Newsletter

Nr. 1/2024 Dicembre 2024

Providing
Compliance Solutions
in a complex world

HIMMEL
ADVISORS
www.himmeladvisors.it

www.himmeladvisors.it/newsletter

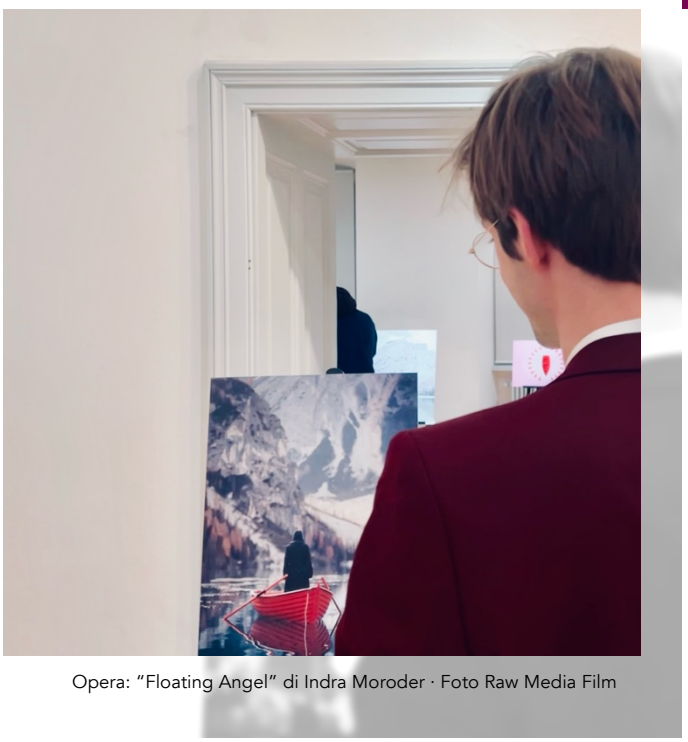
La presente Newsletter è stata elaborata da HIMMEL ADVISORS e viene resa disponibile gratuitamente sul relativo sito web. Si tratta di un documento informativo che ha lo scopo di fornire aggiornamenti e approfondimenti su temi rilevanti per gli interessati, aiutandolo a rimanere informato sulle ultime novità e tendenze del settore. Si specifica che non si assumono responsabilità alcuna in merito ai contenuti o al loro utilizzo.

Ulteriori informazioni
www.himmeladvisors.it

Impresa dell'
ALTO ADIGE

sommario

benvenut*



Opera: "Floating Angel" di Indra Moroder · Foto Raw Media Film

Ogni articolo, analisi e riflessione che troverete qui è concepito non solo per informarvi, ma per stimolare un dialogo costruttivo e per incoraggiarvi ad approcciare le sfide della *Compliance* con serenità e determinazione. La Vostra fiducia rappresenta per noi un onore, e aspiriamo a mantenerla, nel corso degli anni, con impegno verso la professionalità ed eccellenza che ci contraddistingue.

Nella newsletter di questo novembre 2024, ci sembra appropriato dedicare una riflessione anche a un tema di vitale importanza, come si evince dall'immagine di copertina (opera di H. Armstrong Roberts) e dall'immagine di cui sopra – scattata lo scorso 25 novembre 2024 in occasione della mostra "Das rote Boot" organizzata dalla Südtiroler Künstlerbund presso la SKB ARTES di Bolzano in occasione della "Giornata internazionale per l'eliminazione della violenza contro le Donne".

La violenza di genere è un'ombra che si estende, ancora nei nostri anni, nel contesto aziendale. Le sue ripercussioni si avvertono ben oltre l'immediato. Essa interroga il nostro senso di giustizia, uguaglianza e umanità. Come professioniste e professionisti ma, soprattutto, come membri della nostra Comunità, abbiamo la responsabilità di partecipare attivamente alla creazione di un ambiente che non tolleri la violenza, ma promuova il rispetto e la dignità per tutte e per tutti.

Carissimi Lettori,

È con entusiasmo e profonda gratitudine che vi presentiamo il primo numero della nostra Newsletter, uno strumento dedicato a esplorare e discutere le dinamiche complesse del mondo della *Compliance* aziendale. In un'epoca in cui le normative e le responsabilità aziendali sono in costante cambiamento, diventa imperativo per professioniste, professionisti e aziende non solo adeguarsi, ma anche anticipare le sfide che potrebbero sorgere nei prossimi mesi in ambito privacy, whistleblowing, trasparenza amministrativa, 231 e NIS2.

La nostra Newsletter bimestrale si presenta come una risorsa (speriamo) utile, volta a facilitare la comprensione e l'approfondimento delle tematiche normative, etiche e operative che modellano il nostro settore. Essa intende anche informare i nostri iscritti sui principali articoli pubblicati da Himmel Advisors e sulle novità della nostra Organizzazione.

Ciò che distingue la nostra società non è soltanto la competenza e la professionalità che portiamo nel nostro operato, ma anche la nostra visione: crediamo fermamente nel potere della conoscenza condivisa.

HIMMEL: un'idea che nasce da valori profondi

"Himmel", che in tedesco significa "cielo", rappresenta la nostra aspirazione a raggiungere le vette più alte in ogni aspetto della nostra attività di consulenza. Questo nome non è solo una parola, ma un impegno verso l'eccellenza, l'innovazione e il servizio impeccabile.

Himmel Advisors incarna la visione di una consulenza che non si limita a fornire soluzioni, ma che punta a ispirare e guidare i nostri clienti verso la compliance aziendale a 360°. Crediamo fermamente che ogni progetto possa raggiungere altitudini straordinarie quando supportato, sempre, da una guida esperta e lungimirante.

Il nostro nome riflette i valori della nostra realtà: ampiezza di vedute, trasparenza, professionalità e un impegno a guardare oltre l'orizzonte. Siamo determinati a stabilire relazioni di fiducia e a fornire un supporto che significhi crescita e prosperità durature per i nostri Partner.

Con questo spirito, ci accingiamo a esplorare i contenuti di questa Newsletter, certi che ognuno di Voi ne trarrà spunto e ispirazione.

Buona lettura!

Francisco Garcia
Partner & Legal Counsel

sezione Grigia

Articoli di interesse

In questa sezione, vi presentiamo una raccolta di articoli che sono stati pubblicati nella sezione 'News' del nostro sito web www.himmeladvisors.it/news Abbiamo pensato di includerli qui per offrire ai nostri lettori un'opportunità unica di esplorare una panoramica completa di tutti i temi e gli argomenti di interesse che sono stati trattati negli ultimi due mesi.

Questa raccolta non solo facilita l'accesso a contenuti preziosi, ma consente anche di rivisitare e approfondire articoli che potrebbero risultare rilevanti per le vostre esigenze aziendali o professionali. Siamo certi che questi contributi offriranno spunti utili e informazioni aggiornate, aiutandovi a rimanere informati sulle tendenze e gli sviluppi del nostro settore. Invitandovi a sfogliare questi articoli, speriamo di stimolare la vostra curiosità e di favorire una continua crescita e apprendimento.

HIMMEL ADVISORS
www.himmeladvisors.it

1 L'accettazione della Nomina ad Incaricato Privacy: Un Obbligo per i Dipendenti? Un'analisi alla luce della recente Ordinanza del Tribunale di Udine

Sintesi

Nel panorama giuridico attuale, la questione della privacy e del trattamento dei dati personali assume un ruolo sempre più centrale, specialmente alla luce del Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea. Un punto di discussione rilevante è se un dipendente possa legittimamente rifiutare la nomina come incaricato del trattamento di dati personali.

Recentemente, una pronuncia del Tribunale di Udine ha sollevato interrogativi significativi su questo tema. Un'ordinanza emessa in tale sede ha esaminato il caso di un dipendente sospeso dal proprio datore di lavoro a causa del suo rifiuto di accettare formalmente la nomina a "incaricato privacy". Tuttavia, un esame approfondito dei fatti di causa mostra che la sospensione non è stata determinata dalla semplice riluttanza a firmare la nomina, ma da una condotta contraria agli obblighi contrattuali. Nello specifico, il dipendente si era rifiutato di trattare dati essenziali per lo svolgimento delle proprie mansioni, compromettendo così il patto fiduciario tra lui e l'azienda.

Il testo della sentenza è disponibile qui

Il Cliente si domanda...

Ma questa lettera di incarico dev'essere "obbligatoriamente" sottoscritta dal dipendente? Vi sono delle responsabilità in capo al datore di lavoro (che agisce quale Titolare del trattamento) qualora non richieda la sottoscrizione della stessa?

Himmel risponde:

È fondamentale comprendere che, ai sensi del GDPR, **non è richiesta la sottoscrizione di una lettera di incarico "formale" da parte dei dipendenti** per essere considerati incaricati del trattamento. L'articolo 29 del GDPR stabilisce che chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento, inclusi i dipendenti, deve trattare i dati personali attenendosi alle istruzioni impartite da tali figure.

> ***Art. 29 GDPR (sottratto dal testo integrale del Regolamento (UE) 2016/679 del 27 aprile 2016)***
> *Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*

Le c.d. lettere di incarico devono essere notificate ma non necessariamente accettate formalmente tramite sottoscrizione. **La distinzione chiave in questo contesto** risiede tra l'obbligo di conformarsi alle direttive dell'azienda riguardo al trattamento dei dati e l'atto formale di accettare una lettera di incarico formale. Mentre il primo è un obbligo legale per il dipendente, il secondo può essere considerato più che altro un formalismo. La mancata conformità alle

direttive operative in materia di privacy, invece, può costituire una violazione del rapporto di lavoro e giustificare provvedimenti disciplinari, in quanto compromette l'efficienza operativa e la sicurezza dei dati aziendali.

Di particolare importanza è, invece, **l'obbligo di "istruire" il personale** coinvolto nel trattamento dei dati personali.

Qual è la valenza giuridica di una lettera di incarico, eventualmente sottoscritta da un dipendente, che non include le istruzioni dettagliate per il corretto trattamento dei dati personali né le misure di sicurezza tecniche e organizzative necessarie da seguire?

In conclusione, è sempre consigliabile che le aziende spieghino chiaramente ai propri dipendenti i loro obblighi in materia di protezione dei dati e le conseguenze del mancato adempimento. L'obbligo di **formazione** e di **istruzione** è fondamentale. Ma attenzione: è importante sottolineare che i datori di lavoro sono tenuti per legge a fornire ai propri dipendenti tutte le risorse e gli strumenti necessari per svolgere le loro attività e trattare i dati in modo lecito, organizzato e sicuro, conformemente alla normativa vigente.

Questo caso sottolinea l'importanza di un **approccio equilibrato tra il dovere** di protezione dei dati e i **diritti e obblighi** dei dipendenti, che continua a evolvere nel quadro di applicazione del GDPR e delle normative correlate. Un'efficace politica di formazione e comunicazione interna può prevenire incomprensioni e garantire la conformità normativa dell'organizzazione.

Leggi l'articolo online su www.himmeladvisors.it — Link esterno

2 Valutazione dei canali di Segnalazione Whistleblowing alla luce della Direttiva NIS2 e del D. Lgs. 138/2024

Sintesi

Nel contesto attuale, la protezione dei dati e la sicurezza informatica sono cruciali. Con l'entrata in vigore del D. Lgs. 138/2024, che recepisce la Direttiva NIS2, il monitoraggio continuo delle performance dei fornitori dei canali interni per la raccolta e gestione delle segnalazioni Whistleblowing diventa cruciale. La normativa applicabile insta le organizzazioni all'effettuazione di analisi periodiche e revisioni delle policy di sicurezza interne per garantire un allineamento costante con gli obblighi normativi. Le aziende devono predisporre valutazioni regolari del rischio per identificare eventuali falle nel sistema e sviluppare piani di risposta efficaci in caso di potenziali violazioni o "fuga di dati".

Nel contesto aziendale attuale, la protezione dei dati e la sicurezza informatica stanno assumendo un ruolo di primo piano a causa di un **panorama normativo sempre più complesso** e di una crescente attenzione alla trasparenza e alla necessità di compliance aziendale. Circa un anno fa, entrava in vigore nell'ordinamento italiano il D. Lgs 24/2023 di recepimento della **Direttiva (UE) 1937/2019 sul Whistleblowing**, recentemente aggiornato con riguardo agli illeciti cui è applicabile (in particolare quelli relativi ai mercati delle cripto-attività ai sensi del D. Lgs 129/2024 recante l'adeguamento delle norme nazionali al Regolamento (UE) 1114/2023 – c.d. MICA).

Ricordiamo che il termine "whistleblowing" si riferisce all'atto volontario attraverso il quale un individuo, denominato "segnalante" o "whistleblower", comunica una condotta illecita o un'irregolarità verificatasi all'interno di un'organizzazione, di cui abbia avuto conoscenza nel contesto lavorativo. Il segnalante, sebbene frequentemente identificato con un dipendente dell'organizzazione, può altresì essere un soggetto esterno (es. un fornitore o un ex tirocinante). In questo contesto, il legislatore europeo, mediante la Direttiva UE 1937/2019, ha inteso promuovere l'adozione, da parte delle organizzazioni sia pubbliche che private, di sistemi strutturati per la raccolta e la gestione di segnalazioni Whistleblowing. Questi canali devono essere progettati per garantire la riservatezza delle informazioni ricevute e la protezione dell'identità dei segnalanti. L'obiettivo è quello di favorire un ambiente in cui le segnalazioni di (potenziali) illeciti possano essere effettuate in modo sicuro e protetto, preservando l'integrità delle procedure interne e indirizzando tempestivamente le eventuali violazioni in conformità con i requisiti normativi stabiliti a livello europeo.

Il recente recepimento della Direttiva NIS2 attraverso il Decreto Legislativo 138/2024 crea una **nuova cornice di riferimento per le organizzazioni, siano pubbliche o private**, spingendo verso un rafforzamento della sicurezza nei processi di gestione delle segnalazioni ma anche riguardo la scelta del canale interno tramite cui poter raccogliere e gestire le segnalazioni.

L'implementazione della Direttiva NIS2 si propone di **rafforzare la resilienza informatica** in tutta l'Unione Europea, ampliando l'ambito dei soggetti obbligati e introducendo requisiti più stringenti per la prevenzione e la gestione degli incidenti di sicurezza. Questo impone ai **soggetti operanti nel settore dei servizi TIC quali i fornitori di piattaforme Whistleblowing** (di cui all'Allegato I – Settori ad alta criticità) di intraprendere un'attenta revisione delle loro infrastrutture tecnologiche. Devono garantire che le misure di sicurezza siano, *granularmente*, **integrate e aggiornate per rispondere efficacemente agli standard richiesti** (specificatamente gli obblighi in materia di "misure di gestione dei rischi per la

sicurezza informativa", di cui all'art. 24 del D. Lgs 138/2024).

È indispensabile che i portali e le piattaforme dedicate garantiscano non solo la **crittografia** dei dati sensibili che potrebbero transitare all'interno ma che **l'accesso alle informazioni sia limitato a personale accuratamente autorizzato**.

A tale scopo, i fornitori devono condurre **audit di sicurezza regolari e *penetration test*** per identificare potenziali vulnerabilità. Questi audit devono essere supportati da una **stretta collaborazione con esperti in materia** per assicurare che tutti gli aspetti dei canali interni siano in linea non solo con la Direttiva NIS2 ma anche con altre normative applicabili, come il GDPR ed il Decreto 24/2023 in materia Whistleblowing.

Dal punto di vista delle aziende utilizzatrici, la selezione di questi servizi non può più essere vista semplicemente come una **scelta di convenienza prettamente legata alla questione economica**. Si tratta di un decisivo passo strategico che richiede un'**approfondita valutazione dei potenziali fornitori** oppure delle piattaforme e dei canali già implementati. Le aziende devono eseguire un ***assessment annuale*** per valutare non solo la capacità tecnologica del proprio fornitore, ma anche la loro adesione alle normative in vigore (nello specifico alla Direttiva NIS2 e al D. Lgs. 24/2023). Questo processo dovrebbe includere una verifica delle certificazioni di sicurezza e delle politiche di gestione dei dati messe in atto dal fornitore.

> *Si ricorda che l'art. 27 del D. Lgs. 138/2024 fa rinvio all'uso di schemi di certificazione della cybersecurity al fine di dimostrare il rispetto di determinati obblighi di cui all'articolo 24. Tant'è che l'Autorità nazionale competente NIS promuove, l'utilizzo di servizi fiduciari qualificati da parte dei soggetti essenziali e dei soggetti importanti.*

Un aspetto critico dell'adeguamento alla Direttiva NIS2 da parte dei fornitori di piattaforme e canali di segnalazioni consiste nel **coordinamento interno tra il Dipartimento IT e il DPO** aziendale.

> *Veniva infatti ricordato, quale giorno fa, da Federprivacy nell'articolo di Pasquale Mancino "Whistleblowing e canale esterno di segnalazione: alcuni aspetti da approfondire che il Data Protection Officer deve supervisionare". Fermo restando che entrambe le figure non sono deputate alla gestione delle segnalazioni Whistleblowing e, pertanto, non potrebbero venire a conoscenza delle segnalazioni in corso oppure di quelle precedenti; tale collaborazione – dal punto di vista materiale – è fondamentale per assicurarsi che le piattaforme adottate siano completamente integrate nei sistemi di sicurezza aziendali esistenti e che rispettino tutti i requisiti di compliance pertinenti.*

Leggi l'articolo completo online su www.himmeladvisors.it Link esterno

3 Dolcetto o scherzetto? Il Decreto Legislativo 138/2024 e la sinfonia incompiuta della cybersecurity

Sintesi

Quando si parla di nomine ai sensi dell'art. 28 GDPR possiamo giocare a "Dolcetto o Scherzetto", ma con un significato tutto particolare! Un fornitore ben selezionato con una solida reputazione e prassi sicure è il nostro "dolcetto" preferito, sicuro e senza sorprese! Trascurare la verifica dei fornitori – un brutto tiro che può portare a un incidente di sicurezza o a un audit sgradito. Non c'è niente di peggio che ricevere una sorpresa non gradita quando meno te lo aspetti.

Il 18 ottobre 2024 segna l'entrata in vigore del D. Lgs. 138/2024, che recepisce la Direttiva NIS2. Per le pubbliche amministrazioni e gli operatori dei settori essenziali (e non solo), questo non significa semplicemente **spuntare voci** su una lista di controllo. Si apre una nuova era che richiede un approccio proattivo e strutturale alla sicurezza informatica, ben più complesso di una mera attività di *compliance*.

Si potrebbe pensare: "finalmente una normativa che obbliga ad occuparsi di sicurezza!". E invece, la realtà è un po' più complessa. Perché, diciamocelo, la necessità di implementare misure di sicurezza tecniche ed organizzative non è nata con la NIS2. È come scoprire l'acqua calda nel XXI secolo.

Nel settore pubblico, si parla di misure di sicurezza tecniche e organizzative dalla lontana Circolare AgID n. 61/2013. Il Codice dell'Amministrazione Digitale (CAD), un vero monumento legislativo (e a volte anche un labirinto), contiene numerose disposizioni sulla sicurezza, come l'art. 13-bis, che parla di **Codice di condotta tecnologica ed esperti**. Insomma, la letteratura in materia non mancava. Ma, come direbbe un ottimista (o forse un ingenuo), "la buona volontà non basta mai".

Ma veniamo al dunque. La vera sfida, quella che mette a nudo la fragilità del sistema, non risiede solo nell'adeguamento interno delle PA, ma nella consapevolezza e la sensibilità delle organizzazioni stesse. Pensiamo, ad esempio, alla valutazione tecnica dei fornitori. Il principio di *privacy by design* e *by default* (art. 25 GDPR) impone una valutazione accurata della sicurezza informatica di ogni fornitore prima di affidare un incarico. Immaginiamo la scena: il RUP alle prese con la valutazione di un fornitore. Sarà dotato di un questionario sofisticato? O, peggio ancora, si affiderà al "sentito dire", all'offerta più vantaggiosa o alla fama del fornitore?

Le nomine ex art. 28, a partire dal 18 ottobre 2024, dovrebbero contenere **clausole stringenti** in materia di sicurezza. Basta con la nebulosa responsabilità diffusa. Tali clausole, idealmente, dovrebbero prevedere:

- **Obblighi di sicurezza granitici:** nessuna possibilità di interpretazione ambigua. Misure tecniche e organizzative precise e dettagliate.
- **Procedure di notifica degli incidenti stile "rapida e furiosa":** nessun ritardo, nessun tentativo di insabbiamento. Trasparenza assoluta (o quasi).
- **Obblighi di gestione del rischio da manuale:** valutazione, mitigazione, monitoraggio del rischio... un vero incubo per chi è abituato a lavorare con la filosofia del "vedremo".

- **Clausole contrattuali con responsabilità chiare:** se qualcosa va storto, si sa chi paga il conto.

I NOSTRI CONSIGLI
per affrontare la NIS2

- **Mappatura dei fornitori:** una vera e propria caccia al tesoro per trovare tutti i fornitori, anche quelli nascosti negli angoli più bui della burocrazia.
- **Questionario di valutazione:** un'arma potente, se utilizzata correttamente. Ma attenzione, potrebbe trasformarsi in un'arma a doppio taglio se mal concepito.
- **Monitoraggio continuo:** l'occhio vigile di un grande fratello digitale (ma in versione benevola, ovviamente).
- **Formazione del personale:** l'investimento più importante, anche se spesso sottovalutato.

In definitiva, la NIS2 non è solo una Direttiva da rispettare, ma un'occasione per una vera e propria trasformazione digitale, seguita da misure di sicurezza tecniche ed organizzative adeguate. Una trasformazione che, però, richiede una profonda rivoluzione culturale, oltre che tecnologica. Solo così potremo evitare di trasformare la NIS2 in un'altra sinfonia incompiuta nella lunga storia della digitalizzazione.

Leggi l'articolo online su www.himmeladvisors.it Link esterno

4 Temu sotto la lente: indagine UE tra sicurezza digitale, diritti dei consumatori e privacy

Sintesi

La Commissione Europea ha recentemente annunciato l'avvio di un procedimento formale mirato ad accertare eventuali violazioni da parte di Temu delle normative sui servizi digitali. L'indagine si concentra su diversi ambiti critici che sollevano questioni di conformità e sicurezza e che potrebbero influenzare il mercato unico digitale europeo.

L'indagine analizzerà i meccanismi impiegati da Temu per limitare, ove effettuata, la commercializzazione di beni potenzialmente non conformi all'interno dell'Unione Europea. In particolare, verrà esaminata l'efficacia dei sistemi volti a prevenire la ricomparsa di venditori disonesti, già individuati e sospesi per la commercializzazione di prodotti non conformi. Questi sistemi devono garantire una sorveglianza adeguata che prevenga la reintroduzione di merci che non rispettano le normative europee, proteggendo così i consumatori e il mercato europeo da eventuali rischi.

Inoltre, un altro aspetto di grande rilievo riguarda la progettazione del **servizio di Temu che potrebbe indurre dipendenza**, specialmente attraverso l'utilizzo di programmi basati su meccanismi ludici di ricompensa. L'obiettivo dell'indagine è stabilire se Temu abbia implementato **misure effettive per attenuare i rischi associati a tali pratiche**, considerando le possibili ripercussioni negative sul benessere, principalmente psicologico, degli utenti. La normativa europea in materia impone ai fornitori di servizi digitali di considerare attentamente gli impatti psicologici delle loro piattaforme e di intraprendere azioni concrete per proteggere i loro diritti.

Un'ulteriore area di interesse è il rispetto delle obbligazioni previste dalla normativa sui **servizi digitali riguardanti i sistemi di raccomandazione** usati da Temu per suggerire contenuti e prodotti agli utenti. La normativa europea impone che Temu debba divulgare in maniera trasparente i principali parametri che governano tali sistemi di raccomandazione. Inoltre, vi è l'obbligo di fornire almeno un'opzione di raccomandazione che non si basi sulla profilazione degli utenti, rendendo queste opzioni facilmente accessibili a tutti gli utilizzatori della piattaforma. Tale pratica rientrerebbe nell'ambito della profilazione degli utenti, che consiste nell'analisi automatizzata di dati personali per valutare aspetti personali, come le preferenze o gli interessi, al fine di prevedere il comportamento futuro.

In Italia, la profilazione è regolamentata dal Regolamento UE 2016/679 o GDPR, e dal Codice in materia di protezione dei dati personali (D.lgs. 196/2003, come modificato dal D.lgs. 101/2018), che stabiliscono i requisiti per il trattamento lecito dei dati personali e per la tutela dei diritti degli interessati. Piu specificatamente, nell'ordinamento giuridico italiano sarebbero anche applicabili le Linee guida dell'Autorità Garante per la Protezione dei Dati Personali in materia di trattamento di dati personali per profilazione on line del 19 marzo 2015. L'Autorità Garante ricordava, in tale sede, che "le operazioni di trattamento tese alla profilazione dell'utente realizzate anche attraverso l'incrocio di dati raccolti in relazione a funzionalità diverse, non rientrando in alcuno dei casi di esonero dall'obbligo di acquisizione del consenso di cui all´art. 24 del Codice, possono essere effettuate soltanto previa espressa manifestazione di volontà dell'utente stesso".

Sicurezza e diritti dei consumatori. Ma non solo!

Dal punto di vista della protezione dei dati personali ed in virtù al Regolamento (UE) 2016/679 abbiamo

svolto un'analisi dettagliata dei termini e condizioni di Temu, oltre alla privacy policy e cookie policy della piattaforma che riporta come data di entrata in vigore il "29 aprile 2024". Dall'analisi emerge che, attualmente, la cookie policy non offre agli utenti la possibilità di rifiutare, materialmente, dal banner introduttivo oppure dalle "Impostazioni" dell'App, la scelta di profilazione potenziale effettuata da Whaleco Technology Limited. Il testo della privacy policy riporta una clausola ***rebus sic stantibus*** che sembrerebbe racchiudere l'esigenza di dover informare ulteriormente l'utente e permettergli di scegliere:

"Utilizzeremo altri dati da te forniti come descritto nella presente Informativa sulla privacy o per qualsiasi altro scopo da te conosciuto al momento della raccolta delle informazioni."

In conclusione, l'indagine avviata dalla Commissione ha l'obiettivo di assicurare che Temu rispetti pienamente le direttive europee, tutelando i diritti dei consumatori e la sicurezza del mercato digitale unico europeo. Si rileva, inoltre, la **necessità di procedere a un'attenta verifica dell'adeguamento di Temu alle disposizioni vigenti in materia di protezione dei dati personali applicabili nel contesto europeo**. Questa verifica è essenziale per garantire un livello di sicurezza più elevato agli utenti, nel rispetto dei principi sanciti dalla normativa europea, con particolare riferimento al GDPR, al fine di preservare la riservatezza e l'integrità delle informazioni personali trattate dall'APP.

Leggi l'articolo online su www.himmeladvisors.it **Link esterno**

5 Segnalazioni Whistleblowing: modalità e avviso di ricevimento alla luce dello schema di Linee guida ANAC

Sintesi

Nel contesto dell'attuazione delle disposizioni normative sul whistleblowing, recentemente l'Autorità Nazionale Anticorruzione (ANAC) ha proposto di aggiornare le proprie linee guida, ponendo l'accento sull'importanza di garantire modalità diversificate e adeguate per la segnalazione di illeciti, in conformità al D.Lgs. n. 24 del 2023. Tali indicazioni si dimostrano di fondamentale rilevanza per le organizzazioni, siano esse pubbliche o private, che sono tenute a implementare adeguate misure per la raccolta e la gestione delle segnalazioni.

In un altro articolo abbiamo discusso del fenomeno del Whistleblowing, focalizzandoci sulla necessità di implementare una scrupolosa valutazione dei canali di segnalazione adottati in conformità con le disposizioni della Direttiva NIS2 e in previsione dell'imminente recepimento della normativa attraverso il Decreto Legislativo n. 138 del 2024.

In questo articolo, invece, vorremmo parlarvi dello "Schema di Linee guida in materia di Whistleblowing sui canali interni di segnalazione", pubblicato dall'Autorità Nazionale Anticorruzione lo scorso 7 novembre 2024. In pratica, a completamento e ad integrazione delle indicazioni già fornite dall'ANAC con la delibera del 12 luglio 2023 n. 311, l'Autorità ha adottato lo schema di nuove Linee Guida volte a fornire indicazioni sulle modalità di gestione dei canali interni di segnalazione. L'obiettivo è garantire un'applicazione uniforme ed efficace della normativa sul Whistleblowing e indirizzare ulteriormente i soggetti tenuti a dare attuazione alla stessa.

Ricordiamo ai nostri lettori che tali Linee Guida non sono ancora cogenti in quanto sono in fase di consultazione pubblica fino al 9 dicembre 2024. Se sei un ente pubblico o una società privata puoi partecipare al processo di consultazione mediante la compilazione di un questionario on line scaricabile dalla pagina dell'ANAC: link qui

La dicotomia delle modalità di segnalazione: forma scritta vs orale

Nel contesto dell'attuazione delle disposizioni normative sul whistleblowing, recentemente l'Autorità Nazionale Anticorruzione (ANAC) ha proposto di aggiornare le proprie linee guida, ponendo l'accento sull'importanza di garantire modalità diversificate e adeguate per la segnalazione di illeciti, in conformità al D.Lgs. n. 24 del 2023. Tali indicazioni si dimostrano di fondamentale rilevanza per le organizzazioni, siano esse pubbliche o private, che sono tenute a implementare adeguate misure per la raccolta e la gestione delle segnalazioni.

L'ANAC, nella sua funzione di vigilanza e di prevenzione della corruzione in tutti gli ambiti dell'attività amministrativa, ha ribadito che i soggetti destinatari della normativa devono garantire una pluralità di modalità di comunicazione al segnalante, contemplando sia le forme scritte che quelle orali. In particolare, risulta essenziale che le organizzazioni che si trovano ad attivare canali di segnalazione assicurino la possibilità di inviare segnalazioni in modo riservato e sicuro. L'Autorità ha nuovamente

richiamato l'attenzione sulla necessità di implementare un'apposita piattaforma informatica, da ritenere preferibile per la gestione delle segnalazioni. Questa scelta è giustificata dalla capacità di tali strumenti digitali di garantire livelli superiori di sicurezza informatica e di protezione dei dati personali, sia nella fase di acquisizione delle segnalazioni, sia in quella di gestione.

Passi indietro nel percorso di digitalizzazione globale?

Lo schema di Linee Guida proposto dall'ANAC pone, ancora una volta, un interrogativo cruciale: sebbene si enfatizzi l'utilizzo delle piattaforme digitali, perché insistere sulla necessità di mantenere altre modalità di segnalazione, quali linee telefoniche dedicate o incontri di persona? Questa apparente contraddizione solleva preoccupazioni relative alla coerenza della strategia di digitalizzazione in atto. Il ricorso a linee telefoniche gratuite, gestite da operatori autorizzati, e a sistemi di messaggistica vocale, pur presentando vantaggi in termini di immediatezza, tendono a compromettere la riservatezza del segnalante. La questione solleva quindi una riflessione critica su come tali approcci possano davvero garantire la protezione delle informazioni e la riservatezza dell'identità del segnalante, elementi cardini della normativa sul Whistleblowing.

Consenso: la base giuridica legittimante per registrare una telefonata

Nell'ambito del D. Lgs. 24/2023 uno dei principi fondamentali rimane quello della riservatezza del segnalante. Tuttavia, è legittimo interrogarsi sull'efficacia delle modalità di segnalazione alternative – come le comunicazioni telefoniche e i messaggi vocali – nel garantire effettivamente tale riservatezza. L'articolato approccio dell'ANAC richiede che il consenso del segnalante sia espresso prima della registrazione delle segnalazioni, portando all'emergere di questioni relative alla natura di tale consenso (ex art. 6 GDPR). Ci si potrebbe domandare come plurimi canali di comunicazione possano assicurare un consenso libero, specifico e informato; e se, nel caso di segnalazioni via telefono, l'incaricato alla raccolta delle informazioni sia tenuto a informare il segnalante riguardo alla registrazione prima di dar seguito alla sua segnalazione. Nel caso in cui l'interessato non fornisca un consenso espresso, ci si interroga su quale debba essere il comportamento del designato whistleblowing. È lecito concludere che egli dovrebbe rifiutarsi di raccogliere la segnalazione, operando così in modo da non compromettere un diritto legalmente riconosciuto?

Doppio consenso: registrazione e condivisione della segnalazione

Nel presente contesto, lo schema di linee guida dell'ANAC pare affermare che il consenso dell'interessato costituisce la base giuridica per il trattamento dei dati, specificamente per la registrazione della telefonata tramite cui viene effettuata la segnalazione. È opportuno sottolineare un aspetto di rilevante importanza: il designato whistleblowing non solo è tenuto a richiedere il previo consenso del segnalante per l'eventuale registrazione della stessa; è altresì tenuto a richiedere al segnalante di fornire il proprio consenso in merito alla comunicazione delle informazioni a soggetti diversi da quelli competenti per la ricezione e la gestione della segnalazione.

La normativa vigente chiarisce esplicitamente che l'identità del segnalante e qualsiasi altra informazione che consenta di dedurre, sia direttamente sia indirettamente, la sua identità, non possono essere divulgate senza il consenso espresso del segnalante stesso a terzi non autorizzati a ricevere o a dare seguito alle segnalazioni. Questo imperativo normativo mira a garantire la massima protezione e riservatezza per chi decide di segnalare irregolarità, preservando dettagli personali e sensibili connessi all'identità dell'interessato.

Caso pratico n. 1

Nel contesto di un ente pubblico, consideriamo il caso del Sig. Bianchi, un dipendente che decide di contattare

il canale di whistleblowing per segnalare un presunto comportamento illecito da parte di un altro dipendente. Quando il Sig. Bianchi chiama, il designato whistleblowing (Dott. Verdi), lo informa che la conversazione verrà registrata al fine di garantire una corretta gestione della segnalazione. Prima di procedere, il Dott. Verdi chiede esplicitamente al Sig. Bianchi se acconsente a questa registrazione. Solo dopo aver ricevuto il consenso orale del Sig. Bianchi, il Dott. Verdi avvia la registrazione della chiamata. Successivamente, il Dott. Verdi chiarisce al Sig. Bianchi che le informazioni fornite potrebbero essere condivise con persone diverse da quelle incaricate della gestione della segnalazione, come ad esempio il personale legale o la direzione. Prima di procedere, il Dott. Verdi richiede un ulteriore consenso al Sig. Bianchi, informandolo sui possibili destinatari delle informazioni. Solo dopo aver ricevuto un consenso chiaro e informato, il Dott. Verdi registra questa informazione. Alla fine della chiamata, è importante sottolineare che, ai sensi della normativa vigente, l'identità del Sig. Bianchi e qualsiasi informazione che possa permettere di identificarlo non possono essere divulgate a terzi non autorizzati senza il suo consenso espresso.

Conservazione delle segnalazioni

Le tempistiche di conservazione delle registrazioni richiedono un chiarimento che trascenda la semplice indicazione normativa relativa alla conservazione per cinque anni (art. 14 del D. Lgs. 24/2023). È lecito interrogarsi se esistano tempistiche specifiche per la conservazione delle registrazioni, dato che il principio che guida l'azione del Titolare del trattamento dovrebbe essere la finalità del trattamento medesimo ovvero l'obbligo normativo. È evidente che, qualora il designato whistleblowing effettui la verbalizzazione e/o la protocollazione della segnalazione, l'organizzazione potrebbe decidere di procedere con la cancellazione della registrazione. Ciò si giustificherebbe, in quanto un ulteriore trattamento dei dati registrati potrebbe risultare eccedente e non conforme ai principi di liceità, necessità e proporzionalità previsti dal GDPR.

Caso pratico n. 2

Immaginiamo che un dipendente di un ente pubblico, il Sig. Rossi, decida di segnalare un presunto abuso di potere da parte di un suo superiore attraverso una telefonata al canale di whistleblowing dell'organizzazione, dove la chiamata viene registrata dal designato per il whistleblowing. Durante la chiamata, previo consenso, il Sig. Rossi fornisce dettagli sulla situazione problematica, e il designato annota anche altre informazioni necessarie per la gestione della segnalazione. Il designato per il whistleblowing, dopo aver concluso la conversazione telefonica, procede a verbalizzare la segnalazione, creando un documento ufficiale che riporta i contenuti dell'informativa ricevuta. Questo documento viene quindi formalmente protocollato in conformità con le procedure amministrative dell'ente. Riconoscendo che il contenuto della telefonata è stato adeguatamente trascritto e documentato, l'organizzazione decide di cancellare la registrazione della chiamata. Questo atto si giustifica in quanto il trattamento aggiuntivo dei dati registrati non è più necessario per le finalità per le quali i dati erano stati inizialmente raccolti, ovvero la gestione della segnalazione.

Noreply: la Tua segnalazione è stata presa in carico!

Un tema di particolare rilevanza riguarda l'onere probatorio gravante sull'organizzazione. L'impiego di canali interni digitalizzati semplifica la registrazione delle segnalazioni, poiché consente di generare un codice univoco capace di identificare la segnalazione, nonché la data e l'orario in cui essa è stata effettuata e, se del caso, presa in carico. Tuttavia, la gestione delle segnalazioni comunicate oralmente può dare luogo a interpretazioni ambigue. Si ritiene, pertanto, che la responsabilità della corretta presa in carico delle segnalazioni debba ricadere sull'organizzazione stessa, la quale è tenuta a rendere esplicito il proprio impegno attraverso atti organizzativi interni.

Le linee guida sembrano perpetuare un errore attribuendo la responsabilità esclusivamente al gestore della segnalazione, il quale si limita a prendere in carico e gestire la segnalazione. Questa figura agisce sotto l'autorità dell'organizzazione, in qualità di soggetto autorizzato (ex art. 29 GDPR), oppure per conto della medesima nel caso di soggetti terzi che operano per conto (ex art. 28 GDPR). La responsabilità della presa in carico è, infatti, di natura istituzionale; è l'organizzazione che deve garantire l'accoglimento della segnalazione, formalizzare le modalità della presa in carico nell'atto organizzativo

interno, governare l'intero processo di segnalazione e verificare, assiduamente, che i soggetti deputati alla gestione delle segnalazioni abbiano dato seguito alla presa in carico e gestito le segnalazioni pervenute tramite i canali interni istituiti.

In questo senso, la garanzia di riservatezza nella verbalizzazione degli incontri è un punto fondamentale. Le modalità di presa in carico meritano di essere definite - nello schema di Linee Guida - con maggior precisione per evitare ambiguità operative. Ci chiediamo, poi, con quali strumenti dovrà un designato whistleblowing verbalizzare l'incontro tenutosi con il segnalante "di persona": dovrà prendere appunti su un quaderno oppure potrà aprire un file word e salvare tutto sul pc che porta con se? Queste modalità garantiscono, la punto di vista della Data Protection, un completo adeguamento alla normativa applicabile?

In una cornice legislativa in continua evoluzione e, di fronte a tali modalità di raccolta delle segnalazioni, si ravvisa la necessità di stabilire un metodo chiaro e sistematico per la presa in carico delle segnalazioni di illeciti. L'accertamento della responsabilità dell'organizzazione e la garanzia della riservatezza del segnalante non possono prescindere dall'adozione di procedure interne chiare e trasparenti. La normativa impone non solo l'utilizzo di strumenti adeguati, ma anche la creazione di un contesto organizzativo che favorisca un ambiente di fiducia, in cui i segnalanti possano operare senza timore di ritorsioni.

Nelle linee guida dell'ANAC si enunciano obblighi espliciti per le organizzazioni, ma permane una lacuna riguardo alle specifiche modalità operative da attuare per garantire una corretta gestione delle segnalazioni. In particolare, qualora le segnalazioni siano inviate in forma scritta tramite busta chiusa e destinate al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) – soprattutto in situazioni di assenza per ferie o malattia del destinatario – il rischio di un'inefficace gestione della segnalazione è palpabile. L'Autorità ha chiarito che l'avviso di ricevimento deve essere comunicato secondo le modalità espresse dal segnalante; tuttavia, ciò solleva interrogativi sulla prassi da seguire in assenza di indicazioni specifiche da parte del segnalante. La questione dell'invio della comunicazione di presa in carico si rivela di notevole importanza. Resta da chiarire se la forma di comunicazione tramite e-mail possa considerarsi lecita e valida nel rispetto delle disposizioni riguardo la riservatezza e la protezione dei dati in assenza di un recapito specificato nell'atto di segnalazione. Tale omissione potrebbe dare origine a problematiche logistiche e di validità della segnalazione e/o sulle garanzie del processo, esponendo l'organizzazione a possibili contestazioni.

+Consapevolezza +Sensibilità +Formazione

In questo contesto, appare fondamentale che le organizzazioni investano in formazione e consapevolezza sulle tematiche del whistleblowing per garantire che tutti gli attori coinvolti, dal personale agli incaricati della gestione delle segnalazioni, comprendano pienamente le loro responsabilità e i diritti dei segnalanti. L'implementazione di un sistema strutturato e tempestivo di feedback e comunicazione è essenziale per consolidare la fiducia del whistleblower nell'efficacia delle misure di protezione e gestione delle segnalazioni.

Alla luce di quanto esposto, una riflessione approfondita sulle linee guida proposte dall'ANAC risulta necessaria non solo per comprendere le implicazioni pratiche della normativa sul whistleblowing, ma anche per valutare l'impatto delle scelte normative sulle organizzazioni e sulle loro dinamiche interne. La futura attuazione delle stesse richiede un'analisi che vada oltre la mera conformità legislativa, mirando piuttosto a integrare un sistema reale di protezione e incoraggiamento dei segnalanti.

Il futuro delle politiche di whistleblowing in Italia dovrà necessariamente concentrarsi sull'elaborazione di strategie efficaci e sull'adozione di strumenti che garantiscano la sicurezza e la riservatezza dei segnalanti, affiancati da una formazione adeguata e da una comunicazione aperta e trasparente. Una vera cultura del whistleblowing, in grado di promuovere la legalità e la trasparenza, può prosperare solo

in un ambiente che riconosce e valorizza il coraggio di chi sceglie di segnalare irregolarità, tutelandone i diritti e assicurando un trattamento equo e rispettoso delle normative in vigore.

In conclusione, lo schema di linee guida fornite dall'ANAC, sebbene rappresenti un passo significativo verso la protezione dei whistleblower e uno strumento operativo molto valido per i destinatari del D. Lgs. 24/2023, necessitano di un'applicazione dettagliata e di una riflessione approfondita per affinare le modalità attuative e garantire che esse rispondano veramente alle esigenze di riservatezza e sicurezza per chi, compiendo un "atto di coraggio", decide di segnalare situazioni di illeceità all'interno della propria organizzazione. Solo attraverso un investimento concreto e mirato in questi aspetti si potrà realmente promuovere un ambiente favorevole alla trasparenza e alla responsabilità.

Leggi l'articolo online su www.himmeladvisors.it Link esterno

6 Costruire un sistema di conformità unificato per promuovere una crescita sostenibile, insieme al MOGC 231/2001

Sintesi

La sostenibilità aziendale e la trasparenza nella conformità possono essere amplificate dall'integrazione dei fattori ESG con i Modelli 231 presenti in azienda ovvero in fase di implementazione dello stesso. In questo contesto, la Direttiva CSDR impone alle aziende a rendere conto delle loro decisioni riguardanti l'ESG. L'integrazione fra le disposizioni della nuova Direttiva e del MOGC 231 non solo genera valore aggiunto, ma contribuisce anche a ridurre i costi e a migliorare l'efficienza operativa, oltre che a facilitare l'accesso a incentivi fiscali, rafforzando così la solidità e l'affidabilità nei confronti ai propri Clienti.

Tra le ultime misure legislative, spicca la Direttiva 2022/2464/UE, nota come Corporate Sustainability Reporting Directive (CSRD), per la quale il Consiglio dei Ministri ha approvato, il 10 giugno scorso, il decreto legislativo volto alla sua integrazione nell'ordinamento giuridico italiano. Questa Direttiva introduce l'obbligo per le imprese di redigere un Bilancio di sostenibilità, che rappresenta una rendicontazione concreta delle loro decisioni sui fattori sociali, ambientali e di governance.

La direttiva sulla sostenibilità CSRD rivede la direttiva sulla comunicazione di informazioni di carattere non finanziario NFRD del 2014 (Direttiva 2014/95/UE che ha modificato la Direttiva 2013/34/UE) e consentirà di garantire la solidità degli impegni assunti dalle imprese introducendo le seguenti novità:

- *estensione dell'ambito di applicazione a tutte le imprese di grandi dimensioni e alle imprese quotate in un mercato regolamento (ad eccezione delle microimprese quotate in borsa)*
- *obbligo di certificazione delle informazioni comunicate sulla sostenibilità*
- *requisiti più dettagliati e standardizzati sulle informazioni che le imprese devono comunicare*
- *migliore accessibilità delle informazioni, imponendone la pubblicazione in una sezione ad hoc delle relazioni sulla gestione redatte dalle imprese.*

Sostenibilità. Reputazione. Responsabilità

La sostenibilità sta diventando cruciale anche per la reputazione delle aziende nel mercato. In questo contesto, le imprese sono sempre più motivate a favorire investitori che non si limitino a cercare il profitto immediato, ma che diano priorità alla sostenibilità, evidenziando il rispetto dei diritti umani, della parità di genere, la protezione dell'ambiente e una governance trasparente. Tale scelta non è casuale: le aziende che integrano i principi ESG tendono a essere viste come più virtuose e, nel lungo termine, hanno maggiori probabilità di ottenere profitti superiori, grazie alla riduzione dei costi legati alla corporate governance e alla creazione di un ambiente lavorativo più etico e sostenibile.

Per ottenere il successo a 360º, le aziende devono necessariamente **identificare correttamente i rischi e attuare un sistema di controllo interno per la loro gestione**. Questo approccio è comune e presente anche durante la fase di implementazione e gestione del MOGC 231, che comporta innanzitutto l'individuazione dei rischi ai quali l'impresa è esposta e, successivamente, la gestione di tali rischi attraverso l'adozione di misure preventive.

Il D. Lgs. 231/2001 e la Direttiva 2022/2464/UE: MOGC e Sostenibilità

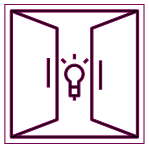
L'innovazione introdotta dal D.Lgs. 231 e la sua significativa diffusione negli ultimi anni, caratterizzata sia da un crescente ruolo nel sistema giuridico sia da un'ampia applicazione pratica, sono argomenti ben noti. Questi aspetti, spesso sottolineati dagli esperti, appartengono ormai a un (sebbene recente) passato.

Esistono numerosi legami tra lo sviluppo sostenibile delle imprese e l'applicazione dei Modelli di organizzazione, gestione e controllo previsti dal D.Lgs. 231/2001, sia nelle aree di interesse che nel sistema di controllo interno. Questo è stato messo in evidenza nel documento intitolato “Modello 231 e fattori ESG: l’importanza di una virtuosa connessione”, elaborato dalla Commissione di studio “Gruppo interdisciplinare ESG – 231” del Consiglio dei Commercialisti e degli Esperti Contabili a cui si fa rinvio.

Ulteriori informazioni qui

In esso viene affermato che il sistema di controllo interno, implementato attraverso il modello organizzativo ex d.lgs. 231/2001, può avere un impatto significativo su attività sensibili anche nel contesto ESG, contribuendo così al raggiungimento di diversi obiettivi di sostenibilità. In questa prospettiva, il **MOGC 231 non solo può fungere da base solida per una governance orientata alla sostenibilità, ma rappresenta anche uno strumento di conformità essenziale per rafforzare le procedure aziendali in chiave ESG che, in ogni caso, sono tenute ad adottare e far rispettare.**

I MOGC 231 possono rivestire un ruolo cruciale nell'integrazione dei fattori ESG all'interno delle aziende, poiché stabiliscono regole comportamentali che coinvolgono tutti gli attori aziendali. Questo approccio trasversale è essenziale per il conseguimento di obiettivi aziendali e di governance a livello nazionale ed europeo. Per garantire un’efficace partecipazione, è fondamentale promuovere la formazione continua, mantenere una comunicazione aperta e coinvolgere attivamente ogni livello dell'organizzazione - dall'organo amministrativo ai dipendenti - rispettando i protocolli stabiliti dai Modelli 231, ai quali si aggiungono le norme comportamentali ESG. Solo attraverso questo processo si potrà favorire lo sviluppo di una cultura aziendale in cui la sostenibilità non è soltanto una "formalità" ma è parte integrante delle decisioni strategiche e delle routine quotidiane.



Considerare le disposizioni di una direttiva come un semplice obbligo o una costrizione non porta benefici all'azienda e non protegge da eventuali sanzioni nel lungo periodo. Al contrario, vederle come strumenti di crescita e opportunità per un miglioramento costante può favorire il successo a lungo termine dell'impresa.

Nel corso degli anni, l'approccio del legislatore nei confronti delle strategie di organizzazione aziendale è diventato sempre più rilevante, come dimostra il riferimento agli adeguati assetti organizzativi nel recente CCII. Grazie alla versatilità dei Modelli organizzativi, questi strumenti non si limitano più a prevenire comportamenti illeciti, ma oggi assumono un ruolo strategico nella gestione complessiva dei rischi aziendali.

L'OdV e la sostenibilità: i controlli dei membri dell'OdV nella prevenzione dei rischi

Alla luce delle analisi finora svolte, ci si può interrogare sul ruolo specifico che i membri degli Organismi di Vigilanza, previsti dal Decreto 231/2001, possono svolgere nel monitorare il rispetto delle normative nazionali ed europee da parte degli operatori nel settore del Wealth Management e del Private Banking. Queste normative, infatti, richiedono alle aziende di impegnarsi attivamente nel raggiungimento degli obiettivi ESG, adottando strategie appropriate in ambito organizzativo, amministrativo e contabile.

Sul punto s.v. "Il ruolo degli O.d.V. nella sorveglianza sulle strategie di sostenibilità" di "M. Bonsegna". Link qui

L'Organismo di Vigilanza avrà un'importanza fondamentale nei prossimi anni, poiché sarà responsabile di controllare regolarmente l'applicazione degli standard operativi e il rispetto delle procedure e dei protocolli implementati per gestire, ridurre o eliminare i rischi, anche alla luce della nuova Direttiva. Come indicato nel documento redatto dal "Gruppo interdisciplinare ESG – 231", **l'Organismo di Vigilanza può diventare il punto di riferimento per i sistemi di compliance integrata, costituendo un pilastro essenziale per il successo sostenibile dell'azienda e il processo di creazione di un valore ampliato**.

Leggi l'articolo completo online su www.himmeladvisors.it Link esterno

7 Pubblicità e trasparenza amministrativa: schemi di pubblicazione che favoriscono enti e amministrazioni nella gestione della sezione “Amministrazione Trasparente"

Sintesi

L'Autorità Nazionale Anticorruzione (ANAC) ha stabilito, mediante la delibera n. 495 del 25 settembre 2024, approvata dal Consiglio, nuove disposizioni. L'Autorità fornisce modelli di pubblicazione per sostenere enti e amministrazioni nella gestione della sezione dedicata all'“Amministrazione Trasparente” sui portali istituzionali, semplificando così le operazioni di pubblicazione e consultazione dei dati da parte dei cittadini e delle cittadine, attraverso modalità standardizzate di organizzazione, codificazione e presentazione.

Il principale obiettivo è quello di facilitare e uniformare la pubblicazione sui siti web istituzionali, dati, documenti e informazioni che devono essere obbligatoriamente pubblicati in conformità agli obblighi di trasparenza e pubblicità previsti dalla normativa applicabile nell'ordinamento italiano.

Il testo della delibera è disponibile qui

L'Autorità ha approvato tre nuovi modelli che riguardano:

- l'impiego delle risorse pubbliche (allegato n. 1);
- la strutturazione delle pubbliche amministrazioni (allegato n. 2);
- e le verifiche in merito all'organizzazione e alle attività amministrative (allegato n. 3).

L’ANAC ha deciso di rendere disponibili sul proprio sito ulteriori dieci modelli (allegati dal n. 5 al n. 14), la cui approvazione finale non è ancora avvenuta, destinati a una fase di sperimentazione annuale su base volontaria per quelle amministrazioni ed enti che desiderano intraprendere un progetto pilota riguardante le modalità di pubblicazione dei vari settori e tipologie di dati previsti.

La deliberazione dell'Autorità tiene conto del dialogo preliminare avviato con Agid, Istat, il Garante per la protezione dei dati personali e la Conferenza unificata, oltre alle proposte emerse dal tavolo tecnico istituito con quest'ultima.

Per quanto concerne i tre modelli approvati, le amministrazioni e gli enti, in considerazione delle esigenze espresse per l'adeguamento dei propri sistemi, disporranno di un periodo transitorio di dodici mesi per aggiornare le relative sezioni nella sezione ‘Amministrazione Trasparente’. I dati dovranno essere pubblicati conformemente ai nuovi modelli adottati dall'ANAC e resi disponibili sul sito dell'Autorità (allegati dal n. 1 al n. 3). Contestualmente ai nuovi schemi, sono state pubblicate delle ‘Istruzioni operative’ (allegato n. 4), che offrono raccomandazioni per l'inserimento dei dati nelle diverse sottosezioni di ‘Amministrazione Trasparente', in accordo con le schede predisposte dall'ANAC.

Gli schemi in oggetto riguardano gli obblighi di pubblicazione relativi a:

atti normativi e amministrativi di natura generale;
- dati sulla valutazione delle performance e sulla distribuzione dei premi al personale;
- provvedimenti adottati dagli organi di indirizzo politico e dai dirigenti amministrativi;
- sovvenzioni, contributi, sussidi e vantaggi economici;
- bilancio, sia preventivo che consuntivo;
- Piano degli indicatori e risultati attesi di bilancio, oltre ai dati sul monitoraggio degli obiettivi;
- servizi forniti;
- procedimenti amministrativi e verifiche sulle dichiarazioni sostitutive e sull'acquisizione d'ufficio dei dati;
- informazioni necessarie per l'esecuzione di pagamenti elettronici;
- attività di pianificazione e gestione del territorio;
- interventi straordinari e di emergenza che prevedono deroghe alla normativa vigente

Ulteriori informazioni: https://www.anticorruzione.it/-/news.19.11.24.trasparenza

Leggi l'articolo completo online su www.himmeladvisors.it Link esterno

sezione Amber

Risorse, opportunità e soluzioni

In questa sezione, abbiamo raccolto una serie di risorse pratiche destinate a supportare le organizzazioni nell'adattamento alle normative vigenti, in seguito alle recenti modifiche apportate dal legislatore, nonché alle buone pratiche per allineare le proprie strutture alle normative nazionali ed europee e alle linee guida pertinenti.

È importante sottolineare che non si tratta di vere e proprie soluzioni definitive, ma piuttosto di strumenti e consigli preziosi che raccomandiamo di considerare e apprendere. Questi materiali sono pensati per offrire spunti utili e orientamenti pratici nelle varie fasi di adeguamento normativo.

Inoltre, ci teniamo a condividere con voi alcune novità e aggiornamenti riguardanti la nostra realtà.

Attraverso questi approfondimenti, desideriamo fornire ai nostri clienti informazioni tempestive e rilevanti, mostrando il nostro impegno costante nel perfezionare i nostri servizi e nel contribuire al successo delle vostre organizzazioni.

HIMMEL ADVISORS
www.himmeladvisors.it

by HIMMEL ADVISORS

NIS2

La sicurezza delle identità rappresenta un metodo completo per salvaguardare le risorse di un'organizzazione, come persone, applicazioni e dispositivi. L'idea centrale è che ogni tipo di utente, sia umano che automatizzato, potrebbe ottenere privilegi in determinate situazioni, potenzialmente compromettendo i sistemi, attraversando le reti e lanciando attacchi. Questo approccio – nel contesto della NIS2 – mira a monitorare e gestire attentamente le identità digitali e la protezione dei dati personali, garantendo che solo gli utenti autorizzati abbiano accesso a informazioni e risorse necessari, attenuando i rischi legati all'accesso non autorizzato e abusivo.

Una strategia completa per la sicurezza delle identità è essenziale per proteggere le infrastrutture critiche da minacce come attacchi informatici, ransomware, vulnerabilità nella catena di fornitura software e altre insidie. Implementare un programma di sicurezza delle identità consente alle organizzazioni di affrontare i requisiti fondamentali previsti dall'articolo 21 della Direttiva NIS2, che includono la gestione e la segnalazione degli incidenti, la sicurezza della catena di fornitura, le tecnologie di crittografia, le politiche di controllo degli accessi e il modello di sicurezza Zero Trust.

www.himmeladvisors.it/nis2

NIS2: check list e adeguamenti per il 2025
La proposta di HIMMEL ADVISORS

Nel mese di gennaio 2023, gli Stati membri dell'Unione Europea hanno formalmente ritenuto opportuno provvedere ad una revisione della già esistente "Direttiva sulla sicurezza delle reti e dei sistemi informatici (Network and Information Systems - NIS)" del 2016.

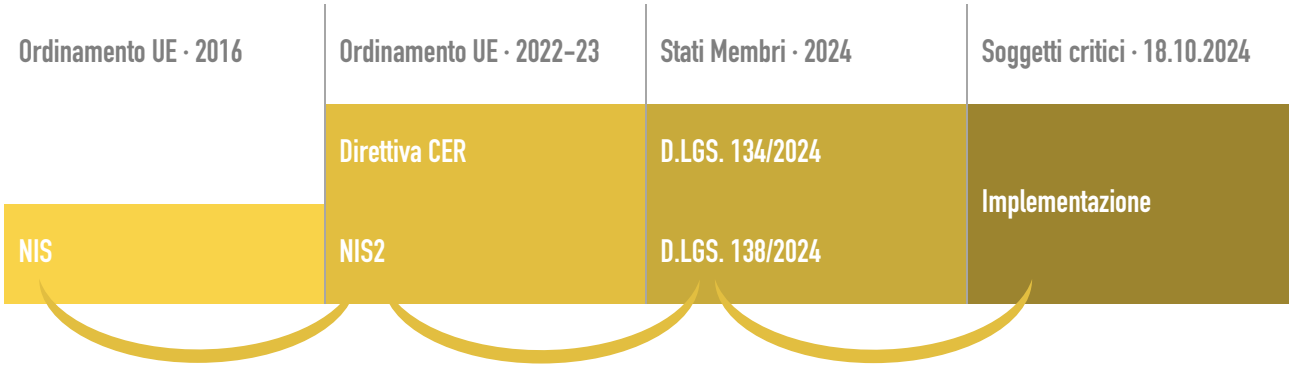
La Direttiva NIS del 2016, conosciuta come Direttiva sulla sicurezza delle reti e dei sistemi informatici, è una normativa dell'Unione Europea adottata per migliorare la sicurezza informatica all'interno degli Stati membri. Essa stabilisce requisiti di sicurezza e obblighi di reportistica per i servizi essenziali e i fornitori di servizi digitali, al fine di garantire un elevato livello di protezione delle reti e dei sistemi informatici.

La revisione alla Direttiva NIS del 2016 è stata avanzata in risposta a una serie di cyber attacchi altamente pubblicizzati e dannosi. In pratica, la Direttiva NIS rappresentava un passo significativo verso un'Europa più sicura dal punto di vista informatico, ponendo le basi per normative più rigorose, culminando poi nella revisione NIS2. L'obiettivo di quest'ultima sarebbe stato quello di rafforzare i requisiti di sicurezza, semplificare gli obblighi di *reporting* e istituire misure di supervisione e requisiti di applicazione più stringenti da parte delle organizzazioni.

La Direttiva NIS2 comporta un ampliamento sostanziale sia della portata sia della profondità della precedente Direttiva NIS. Essa si applica a un ventaglio più ampio di settori industriali rispetto alla sua precursore, introducendo controlli di sicurezza più dettagliati e specifici. Inoltre, la Direttiva NIS2 stabilisce requisiti di reporting in merito agli incidenti informatici che risultano essere significativi e più rigorosi rispetto a quelli precedentemente previsti.

La Direttiva NIS2 potenzia ulteriormente le misure di *enforcement* e le relative sanzioni per garantire il rispetto delle obbligazioni derivanti dalla normativa. È inoltre importante tenere a mente che, a differenza della Direttiva NIS del 2016, i requisiti di cybersecurity della NIS2 si applicano non solo alle organizzazioni che operano all'interno della sua definizione ampliata di "critica" (c.d. soggetti critici) e ai loro dipendenti, ma anche ai subappaltatori e ai fornitori di servizi che le supportano.

La NIS2 impone l'implementazione di controlli di sicurezza rigorosi per tentare di ridurre i rischi e prevenire danni di *cybersecurity* nei sistemi e sui dati. I requisiti comprendono un'ampia gamma di sistemi e risorse IT (a priori regolamentati dalla Direttiva NIS2) inclusa la protezione degli ambienti IT da ransomware, phishing e accesso non autorizzato.

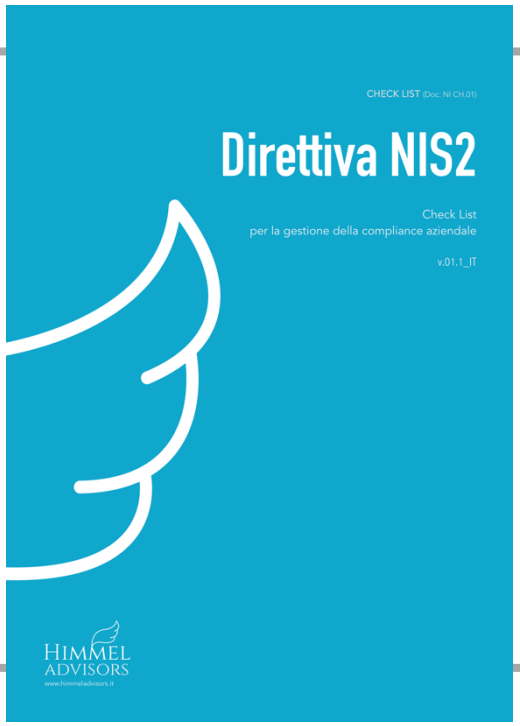


La Check List NIS2 di Himmel Advisors

L'affermazione secondo cui "non esiste un'organizzazione completamente a norma" non è sostenibile, poiché la responsabilità (accountability) delle organizzazioni è un principio che non si conforma a canoni predefiniti o a checklist standardizzate. Essere "a norma" rappresenta un obbligo a cui tutte le organizzazioni devono adempiere, iniziando da una base solida ovvero da un piano d'azione ben definito.

La Check List di Himmel è articolata in quattro distinte sezioni, finalizzate a raggruppare le diverse tipologie di misure in conformità alle prescrizioni della Direttiva NIS2. Questa suddivisione è stata concepita allo scopo di facilitare l'identificazione e l'implementazione sistematica delle misure richieste, fornendo un approccio strutturato alla gestione della sicurezza delle reti e dei sistemi informativi. Ogni sezione del documento si concentra su un macrogruppo specifico di misure, permettendo un'esamina dettagliata e mirata delle aree critiche che richiedono interventi di adeguamento.

Richiedi anche Tu, la Check List. Clicca qui



Legittimo interesse: feedback di HIMMEL ADVISORS al procedimento di consultazione pubblica delle Guidelines 1/2024

L'interesse legittimo è uno dei fondamenti di liceità per il trattamento dei dati personali previsto dal GDPR. Tale base giuridica si applica quando il trattamento dei dati è necessario per perseguire un legittimo interesse del titolare del trattamento o di un terzo, a condizione che su tale interesse non prevalgano i diritti e le libertà fondamentali dell'interessato.

Tuttavia, la definizione e l'ambito di applicazione di tale base legittimante è stato oggetto di vari approfondimenti e interpretazioni giuridiche sia da parte delle autorità di protezione dati dei singoli Stati membri dell'UE, sia da parte dell'EDPB. Queste interpretazioni mirano a chiarire le condizioni e i limiti entro cui l'interesse legittimo può essere invocato, sottolineando la necessità di un attento bilanciamento tra l'interesse legittimo perseguito dal titolare del trattamento o dal terzo e i diritti e le libertà fondamentali dell'interessato/a.

L'EDPB ha pubblicato le Guidelines di cui sopra al fine di poter assistere i titolari del trattamento nell'effettuare tale bilanciamento *case by case* assicurando che i diritti degli interessati/e non siano compromessi. Himmel ha partecipato alla procedura di consultazione pubblica con il proprio contributo che è stato pubblicato sul sito dell'European Data Protection Board lo scorso 27.11.2024

Leggi il nostro contributo (online)	Clicca qui

Parità di genere: i passi della certificazione UNI PdR 125:2022 come strategia d'impresa

La presenza di donne in posizioni dirigenziali e decisionali non solo arricchisce la leadership di diversi punti di vista, ma può anche influenzare positivamente la cultura aziendale, rendendola più inclusiva e orientata al benessere dei dipendenti. Implementare politiche di parità di genere all'interno delle organizzazioni è fondamentale per molteplici ragioni che toccano aspetti etici, sociali ed economici. Promuovere l'uguaglianza di genere si traduce nel garantire a uomini e donne pari opportunità in termini di carriera, formazione e retribuzione, contribuendo a ridurre in modo significativo le disuguaglianze che persistono nel mercato del lavoro.

Quando le politiche di parità di genere sono attuate in modo efficace all'interno di un'organizzazione, si crea un ambiente di lavoro più equo e giusto, dove tutte e tutti, indipendentemente dal loro genere, possono esprimere il proprio potenziale al massimo senza barriere o discriminazioni Inoltre, l'implementazione di tali politiche incoraggia una maggiore diversità all'interno delle organizzazioni, portando a una varietà di prospettive, idee e soluzioni, migliorando la creatività e l'innovazione all'interno dei team di lavoro.

Le squadre diversificate sono infatti in grado di affrontare le sfide aziendali in modo più completo e informato, poiché le diverse esperienze e visioni possono contribuire a decisioni più equilibrate e strategiche

Perché dovrei valutare la Certificazione Parità di Genere?

Implementare politiche di parità di genere significa garantire che uomini e donne abbiano accesso alle **stesse opportunità in termini di assunzione, promozione, formazione e retribuzione**.

La Certificazione serve a combattere le disuguaglianze radicate all'interno della società e per stabilire un clima di lavoro in cui tutti i dipendenti si sentano valorizzati e rispettati. L'uguaglianza di genere nelle organizzazioni non solo riflette un principio etico, ma contribuisce anche a una cultura aziendale più equa e sostenibile.

Contribuiscono a creare un ambiente di lavoro più giusto e inclusivo. Un ambiente in cui le persone si sentono ascoltate e rispettate stimola la fiducia, riduce il turnover e aumenta la soddisfazione generale dei dipendenti

+ Reputazione. Un'ottima reputazione in questo senso può dare all'organizzazione un vantaggio competitivo nell'attrarre i migliori candidati e nel mantenere una forza lavoro di talento.

+ Decontribuzione a favore delle imprese

Le organizzazioni che adottano politiche di parità di genere hanno dimostrato di ottenere risultati finanziari migliori. Diversi studi hanno correlato una maggiore rappresentanza femminile nei ruoli dirigenziali con performance aziendali superiori, indicando che le aziende con una leadership diversificata tendono a prendere decisioni più efficaci e a generare profitti più elevati. Investire nella parità di genere si traduce quindi in vantaggi economici tangibili per l'azienda.

Sul punto www.himmeladvisors.it/parita-genere

Iniziative locali

presso la Camera di Commercio di Bolzano

In data 27.11.2024, presso la Camera di Commercio di Bolzano è stato presentato il Sistema di Certificazione per la parità di genere, un'iniziativa del Piano Nazionale di Ripresa e Resilienza (PNRR) a cui Himmel ha voluto partecipare.

L'iniziativa (nazionale) sulla certificazione parità di genere andrebbe ad ampliare le iniziative già in essere della Camera di Commercio di Bolzano con l'Audit familieundberuf, una certificazione riguardo l'impegno delle aziende a conciliare meglio famiglia, vita privata e lavoro, con un marchio di qualità riconosciuto in tutta Europa.

Ulteriori informazioni qui

HIMMEL ADVISORS entra a far parte dell'Unternehmerverband Südtirol

In data 18 novembre 2024 è stata ratificata l'adesione di Himmel Advisors a Confindustria Alto Adige, "la rappresentanza territoriale di Confindustria, principale associazione di rappresentanza delle imprese manifatturiere e di servizi in Italia che conta oltre 150 mila imprese associate su base volontaria che occupano complessivamente 5,5 milioni di persone".

Con oltre 100 anni di storia, Confindustria ha visto susseguirsi una lunga serie di trasformazioni sociali, politiche ed economiche di cui è diventata protagonista. Ha seguito, anticipato e allo stesso tempo indirizzato le trasformazioni del sistema industriale: dalla produzione a vapore a quella dell'elettricità, dall'automazione industriale all'avvento dei computer, alla digitalizzazione, alla fabbrica intelligente. In parallelo a questi cambiamenti la manifattura italiana si è distinta per una spiccata attenzione al design e alla creatività, dando vita all'Italian Style. Un viaggio lungo oltre un secolo che ha visto l'Italia uscire, con gradualità e tenacia, da una condizione di arretratezza economica fino a divenire un Paese industriale avanzato, 7° al mondo e 2° in Europa. Attraverso un processo guidato dagli imprenditori più dinamici e innovativi, nel 1910 è nata la Confederazione generale dell'industria italiana. Destinata inizialmente alla difesa degli interessi del capitale (in un momento in cui, era nata proprio 4 anni prima la Confederazione generale del lavoro), Confindustria e le sue imprese si sono evolute sempre di più, accompagnando ai mutamenti della società e dell'economia.

Fonte: https://www.confindustria.it/home/chi-siamo/storia

Collaborazioni: HIMMEL ADVISORS sigla un accordo di collaborazione con Def-Con

In foto (da sinistra a destra): Luca Cittadino (Def-Con) e Francisco Garcia (Himmel Advisors S.r.l.)

In data 27 novembre 2024 abbiamo siglato un accordo di partnership con l'azienda bolzanina Def-Con di Cittadino Luca, allo scopo di rafforzare la nostra offerta di servizi nel settore della Data Protection, della Cybersecurity e delle nuove tecnologie.

La nostra decisione di collaborare con realtà imprenditoriali locali nasce dalla volontà di valorizzare *expertise* autentiche e radicate nel territorio, nella convinzione che queste sinergie possano generare valore aggiunto e innovazione. Siamo fermamente convinti che tali partnership contribuiscano non solo alla crescita reciproca, ma anche al mantenimento di un elevato standard di integrità e fiducia nel settore e nel nostro territorio.

Questo accordo sottolinea il nostro impegno nel rafforzare partnership anche con piccoli imprenditori che, nel corso degli anni, hanno dimostrato competenza e dedizione, consolidando la loro reputazione attraverso la trasparenza e la solidità nei rapporti commerciali e professionali.

HIMMEL
ADVISORS
www.himmeladvisors.it

An Idea of
HIMMEL ADVISORS

compliance advent calendar 2024

Carissimi Clienti,
Carissimi Partner,
Carissimi Lettori,

ci avviciniamo a un momento speciale dell'anno, le festività natalizie, un periodo carico di significato e di riflessione. È l'occasione per rallentare, riunirci con i nostri cari e riscoprire **il calore delle piccole cose che rendono la vita davvero unica**.

In questo spirito di gioia e condivisione, desidero porgere a ciascuno di Voi ai Vostri cari famigliari i miei più sinceri auguri per un Natale sereno, ricco di momenti preziosi e affetto. Che queste feste possano portarvi pace, felicità e tanti bei ricordi da custodire nel cuore.

Guardando al futuro, vi auguro **un 2025 colmo di salute, amore e successi**. Possiate affrontare il nuovo anno con rinnovata energia e determinazione, pronti a cogliere ogni opportunità che si presenterà.

Per potervi accompagnare fino al 24 dicembre ci piacerebbe farVi un regalo: il nostro **Compliance Advent Calendar 2024**. Un'idea "creativa" e "formativa". Dal 1° al 24 dicembre, vi invitiamo a esplorare il nostro calendario d'avvento. Ogni giorno, **condivideremo un articolo sulla vigente normativa in materia compliance e le best practices legate al nostro lavoro**.

Buone feste!

Scopri il nostro calendario d'avvento virtuale!

sezione purple

Perspectives

In questa sezione ci proponiamo di ospitare personalità di grande rilievo e influenza nel nostro settore. Questi esperti, ciascuno con una vasta esperienza e una profonda conoscenza delle dinamiche della compliance aziendale, sono invitati e invitate a condividere le loro "prospettive" su temi di particolare interesse e attualità.

L'obiettivo di questa iniziativa è fornire ai nostri lettori un approfondimento significativo su argomenti cruciali, consentendo di trarre insegnamenti preziosi dalle conoscenze e riflessioni di figure di spicco. Attraverso i loro contributi, speriamo di stimolare riflessioni e mettere a disposizione strumenti utili che possano supportare e orientare le organizzazioni nel contesto normativo in continua evoluzione.

HIMMEL ADVISORS
www.himmeladvisors.it

Lazzaroli
Valeria

"Intelligenza Artificiale in azienda: un appuntamento che non può mancare"

Dott.ssa Valeria Lazzaroli. Presidentessa dell'Ente Nazionale di Intelligenza Artificiale (ENIA)

Valeria Lazzaroli è tra le poche persone nel nostro paese che riescono a esprimere la propria passione e dedizione per questa disciplina con autenticità. Quale Presidente dell'Ente Nazionale di Intelligenza Artificiale (ENIA) – l'organizzazione più rappresentativa nel nostro ordinamento nel campo dell'intelligenza artificiale – è riconosciuta per la sua straordinaria competenza e preparazione.

Il suo impegno costante nella promozione dell'innovazione tecnologica contribuisce a comprendere il panorama dell'intelligenza artificiale e ad interpretarlo da un punto di vista diverso. La visione lungimirante di Valeria Lazzaroli e la sua dedizione fanno di lei una figura imprescindibile nel nostro ambito, contribuendo in modo significativo al progresso di tale Istituto.

Informazioni sull'ENIA:
www.enia.ai

"La complessità del nuovo vivere e fare impresa è cosa che impegna trasversalmente tutte le discipline scientifiche e legali. Un momento storico in cui non è consentito fornire risposte ma solo porsi le domande più corrette senza trascurare nulla per consentirsi la più ampia prospettiva"

Lazzaroli

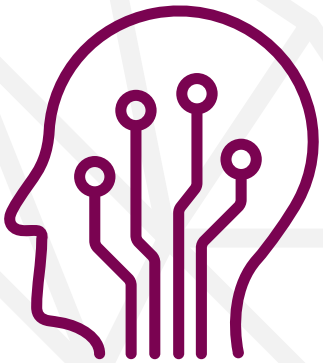
"Intelligenza Artificiale in azienda: un appuntamento che non può mancare"

È un tempo in cui a tutti è chiesto di essere risk manager. Tutto chiede questa nuova funzione come approccio al nuovo divenire. Le grandi normative, la tecnologia, le tecnicalità nelle quali sviluppare processi aziendali.

> La netta percezione che l'AI trovi concretezza, dopo tanti anni dalla sua realizzazione, perché adesso più definito il senso d'essere. Ora che sembra concretizzarsi la società del rischio tanto narrata da Ulrich Beck, l'AI si pone imperiosa e padrona di tutte le informazioni, le nostre debolezze, le carenze, le capacità, i nostri punti di forza.

Ci si dimentica spesso che l'AI nasce per replicare la capacità cognitiva del nostro cervello. Badate bene, di una minima parte. Perché seppur in avvicinamento, il nostro cervello, quello umano, annovera performance straordinarie.

E allora perché "riempirci" di AI?



È storia che parte da lontano. Il Market System nel tempo, con il preciso obiettivo di vendere sempre di più attraverso l'esasperata ricerca di profilazione del proprio utente, ha affinato logiche manageriali e tecnologiche volte al perseguimento. E sicuramente, l'AI un perfetto booster per macinare i 3000 Terabyte al secondo dei nostri telefonini per la definizione dei prodotti più idonei ai nostri bisogni, alle nostre abitudini. Un'occasione imperdibile per evolversi utilizzando ogni presidio digitale per seguirci e restituirci un perfetto, a volte asfissiante, servizio di concierge.

Su questo presupposto di costante innovazione, avremmo dovuto riscontrare una maturità digitale diffusa e più elevata delle nostre imprese. In qualche modo, compatibilmente con le disponibilità e le dimensioni organizzative, queste avrebbero dovuto evolversi tecnologicamente, seppur all'ombra delle BIGTech. Invece no.

E purtroppo il motivo non è da poco. Anzi due.

> Il primo è il dato. Non è stato mai percepito come asset aziendale, cruciale per conoscere meglio la propria azienda. Quindi nessuna postura scientifica per categorizzarlo, per definirlo all'interno dei processi aziendali, per seguirlo, elaborarlo, energizzarlo per averlo costantemente reattivo nel recepire normative, assessment, per assolvere alla compliance.

Lazzaroli

"Intelligenza Artificiale in azienda: un appuntamento che non può mancare"

Un esempio? La GDPR. Un appuntamento mancato per la pluralità delle aziende che avrebbero e l'hanno tutt'ora, la possibilità di definire un proprio sistema informativo. Un impianto che non viva di rimessa ma che sia considerato come primaria leva gestoria. Il primo mezzo per comunicare con gli stakeholders dentro e fuori l'azienda. Già, perché quando normative importanti come il Codice della Crisi d'Impresa chiedono di trovare aziende "forward looking" e "data driven", significa poter contare su aziende con una "data economy", possibilmente allineata per parlarsi con l'intelligenza artificiale ed il machine learning! Disporre, cioè, di quella conoscenza quantitativa che consente di fare analisi predittiva anche di natura qualitativa e quindi prendere decisioni sempre più consapevoli e rispondenti ai criteri di etica e sostenibilità, non sono quella ambientale.

Ed ecco dunque, della **forza dell'AI: terza, oggettiva, indefessa, pragmatica, incorruttibile**.

Puntuale nel ruolo che viene affidato, macina dati per consentire all'imprenditore di conoscere, valutare e predire. Condizione imprescindibile per governare l'azienda in contesti complessi e di difficile codifica. Perché parliamo non di una ma di ben quattro transizioni che ci attraversano e mettono in costante discussione il modo di fare impresa. Parliamo della transizione digitale, di quella energetica, di quella generazionale e di quella di genere. Parliamo anche di un livellamento linguistico speso come una universalità che nei fatti depaupera il patrimonio storico delle aziende. Legate al territorio, alla caratterialità delle generazioni che si sono susseguite, alla materia prima.

> L'AI può riportare un'omeostasi fermando questa forza centrifuga che sembra voler depauperare il passato.

Per farlo, però, l'accuratezza da parte dell'imprenditore di conoscerla, selezionare quella più corretta, quella spiegabile, quella che può valorizzare la privativa intellettuale, che può garantire la riservatezza dei dati, che può definire la postura etica. **Da dove iniziare?** Da conoscere la differenza tra l'AI Narrow e la Generativa. Ma di questo ne parleremo nel prossimo articolo…

Articolo di Valeria Lazzaroli

Le immagini incluse in questa newsletter sono soggette a diritti d'autore e sono utilizzate da HIMMEL ADVISORS secondo le licenze Creative Commons©. In particolare, le immagini o i ritratti presenti nelle sezioni Amber e Purple, che ritraggono persone fisiche nonché altri identificativi, sono state utilizzati previo consenso degli/delle interessati/e. Tale consenso è documentato.

Si precisa che l'utilizzo, totale o parziale, del materiale contenuto nella newsletter è consentito esclusivamente per finalità divulgative e professionali. Qualsiasi impiego per scopi non espressamente regolamentati è vietato. È consentita la condivisione del contenuto 'integrale' della newsletter, mentre è severamente proibita la diffusione di stralci o estratti. Si avverte che qualsiasi uso improprio dei contenuti e delle immagini presenti potrà comportare azioni legali e responsabilità derivanti dall'infrazione dei diritti d'autore."

Ulteriori informazioni
www.himmeladvisors.it/newsletter

Impresa dell'
ALTO ADIGE

sappiamo come aiutarti

aiutaci a capire come possiamo aiutarti
i nostri consulenti sono "sempre" a disposizione*

*Prenota la Tua prima consulenza gratuita

Clicca qui per saperne di più

Ulteriori informazioni sul trattamento dei dati personali per tali finalità sono contenute nell'informativa privacy (ex art. 13 del Regolamento (UE) 2016/679) reperibile sul sito web di HIMMEL ADVISORS a cui si fa rinvio (sezione "privacy policy"): www.himmeladvis

HIMMEL
ADVISORS
www.himmeladvisors.it

Newsletter disponibile online sul sito
www.himmeladvisors.it/newsletter