. La sfida è quindi capire come garantire la governance etica di questo fenomeno e come intervenire. Certamente la velocità e la potenza con cui, attraverso l'uso di tali strumenti, si possono irradiare determinati fatti illeciti – ad esempio rispetto alla compromissione dei diritti della persona – rende prioritario un intervento tempestivo.

È quello che tutto il mondo sta iniziando a fare, agendo e reagendo sia a livello culturale che normativo/operativo (è notizia di questi giorni l'approvazione definitiva del Regolamento Europeo sull'Intelligenza Artificiale).

Si tratta, infatti, prima di tutto di una questione culturale. Credo che non serva alimentare la paura dell'utilizzo dell'AI e delle nuove tecnologie, di cui sempre più non potremo fare a meno. Come manager, ritengo si debba promuovere uno human centered approach, ponendosi domande quali "*Come poter garantire che la titolarità dell'azione resti sempre in capo all'attore umano che governa i sistemi di AI?E come salvaguardare la libertà dell'essere umano di ignorare una decisione o una raccomandazione presa dalla AI se ciò potrebbe causare danni?*".

Per farsi trovare pronti, i manager dovranno avere sempre più un profilo multidisciplinare che affianchi alle competenze specifiche la capacità di interpretare dati e comunicare efficacemente con le funzioni di IT.

A livello operativo, le aziende – così come le Pubbliche Amministrazioni – si stanno orientando sempre più verso l'applicazione di soluzioni digitalizzate ai propri processi. Per cavalcare quest'onda, Leonardo ha istituito al proprio interno i Leonardo Labs,

Credo che non serva alimentare la paura dell'utilizzo dell'AI e delle nuove tecnologie, di cui sempre più non potremo fare a meno. Come manager, ritengo si debba promuovere uno *human centered approach*.

un'infrastruttura trasversale a tutte le Divisioni, orientata alla ricerca e all'innovazione, dedicata allo sviluppo di nuove tecnologie in ambiti strategici per l'azienda.

Questa migrazione pone sicuramente al centro il tema della sicurezza delle informazioni. Leonardo può contare su un sistema avanzato di gestione della sicurezza delle informazioni aziendali, certificato ISO 27001, che prevede azioni continue di training&awareness rivolte a tutti i propri dipendenti, volte a tenere viva l'attenzione e la consapevolezza di tutti su questi temi.

La domanda che avrebbe voluto sentirsi fare e che non è stata fatta?

Quanto influisce il fattore umano sul raggiungimento degli obiettivi dell'organizzazione? Tantissimo. Possiamo avere un solido impianto procedurale ed un'organizzazione perfettamente strutturate, ma se il fattore umano fallisce è quello che produce il danno.

Possiamo avere un solido impianto procedurale ed un'organizzazione perfettamente strutturate, ma se il fattore umano fallisce è quello che produce il danno. Credo che per valorizzare il fattore umano sia fondamentale stimolare nelle persone un sano senso di appartenenza all'azienda che dia loro la motivazione per contribuire con le loro migliori energie alla prosperità dell'organizzazione

In Leonardo l'attenzione alle persone si traduce in un impegno trasversale sui temi delle competenze (ad esempio promuovendo percorsi STEM) e dell'inclusione, ma anche nel concepire un'offerta formativa a supporto del rafforzamento e dello sviluppo delle competenze delle persone, nonché della cultura aziendale sui temi di compliance a normative interne ed esterne. Aggiungo una considerazione: credo che per valorizzare il fattore umano sia fondamentale stimolare nelle persone un sano senso di appartenenza all'azienda che dia loro la motivazione per contribuire con le loro migliori energie alla prosperità dell'organizzazione.

Elena Napolitano
Chief Compliance Officer Leonardo

Lamborghini

Tutela e gestione dei dati, un valore strategico per l'azienda

di Matteo Rizzi

In un mondo sempre più

digitalizzato, la gestione dei dati e la sicurezza informatica rappresentano pilastri fondamentali per le aziende. Per ottenere risultati di successo in termini di gestione dei dati e della sicurezza informatica servono la consapevolezza e il supporto di tutti i membri dell'organizzazione.

Di conseguenza, la prevenzione e il rispetto delle normative devono essere considerati in un'ottica strategica. Rappresentano modi per tutelare il patrimonio informativo, preservare la reputazione aziendale e garantire il raggiungimento di obiettivi sostenibili.


Elisa Romano

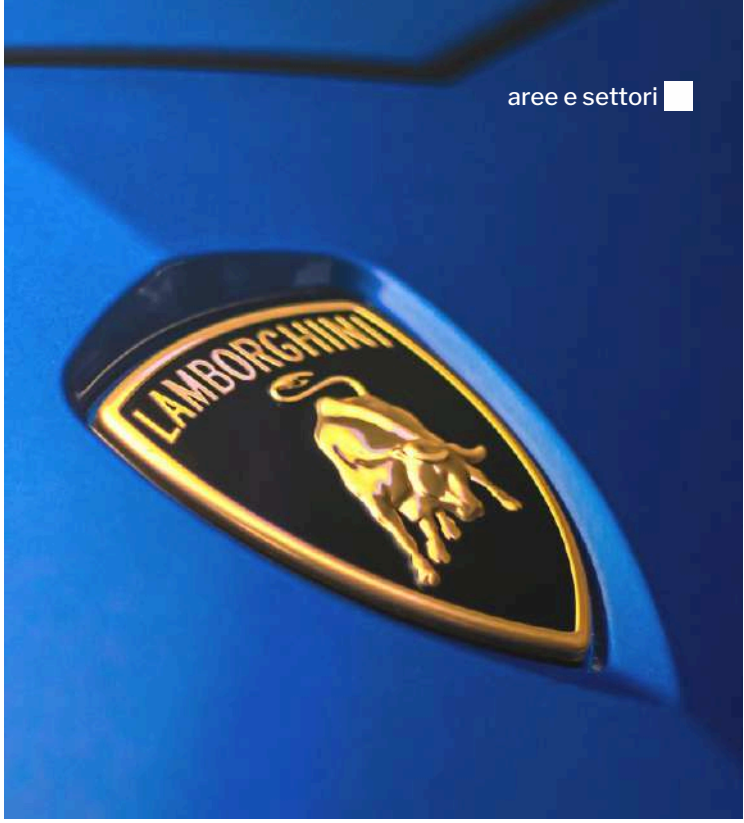
Per capire come una realtà come Automobili Lamborghini affronta queste sfide, ***compliancedesign.it*** ha incontrato **Elisa Romano**, Head of Data Protection & Information Security di Lamborghini.

La tutela e la gestione dei dati dei clienti non sono solo un obbligo legale, ma rappresentano anche un valore strategico per l'azienda.

I dati dei clienti sono fondamentali per lo sviluppo dei prodotti e servizi

"Il mio compito principale è quello di gestire correttamente tutti i trattamenti delle informazioni classificate, compresi i dati personali, che sono di valore strategico per l'azienda. La mia responsabilità è garantire che l'intera organizzazione abbia gli strumenti necessari per trattare le informazioni in modo sicuro, proteggendo il patrimonio informativo e rispettando le normative vigenti a livello italiano, europeo e mondiale", spiega Romano. "Dato che operiamo a livello globale, dobbiamo adattarci anche a normative specifiche di alcuni paesi, come ad esempio la normativa sulla sicurezza informatica in Cina".

Lamborghini parte dalla consapevolezza come pilastro fondamentale, "poiché la maggior parte degli incidenti (80-90%) è causata da errori umani". Oltre alle tecnologie di supporto, l'azienda investe quindi molto nella formazione e nella sensibilizzazione del personale sull'importanza della sicurezza informatica. "Anche se sappiamo che la sicurezza al 100% non è possibile, consideriamo questo aspetto come uno dei passaggi fondamentali per garantire una sicurezza informatica efficace".



Come detto, la tutela e la gestione dei dati dei clienti non sono solo un obbligo legale, ma rappresentano anche un valore strategico per l'azienda. I dati dei clienti sono fondamentali per lo sviluppo dei prodotti e servizi. "La gestione dei dati avviene con grande attenzione e cura, poiché il legame tra il nostro brand e i nostri appassionati è molto speciale". Dalla tutela dei dati alla qualità e all'etica nella gestione, l'azienda si impegna a garantire un'eccellenza operativa in tutti gli aspetti, compresa la reputazione, "poiché siamo consapevoli che il lusso non riguarda solo il prodotto finale, ma anche l'intera esperienza e il rapporto con i nostri stakeholder".

La tutela del patrimonio informativo serve inoltre per proteggere i nuovi prodotti, le strategie e le decisioni aziendali. "Nel nostro settore, che coinvolge un pubblico particolarmente attento e esigente, la protezione del segreto industriale è vitale". L'attenzione e l'interesse suscitati attorno a nuovi prodotti, come ad esempio il lancio della Revuelto nel 2023, sono parte del successo della casa automobilistica.

Le terze parti

Un tema fondamentale che attualmente si sta gestendo con grande attenzione, e che diventerà ancora più importante con l'introduzione della NIS2, è la corretta gestione delle terze parti con cui l'azienda collabora. "Questo è particolarmente critico quando si tratta di dati confidenziali o segreti relativi alle automobili Lamborghini, poiché è fondamentale che tali terze parti rispettino rigorose regole di sicurezza".

Lamborghini conduce verifiche sin dalla fase di selezione e ingaggio dei fornitori, per assicurare che dispongano di una solida postura di sicurezza e un livello di maturità tale da potersi affidare nella trasmissione di informazioni

La tutela del patrimonio informativo serve inoltre per proteggere i nuovi prodotti, le strategie e le decisioni aziendali. Nel nostro settore, che coinvolge un pubblico particolarmente attento e esigente, la protezione del segreto industriale è vitale

sensibili, sia di natura tecnica che dati personali. Queste verifiche includono la valutazione dei requisiti di professionalità e competenza, che vengono successivamente tradotti in audit sulla consapevolezza, la competenza e l'infrastruttura di sicurezza.

Le certificazioni

In tema di sicurezza informatica, Lamborghini ha completato con successo una prima certificazione secondo la norma ISO 27001, la quale regola l'Information Security Management System (ISMS).

L’azienda ha quindi deciso di estendere la certificazione alla norma ISO 27701, che riguarda specificamente la gestione dei dati personali (Personal Information Management System - PIMS). “Questo ci ha permesso di avere una misurazione esterna delle nostre pratiche e procedure, e di garantire un elevato standard di eccellenza operativa che coinvolge l'intera azienda”, sottolinea Romano. “Ottenere questa certificazione è stata una sfida, poiché non è diffusa a livello nazionale, ma abbiamo ritenuto importante avere un riconoscimento esterno del nostro impegno per garantire la protezione dei dati personali e la conformità alle normative internazionali”.

Ottenere e mantenere le certificazioni ISO potrebbe essere un percorso sfidante ma che crea vantaggi specifici. “In primo luogo, una volta ottenuta la certificazione, è necessario mantenerla annualmente".

L’azienda ha deciso di estendere la certificazione alla norma ISO 27701, che riguarda specificamente la gestione dei dati personali (Personal Information Management System - PIMS).

Questo ci ha permesso di avere una misurazione esterna delle nostre pratiche e procedure, e di garantire un elevato standard di eccellenza operativa che coinvolge l'intera azienda

Questo obbliga l'azienda a tenere aggiornata tutta la documentazione, a effettuare verifiche periodiche e a “non abbassare mai la guardia”. Inoltre, queste attività portano ad avere un calendario di scadenze che contribuisce a “ricontrollare e migliorare continuamente i processi”. Ciò consente di individuare eventuali punti deboli o aree non ancora ben coperte dalle normative, spingendo l'azienda a strutturare meglio i processi e le procedure.

Un altro aspetto positivo riguarda il coinvolgimento di tutta l'organizzazione in questi percorsi. “Questo aumenta notevolmente la consapevolezza dei dipendenti riguardo alla protezione dei dati e alla sicurezza informatica”, il che è importante perché la gestione dei dati e la sicurezza informatica non riguardano solo il team responsabile della protezione dei dati, “ma coinvolgono l'azienda nel suo complesso”. Questo prepara l'azienda ad affrontare con successo audit e verifiche, coinvolgendo tutti i dipartimenti e garantendo un approccio olistico a questi importanti temi. Oltre al beneficio interno, la certificazione può essere utilizzata anche a livello di marketing, comunicando ai clienti e ai partner che l'azienda gestisce correttamente i dati e adotta le migliori pratiche nel campo della sicurezza informatica.

Tra sostenibilità e intelligenza artificiale

Il tema della sostenibilità e dell'etica dei dati rappresentano una naturale estensione del percorso di corretta gestione dei dati. Raccogliere e conservare solo i dati necessari, un principio fondamentale della GDPR noto come "necessarietà", è cruciale anche dal punto di vista della sostenibilità. Più dati si possiedono, maggiori sono i rischi associati, come la perdita di dati, l'accesso non autorizzato e i potenziali breach di sicurezza.

Questi rischi possono portare a danni all'immagine dell'azienda, sanzioni e costi aggiuntivi. “Pertanto, gestire un patrimonio informativo in modo mirato, conservando solo i dati effettivamente utili per raggiungere gli obiettivi aziendali e ambientali, è di fondamentale importanza”.

Questo approccio si allinea anche al principio della "Net 1.0" in materia di Information Security, il quale richiede che i dati siano disponibili, integri e gestiti correttamente in base alla loro confidenzialità e classificazione. “Rispettare questi principi non solo riduce i rischi per l'azienda, ma contribuisce anche a garantire un uso etico dei dati, evitando attività che non siano in linea con lo scopo per cui i dati sono stati raccolti”.

L'intelligenza artificiale in tema di salvaguardia dei dati è un argomento di grande rilevanza e attualità, come dimostrato anche dall'intervento del Garante per la protezione dei dati personali. “L'adozione di questi strumenti comporta una serie di rischi che vanno gestiti con attenzione”. Uno dei rischi principali è che all'interno di un'organizzazione vengano trattati dati confidenziali o segreti in modo improprio, uscendo dal perimetro aziendale o violando la privacy di persone fisiche. “Ciò potrebbe portare a violazioni delle normative sulla protezione dei dati, violazioni della proprietà intellettuale e brevetti di terze parti, con tutte le conseguenze legali e reputazionali che ne derivano”. Questi rischi devono essere affrontati e gestiti adeguatamente, soprattutto considerando che l'utilizzo dell'intelligenza artificiale è sempre più diffuso sia nell'ambito aziendale che a livello personale. “È importante che le organizzazioni adottino politiche e procedure rigorose”.

Il futuro della data-driven economy è già realtà, ma è fondamentale che il progresso tecnologico avvenga nel rispetto dei principi etici e della sostenibilità. “È responsabilità dei legislatori, delle aziende e di tutti gli attori coinvolti indirizzare correttamente questo progresso, assicurando che sia compatibile con il rispetto dei diritti e della dignità delle persone e con la tutela dell’ambiente".

AITRA
ASSOCIAZIONE ITALIANA
TRASPARENZA E ANTICORRUZIONE

LE SFIDE DELLA *COMPLIANCE* INTEGRATA PER FRONTEGGIARE I RISCHI: RUOLO DI AUTORITÀ INDIPENDENTI, MAGISTRATURA, P.A. E OPERATORI ECONOMICI

PROGRAMMA E RELATORI

ore 09:30 - 10:00
Accredito e Welcome coffee

SALUTI DI APERTURA

Giorgio Martellino
AITRA *Presidente*

INTERVENTI ISTITUZIONALI

Luca Forteleoni
Consigliere ANAC

Guido Scorza
Componente del Collegio del Garante per la protezione dei dati personali

Giovanni Calabrò
Capo di Gabinetto dell'Autorità Garante della Concorrenza e del mercato

Mauro Orefice
Magistrato Presidente di sezione della Corte dei Conti

INTERVENTI

Stefano Toschei
Consigliere di Stato e Presidente del Comitato Scientifico di AITRA

Alessandro De Nicola
Partner di Bonelli Erede e membro del Comitato Scientifico di AITRA

ROUNDTABLE

Introduce e modera

Paola Balducci
Docente Procedura Penale LUISS Guido Carli, Responsabile Centro Studi Camera Penale di Roma, Membro del Comitato Scientifico AITRA

Michela Adinolfi
Data Protection Officer TERNA

Antonio Enrico Agovino
Head of Risk Compliance & Corporate Security - DPO INWIT

Nicola Allocca
Risk, Business Integrity, Resilience and Quality Director Autostrade per l'Italia

Giorgio Centurelli
Direttore Generale del Ministero dell'ambiente e della sicurezza energetica

Valentina Laroccia
Anticorruption, Antitrust & Financial Regulation Compliance Eni Plenitude

Aristide Police
Professore ordinario di Diritto amministrativo LUISS e membro del Comitato Scientifico AITRA

ore 13:00 soft lunch

REGISTRATI

In fase di accreditamento presso il Consiglio dell'Ordine degli Avvocati di Roma per la modalità in presenza

ROMA, 3 GIUGNO 2024 I ORE 09:30

Ceida – Scuola Superiore di Amministrazione Pubblica e degli Enti Locali
Aula Magna, Via Palestro, 24

CEIDA
ALTA FORMAZIONE DAL 1980

media partner
compliance design

Aeroporti di Roma

Una compliance semplice e integrata a sostegno dei process owner

di Matteo Rizzi

Obiettivi ambiziosi richiedono

sistemi di controllo strutturati, anche vista la crescente complessità normativa e la necessità di gestire un set di rischi in continua evoluzione. In questo contesto, Aeroporti di Roma (ADR) emerge come best practice nell'adozione di approcci innovativi, multidisciplinari e integrati per garantire la conformità normativa, la gestione efficace dei rischi e la resilienza del business.

compliancedesign.it ha incontrato **Lorenzo Rinaldi**, *Chief Risk Officer e Vice President Risk Governance & Compliance* di Aeroporti di Roma.

Le organizzazioni hanno infatti la responsabilità di contribuire attivamente alla lotta a frodi e corruzione, consapevoli che le normative di riferimento rappresentano un elemento necessario ma non sufficiente a contrastare tali fenomeni, ma sono la base da cui partire per costruire una cultura aziendale e del modo di operare delle società.

Trasparenza, integrità e rispetto delle regole sono dei pilastri su cui si basano le attività quotidiane di ADR, insieme all'innovazione, alla qualità e alla sostenibilità. In tale contesto, anche al fine di supportare al meglio il raggiungimento di questi obiettivi, "la società negli ultimi anni ha ulteriormente rafforzato le strutture di controllo a presidio dei principali rischi e sviluppato modelli integrati e smart per una gestione efficace degli stessi", spiega Rinaldi.

"In un ambiente così complesso come il nostro è importante dotarsi di strumenti efficaci di contrasto e prevenzione dei fenomeni di illegalità che hanno impatto negativo non solo su di noi, ma sull'intera collettività, come ad esempio le frodi e la corruzione".

Le organizzazioni hanno infatti la responsabilità di contribuire attivamente alla lotta a frodi e corruzione, "consapevoli che le normative di riferimento rappresentano un elemento necessario ma non sufficiente a contrastare tali fenomeni, ma sono la base da cui partire per costruire una cultura aziendale e del modo di operare delle società".

A tal fine, ADR si è dotata di un Sistema di Gestione per la prevenzione della corruzione secondo lo standard internazionale ISO 37001:2016, certificazione recentemente rinnovata da ADR per il triennio 2024-2027, ed ha definito un Modello Antifrode per la gestione dei rischi e per diffondere la cultura dell'integrità promuovendo i valori e i principi in grado di sostenere comportamenti virtuosi.

In un contesto in cui la proliferazione normativa ha caratterizzato complessivamente i diversi settori economici (e ancor più significativamente i settori regolamentati), a cui si aggiungono anche le norme esterne volontarie (es. norme ISO) e le forme di autoregolamentazione interna, un approccio disomogeneo alla compliance comporta il rischio di allocare le risorse in base alla spinta di fattori contingenti e soggettivi, quindi non in modo ottimale, con approcci frammentati e a "silos".

Diventa quindi cruciale attuare un processo di compliance integrata, ovvero implementare metodologie di compliance coerenti tra loro per le diverse normative, utilizzando un linguaggio comune e consentendo la comparabilità dei risultati delle diverse attività, che, in un contesto complesso, abilita una serie di benefici tra i quali, ad esempio, la possibilità di pianificare in modo integrato le diverse attività di compliance connesse alle varie normative, svolgere le attività di verifica e di audit in logica multi-compliance, integrare e razionalizzare le azioni sul Sistema di Controllo Interno e di Gestione dei Rischi, semplificando l'attività di follow up delle stesse.

"In questo modo è possibile sia ridurre l'effort delle strutture di controllo e dei process owner sia affrontare la compliance in modo evoluto e maturo, consentendo alle funzioni di controllo anche di supportare il management nell'identificazione, valutazione e gestione dei rischi di conformità associati alle decisioni di business, per promuovere scelte consapevoli e coerenti con il profilo di rischio atteso dagli stakeholder, fin dalla fase di pianificazione strategica".

Lorenzo Rinaldi

Gestire in modo integrato e uniforme le nostre terze parti nell'intero ciclo di vita del rapporto - dalla fase di identificazione e qualifica, fino alle attività di monitoraggio delle performance e della compliance - supera una visione frammentata e parziale dei rischi attraverso un approccio olistico.

Complessità significa anche operare in un ecosistema composto da una pluralità di stakeholder ampia e diversificata - vettori, handler, subconcessionari, fornitori - i cui rischi associati possono ricadere direttamente o indirettamente sul gestore aeroportuale.

Un lavoro di tutta l'organizzazione

Servono comunicazione e formazione nella costruzione di una cultura diffusa del rispetto delle norme e della legalità, ma al di là di ogni implementazione tecnica, le organizzazioni sono fatte da persone con una propria storia, una propria percezione e sensibilità, distinte e diverse. "L'errore più comune nasce nel pensare di poter implementare un Sistema di Controllo e di Gestione dei Rischi che non sia su misura".

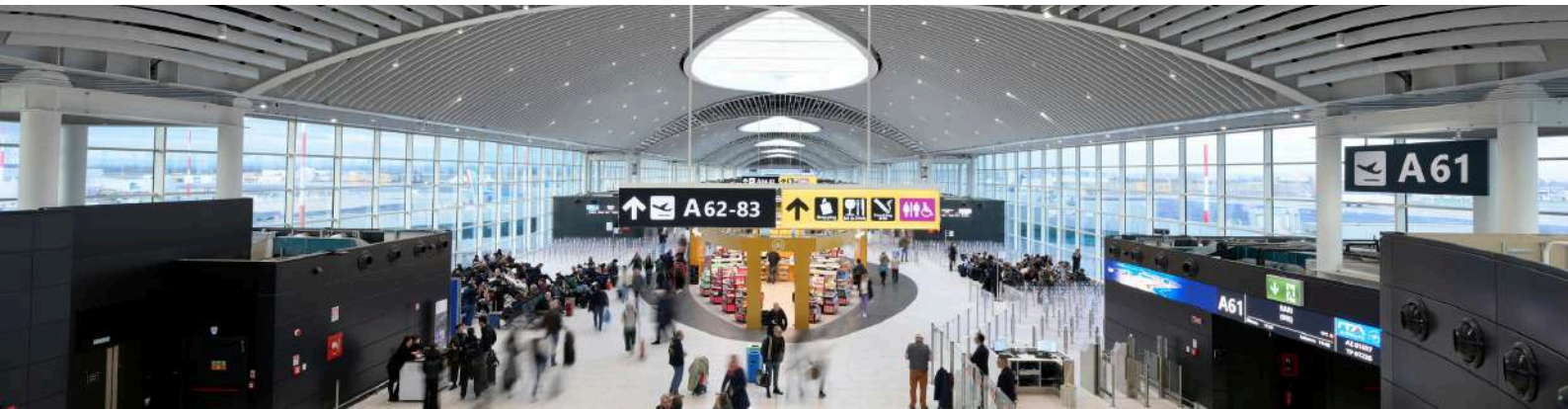
Ogni forma di trasformazione o mitigazione dei rischi dipende fondamentalmente dalle azioni della leadership. "Pertanto, il concetto di coerenza tra parole e azioni è fondamentale, oltre a quello del l*ead by example* della leadership.
Inoltre, la pluralità di attori coinvolti ed il contesto normativo ed organizzativo in continua evoluzione rendono il processo di gestione dei rischi articolato con il pericolo di creare sovrastrutture che non facilitano di certo l'integrazione: la soluzione è semplificare il processo.

Questo può avvenire sia attraverso una compliance integrata, riducendo i requisiti a pochi e rendendo il processo di conformità più chiaro, sia attraverso la comprensione dei compiti e degli obiettivi di ciascun requisito normativo.

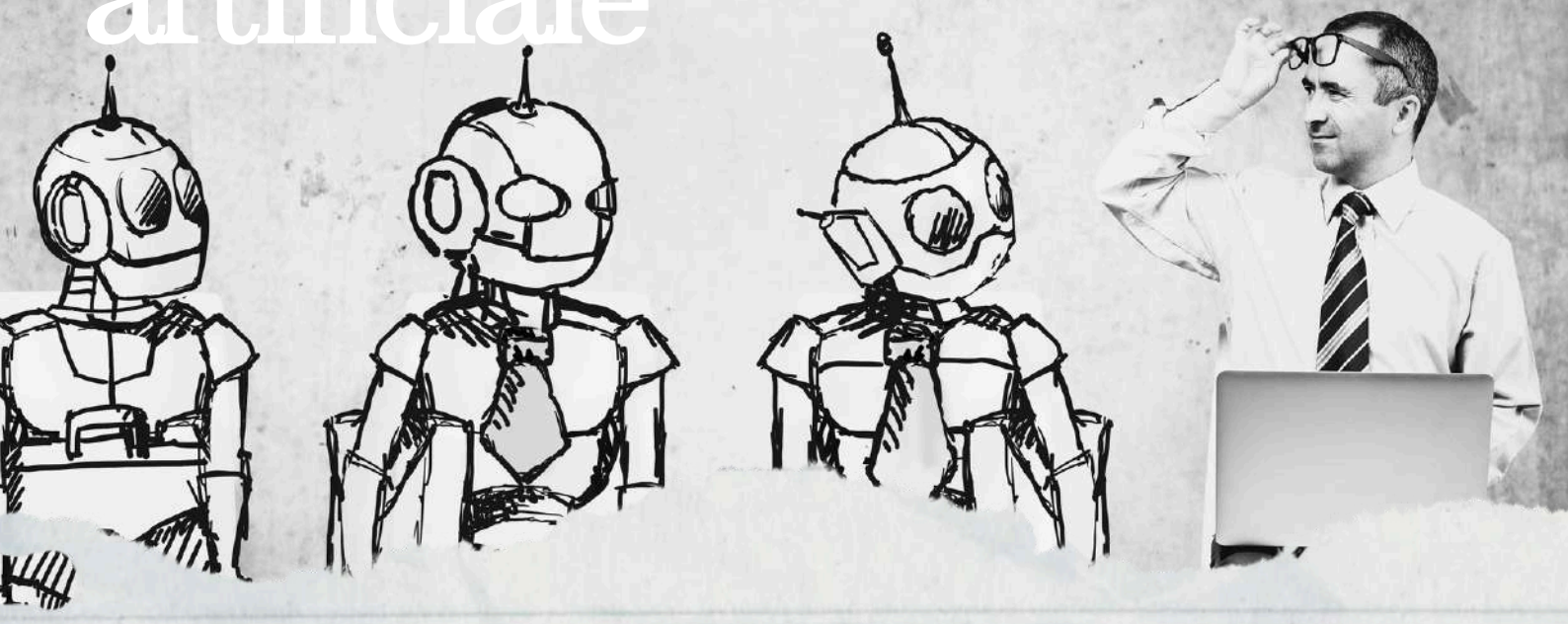
"Se la compliance è percepita come un rallentamento o un'imposizione dall'alto, ciò può influenzare negativamente i process owner che potrebbero vedere la compliance come un ostacolo al loro lavoro e al raggiungimento degli obiettivi".

Al contrario, è fondamentale che le funzioni di compliance siano "più consulenti e advisor". È quindi necessario semplificare il più possibile i messaggi, i requisiti e il lavoro che i responsabili dei processi devono svolgere. La formula è quella di "fornire una sorta di *plug and play* delle azioni necessarie, supportando i process owner nell'applicazione pratica". Un obiettivo che si facilita attraverso un modello integrato.

È necessario semplificare il più possibile i messaggi, i requisiti e il lavoro che i responsabili dei processi devono svolgere. La formula è quella di fornire una sorta di 'plug and play' delle azioni necessarie, supportando i process owner nell'applicazione pratica. Un obiettivo che si facilita attraverso un modello integrato.



L'intelligenza artificiale



La mia nuova e-assistant in cloud globale,
suggerisce cose inutili da fare.
E caricando un dato camerale,
me l'ha tradotto in lingua medioevale.
La foto di mia suocera, a Natale,
è pubblica sull'intranet aziendale.
In questo mondo di rivoluzione digitale
Io predico il ritorno all'intelligenza artigianale.

Barney R.

compliance design

COMPLIANCE, KNOWLEDGE & NETWORKING