Newsletter

Nr. 2/2025 Febbraio 2025

Providing
Compliance Solutions
in a complex world

HIMMEL
ADVISORS
www.himmeladvisors.it

www.himmeladvisors.it/newsletter

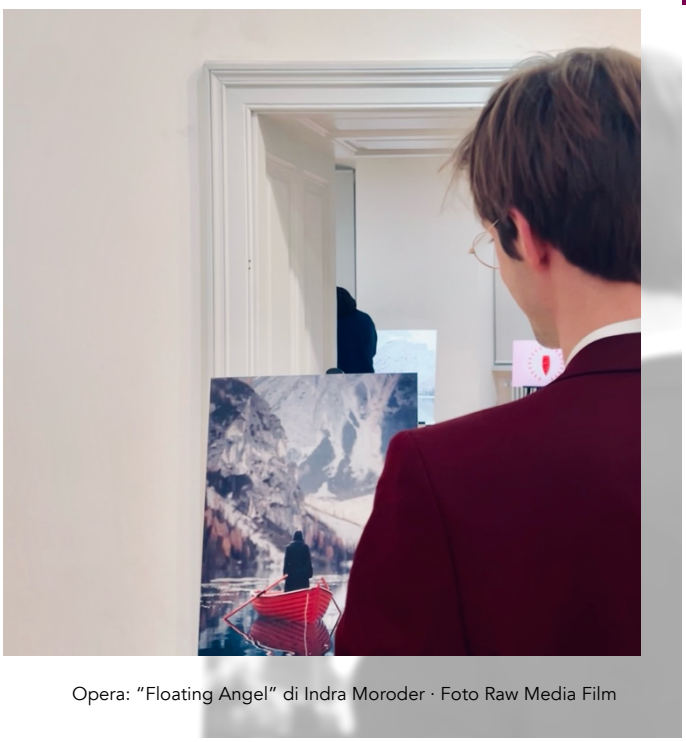
La presente Newsletter è stata elaborata da HIMMEL ADVISORS® e viene resa disponibile gratuitamente sul relativo sito web. Si tratta di un documento informativo che ha lo scopo di fornire aggiornamenti e approfondimenti su temi rilevanti per gli interessati, aiutandolo a rimanere informato sulle ultime 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

Carissimi Lettori,

È con entusiasmo e profonda gratitudine che vi presentiamo il secondo numero della nostra Newsletter bimestrale, 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.

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.

"***Fatta la legge, trovato l'inganno***" potrebbe suonare come l'eco di un adagio senza tempo e tuttavia incarna con ironica precisione la tematica della nostra newsletter bimestrale di febbraio 2025. In un contesto normativo che aspira alla perfezione ma si scontra con l'astuzia umana, abbiamo scelto questo tema per mettere in luce la perenne battaglia per la trasparenza, la correttezza e l'integrità: principi di ampio respiro o "virtù" che, sebbene elevate, dovrebbero essere viste non solo come eterei ideali filosofici ma come endemiche alla struttura normativa contemporanea. Una riflessione che invita a guardare oltre il mero testo della legge, esaminando il fertile terreno dell'inganno che spesso s'intreccia con le pieghe della legalità, sfidando giuristi e appassionati del diritto a ribadire l'importanza dei valori integri in cui le norme si radicano.

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.

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

fatta la legge trovato l'inganno

Cosa c'è di più affascinante del mondo della compliance, dove il rispetto delle norme è spesso un optional e la **trasparenza diventa un concetto malleabile** come una scultura di argilla? Nonostante il crescente impegno delle organizzazioni nella costruzione di modelli organizzativi orientati all'etica, alla trasparenza e all'accountability, si intravede una realtà in cui il proverbio "fatta la legge, trovato l'inganno" sembra prevalere nella cultura dei nostri giorni, evidenziando che le norme stesse possono essere furbescamente eluse.

Immaginate di entrare in un'azienda che ha recentemente aggiornato il proprio Modello organizzativo. I dirigenti ed i propri consulenti si riuniscono in un meeting, accompagnati da slide colorate e buone intenzioni. Molti di loro credono che i nuovi regolamenti rappresentino un'opportunità per rinnovare l'approccio all'etica aziendale e dimostrare l'adeguamento alle vigenti normative. Tuttavia, dietro l'apparente impegno si cela un'idea che assomiglia più a un trucco di magia che a un solido piano di governance. Proprio come in una performance con un cappello a cilindro, dove le illusioni possono prevalere, in questo intricato mondo di normative, decreti e *soft law*, le sorprese possono rivelarsi più ingannevoli di un coniglio che, all'improvviso, diventa un piccione.

"Dimostrare" è la parola più pericolosa che esista. Perché nella compliance nessuno è tenuto a dimostrare. La compliance non va "dimostrata" ma "garantita", perché la privacy, la NIS2, l'IA, l'anticorruzione, la 231/2001 non sono semplici adempimenti ma opportunità per le organizzazioni del domani in cui dovranno lavorare i nostri figli e le nostre figlie.

Mentre **i legislatori si affannano a produrre nuove disposizioni**, il mondo continua a cercare il modo più ingegnoso per aggirarle. Eppure, in questo panorama desolante, di apparenze, esiste un elemento spesso dimenticato: l'opportunità di crescere, di comprendere e di affrontare nuove sfide. È proprio nel processo di adattamento a normative sempre più complesse che risiede il germoglio dell'innovazione. L'intelligenza artificiale, apparente portatrice di semplicità, in realtà non promette sempre la tanto agognata semplificazione. Anzi, la ricerca di quest'ultima – per alcuni – diventa un viaggio tortuoso e ricco di ostacoli.

Nel mezzo di questa **tempesta di cambiamenti**, le aziende, le pubbliche amministrazioni e i loro consulenti emergono come i protagonisti della narrazione. Coloro che rispondono con prontezza, che ascoltano e che si impegnano, sono in grado di portare le aziende verso un futuro più luminoso. Perché la luce non si trova nel semplice seguire le leggi, ma nell'interpretare il loro spirito, nell'abbracciare la crescita come un valore fondamentale. Le organizzazioni hanno il diritto e il dovere di conoscere ogni angolo della propria casa e prendere in mano il proprio destino, liberandosi dall'abitudine di delegare o di conformarsi. Affidarsi a chi ignora la **complessità delle normative** o trascura ciò che non è regolamentato ma è fondamentale per la crescita ed il successo di un'organizzazione non può più essere un'opzione valida per il futuro. Il danno che l'assenza di compliance, persino se voluta, può infliggere alle organizzazioni è simile all'assenza di educazione in una famiglia. Non stupiamoci quindi se nelle piccole, medie e grandi aziende i comportamenti scorretti proliferano come erbacce in un giardino trascurato.

Ecco ciò che si osserva nel mondo di oggi: una **mancanza di disciplina e responsabilità che si riflette nelle prestazioni e nella reputazione** delle organizzazioni stesse. Questo concetto trova ampio riscontro nel libro di Marianna Mazzucato e Rosie Collington, *Il grande imbroglio*. In particolare, quest'opera coraggiosa rompe il silenzio sulle società di consulenza, rivelando come queste possano indebolire le imprese, infantilizzare i governi e distorcere l'economia. Le società di consulenza, talvolta, non sono altro che maghi del cappello a cilindro, capaci di affascinare con le loro promesse di semplificazione e successo, ma che spesso nascondono realtà più complesse e scomode. Mazzucato e Collington sollevano una questione cruciale: come possono le aziende costruire una solida cultura della compliance se si affidano a consulenti che trattano la compliance come una mera formalità o, peggio, un modo per lucrare senza realmente contribuire a una crescita sostenibile? La verità è che in un contesto normativo in continua evoluzione e sempre più intricato, la chiave del successo non risiede solo nell'aderire superficialmente alle normative, ma nel **promuovere una mentalità proattiva e una cultura aziendale che abbraccia la compliance** come un'opportunità di crescita e sviluppo.

Apriamo quindi le nostre menti alle nuove generazioni, preparandole ad affrontare sfide sempre più complesse ma, allo stesso tempo, opportune e contestuali ai nostri tempi. **La compliance non deve essere vista come un fardello, ma come una leva strategica** per migliorare la reputazione aziendale, fidelizzare i clienti, attrarre talenti e "vivere meglio". Dobbiamo avere il coraggio di uscire dalla nostra zona di comfort e abbracciare un futuro in cui la compliance non sia solo una parola d'ordine, ma una prassi vivente e pulsante dentro le nostre organizzazioni.

HIMMEL ADVISORS ***lab***
compliance is the #future of competitiveness

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 Enti locali e obbligo di pubblicazione e consultazione della documentazione relativa agli affidamenti ed alla gestione dei servizi pubblici locali

Sintesi

Il Decreto legislativo 23 dicembre 2022, n. 20 di riordino della disciplina dei servizi pubblici locali di rilevanza economica affida all'Autorità Nazionale Anticorruzione il compito di pubblicare la documentazione degli enti locali relativa ai contratti di affidamento e alla gestione dei servizi pubblici locali di rilevanza economica, trasmessa all'ANAC dai medesimi enti interessati.

Il Decreto legislativo 23 dicembre 2022, n. 201 riveste un'importanza centrale nella regolamentazione dei servizi di interesse economico generale a livello locale. Questo provvedimento si inserisce all'interno di un contesto normativo che deve rispettare il diritto dell'Unione Europea, il quale promuove principi fondamentali come la concorrenza leale, la libertà di stabilimento e la libertà di prestazione dei servizi. L'articolo 117 della Costituzione italiana, nel secondo comma, lettera e), conferisce allo Stato la competenza esclusiva per la regolamentazione della concorrenza. La tutela e promozione della concorrenza diventano quindi essenziali per garantire un mercato equo e aperto, evitando situazioni di monopolio e pratiche anticoncorrenziali.

> ***Art. 1 D.Lgs. 23 dicembre 2022, n. 201***
> *"stabilisce i principi comuni, uniformi ed essenziali, in particolare i principi e le condizioni, anche economiche e finanziarie, per raggiungere e mantenere un alto livello di qualità, sicurezza e accessibilità, la parità di trattamento nell'accesso universale e i diritti dei cittadini e degli utenti"*

Il Decreto legislativo 23 dicembre 2022, n. 201 riveste un'importanza centrale nella regolamentazione dei servizi di interesse economico generale a livello locale. Questo provvedimento si inserisce all'interno di un contesto normativo che deve rispettare il diritto dell'Unione Europea, il quale promuove principi fondamentali come la concorrenza leale, la libertà di stabilimento e la libertà di prestazione dei servizi.

L'art. 117 della Costituzione, nel secondo comma, lettera e), conferisce allo Stato la competenza esclusiva per la regolamentazione della concorrenza. La tutela e promozione della concorrenza diventano quindi essenziali per garantire un mercato equo e aperto, evitando situazioni di monopolio e pratiche anticoncorrenziali.

Il decreto mira a garantire una concorrenza sana nel settore dei servizi pubblici locali, permettendo l'ingresso di nuovi operatori sul mercato e assicurando che i cittadini possano beneficiare di servizi di qualità a prezzi competitivi. Promuovendo la libertà di stabilimento e di prestazione dei servizi, il provvedimento sottolinea l'importanza di consentire agli operatori economici di avviare attività in differenti aree locali e di offrire servizi senza ostacoli. Questo approccio è fondamentale per stimolare la crescita economica e migliorare la qualità dei servizi, che sono essenziali per soddisfare le esigenze della popolazione.

I servizi di interesse economico generale, come quelli relativi all'acqua, all'energia, ai trasporti e alla gestione dei rifiuti, sono al centro dell'attenzione del decreto, che cerca di bilanciare l'interesse pubblico con le necessità di redditività da parte dei gestori. In sintesi, il Decreto legislativo 201/2022 rappresenta un'importante evoluzione verso una gestione efficace dei servizi pubblici locali, promuovendo la concorrenza e garantendo un ambiente favorevole per gli operatori economici, a beneficio dei cittadini e dell'economia locale.

In sintesi, il servizio di trasparenza dei servizi pubblici locali di rilevanza economica dell'ANAC (c.d. STSPL) mira a creare un archivio digitale unico che raccoglie la documentazione relativa alle procedure di assegnazione e gestione dei servizi pubblici locali di importanza economica. L'obiettivo è facilitare la consultazione e la comparazione di tali informazioni, aumentando così la trasparenza.

Ulteriori informazioni sul servizio qui

Principale obiettivo del servizio TSPL

Dal 18 luglio 2023, come previsto nel Comunicato del Presidente del 27 giugno 2023, è cambiato il modo in cui gli enti inviano la documentazione all'Autorità. L'invio tramite PEC è stato sostituito da un'applicazione web riservata ai RUP, che potranno caricare i documenti. Tuttavia, la relazione periodica ex art. 30 c.2 continuerà ad essere inviato via PEC, come descritto in precedenza. Questi documenti saranno pubblicati nella sezione dedicata alla trasparenza dei servizi pubblici locali.

Proposta di ANAC

Per aiutare gli Enti a preparare la documentazione richiesta dal decreto e per semplificare e uniformare i contenuti, nonché orientare le valutazioni necessarie per l'affidamento dei servizi pubblici locali, è stata avviata una collaborazione fruttuosa tra l'ANAC, la Presidenza del Consiglio dei ministri e l'Autorità Garante della Concorrenza e del Mercato. Nell'ambito di questo processo, sono stati sviluppati modelli specifici per alcuni documenti importanti, tra cui la relazione sulla scelta della modalità di gestione del servizio pubblico locale, come indicato dall'articolo 14, comma 3, e la motivazione qualificata prevista dall'articolo 17, comma 2, per gli affidamenti diretti a società in house che superano le soglie di rilevanza europea nei contratti pubblici.

Relazione annuale

Per redigere la relazione annuale (ex art. 30 c.2) è attualmente accessibile, nella sezione dedicata al servizio Trasparenza dei servizi pubblici locali di rilevanza economica sul portale istituzionale di ANAC, un modello che si basa sullo schema contenuto nel Quaderno n. 46 di ANCI. Questo schema è fornito come guida per la pubblicazione.

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

2 Artificial Intelligence: svolgere la Fundamental Rights Impact Assessments (FRIA) secondo il "metodo HUDERIA" proposto dal Committee on Artificial Intelligence (CAI)

Sintesi

La valutazione di impatto che i deployer o titolari devono effettuare nell'ambito dei trattamenti di dati personali per cui si avvalgono di sistemi di AI ad alto rischio (e non solo) riceve il nome di "FRIA" (Fundamental Rights Impact Assessments). Tale strumento, proposto nell'ambito del regolamento AI Act, ha come obiettivo quello di valutare l'impatto dei sistemi di Intelligenza Artificiale sui diritti fondamentali. La valutazione d'impatto relativa all'Intelligenza Artificiale deve concentrarsi non esclusivamente sui dati personali, ma anche, in maniera più ampia, sui diritti fondamentali, comprendendo dignità e integrità umane, libertà individuali, uguaglianza e solidarietà, giustizia, democrazia, lo stato di diritto e la tutela ambientale

Partiamo dalle basi: che cosa è il CAI?

Il Comitato per l'IA (CAI) è il centro delle competenze in materia di IA in tutta l'UE. Svolge un ruolo chiave nell'attuazione del Regolamento (UE) sull'IA, in particolare per l'IA generativa, promuovendo lo sviluppo e l'uso di un'IA affidabile e della cooperazione internazionale. Il CAI è dotato di strumenti unici per sostenere l'approccio dell'UE all'IA. Svolge un ruolo chiave nell'attuazione della legge sull'IA sostenendo gli organi di governance degli Stati membri nei loro compiti. Applica le norme per i modelli di IA generativa. Ciò è sostenuto dai poteri conferiti alla Commissione dal Regolamento (UE) sull'IA, compresa la capacità di effettuare valutazioni dei modelli di IA, richiedere informazioni e misure ai fornitori di modelli e applicare sanzioni.

Il CAI promuove un ecosistema innovativo di IA affidabile per raccogliere i benefici sociali ed economici. Garantisce un approccio strategico, coerente ed efficace all'IA a livello internazionale, diventando un punto di riferimento sia a livello europeo che globale.

> *Per un processo decisionale ben informato, il CAI collabora con gli Stati membri e la più ampia comunità di esperti attraverso forum e gruppi di esperti dedicati. Questi combinano le conoscenze della comunità scientifica, dell'industria, dei gruppi di lavoro, della società civile in generale e delle risorse open source, garantendo che le loro opinioni e competenze siano prese in considerazione. Basato su approfondimenti completi dell'ecosistema dell'IA, compresi i progressi nelle capacità, nella diffusione e in altre tendenze, il CAI promuove una comprensione approfondita dei potenziali benefici e rischi.*

Si parla del "metodo HUDERIA" del CAI

Recentemente, il Consiglio d'Europa ha ufficialmente espresso il proprio sostegno a un nuovo strumento mirato a fornire orientamenti e un approccio strutturato per l'esecuzione delle valutazioni dei rischi e degli impatti associati ai sistemi di Intelligenza Artificiale (IA).

> ***Art. 1 del Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio sull'intelligenza artificiale del 13 giugno 2024***
> *"prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i deployer che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i deployer di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre"*

La valutazione di impatto che i deployer o titolari devono effettuare nell'ambito dei trattamenti di dati personali per cui si avvalgono di sistemi di AI ad alto rischio (e non solo) riceve il nome di "FRIA" (Fundamental Rights Impact Assessment). Tale strumento, proposto nell'ambito del regolamento AI Act, ha come obiettivo quello di valutare l'impatto dei sistemi di Intelligenza Artificiale sui diritti fondamentali.

La valutazione d'impatto relativa all'Intelligenza Artificiale deve concentrarsi non esclusivamente sui dati personali, ma anche, in maniera più ampia, sui diritti fondamentali, comprendendo dignità e integrità umane, libertà individuali, uguaglianza e solidarietà, giustizia, democrazia, lo stato di diritto e la tutela ambientale.

In riferimento alla FRIA, è imprescindibile che tale valutazione venga effettuata in una fase preventiva, antecedente l'introduzione sul mercato o l'utilizzo in contesti critici di un sistema di Intelligenza Artificiale, quali, a titolo esemplificativo, il riconoscimento facciale, l'analisi predittiva e la ricerca scientifica.

Al fine di coadiuvare i deployer ovvero i titolari interessati ad utilizzare sistemi di AI, il CAI ha pubblicato recentemente nel mese di novembre 2024 il documento intitolato "**Methodology for the Risk and Impact Assessment of Artificial Intelligence Systems from the Point of View of Human Rights, Democracy and the Rule of Law (Huderia Methodology)**".

Il suddetto metodo non si rivela utile soltanto per i titolari o i soggetti responsabili dell'implementazione, bensì anche per i Data Protection Officer, i quali, durante la fase di valutazione, possono essere chiamati a partecipare attivamente al processo valutativo e sono chiamati a esprimere un parere riguardo al trattamento dei dati personali implicato nel sistema di Intelligenza Artificiale in uso

Link qui per scaricare la metodologia

Secondo il CAI, la metodologia HUDERIA è stata specificamente adattata alla protezione e alla promozione dei diritti umani, della democrazia e dello Stato di diritto. Può essere utilizzata da attori sia pubblici che privati per identificare e affrontare i rischi e l'impatto sui diritti umani, sulla democrazia e sullo Stato di diritto nell'intero ciclo di vita dei sistemi di IA.

In ogni circostanza, il metodo proposto dal Comitato per l'Intelligenza Artificiale (CAI) dovrebbe essere valutato dal Chief AI Officer, dal Data Protection Officer o dal Privacy Officer prima della sua adozione, in quanto potrebbe risultare applicabile parzialmente.

Inoltre, i soggetti coinvolti nella FRIA hanno pertanto il dovere non solo di considerare i passaggi previsti dalla metodologia del CAI, ma anche di intervenire nella valutazione di ulteriori normative applicabili, comprese quelle di dettaglio (sia in ambito privacy che in altri ambiti), per comprendere in maniera esaustiva i potenziali rischi connessi all'impiego di un sistema di Intelligenza Artificiale (ad alto rischio).

La metodologia HUDERIA non fornisce un risultato definitivo, ma si presenta come una guida destinata ad orientare i responsabili dell'implementazione, approvazione e gestione di un sistema di AI prima dell'utilizzo.

I punti salienti della metodologia Huderia

Probabilmente la parte più interessante della metodologia Huderia è quella relativa al "Stakeholder Engagement Process (SEP)". Secondo il CAI, "la possibilità di eseguire questa fase può essere presa in considerazione per migliorare la qualità delle informazioni da raccogliere", quale elemento successivo fondamentale per la conduzione di una valutazione di impatto

Tale processo permetterebbe di incorporare i punti di vista dei soggetti potenzialmente interessati e di stakeholders, compresi quelli in situazioni vulnerabili. Il coinvolgimento delle parti interessate, come indicato nella Metodologia HUDERIA, può assumere varie forme. Il livello di partecipazione delle persone colpite deve essere informato dai fattori di rischio e dagli impatti potenziali ed effettivi identificati.

Il coinvolgimento delle parti interessate durante l'intero ciclo di vita del sistema di IA può offrire una serie di vantaggi aggiuntivi, come la promozione della trasparenza (particolarmente nel settore pubblico), il mantenimento della fiducia e il miglioramento dell'usabilità e delle prestazioni del sistema di IA, anche in futuro.

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

3 Principio di "non discriminazione" vs Principio di liceità del trattamento dei dati personali alla luce della Sentenza della CGUE (C-394/23)

Sintesi

Nell'era digitale, la raccolta e l'analisi dei dati sono diventate pratiche fondamentali per le aziende che desiderano personalizzare le loro comunicazioni e migliorare l'esperienza del cliente. Tuttavia, la recente sentenza della Corte di Giustizia dell'Unione Europea (CGUE) ha sollevato interrogativi cruciali sulla legittimità di tali pratiche, in particolare riguardo all'utilizzo di alcuni dati come l'appellativo dei clienti.

La recente sentenza della Corte di Giustizia dell'Unione Europea (Causa C-394/23) solleva importanti interrogativi riguardo all'uso degli appellativi di cortesia, come "Sig." e "Sig.ra", nel contesto della formalizzazione dei contratti e dell'erogazione dei servizi. È fondamentale chiarire che il giudice non vieta l'utilizzo di tali appellativi in situazioni specifiche, ma piuttosto ricorda i principi giuridici che, nel diritto UE, le aziende sono tenute a rispettare.

La Corte ha stabilito che la raccolta di tali informazioni non possa considerarsi "oggettivamente indispensabile", specialmente quando il fine è la personalizzazione della comunicazione commerciale. La recente pronuncia della Corte pone sotto la lente un delicato equilibrio tra il legittimo interesse delle aziende a raccogliere tali informazioni e il principio di non discriminazione, sollevando questioni etiche fondamentali su privacy e tutela dei consumatori che riguardano, specificamente, la causa C-394/23.

La CGUE vieta l'utilizzo dell'appellativo sig. / sig.ra?

La recente sentenza della Corte di Giustizia dell'Unione Europea (Causa C-394/23) solleva importanti interrogativi riguardo all'uso degli appellativi di cortesia, come "Sig." e "Sig.ra", nel contesto della formalizzazione dei contratti e dell'erogazione dei servizi. È fondamentale chiarire che il giudice **non vieta l'utilizzo di tali appellativi in situazioni specifiche**, ma piuttosto ricorda i principi giuridici che, nel diritto UE, le aziende sono tenute a rispettare.

Dal punto di vista della protezione dei dati personali, la sentenza mette in luce, a nostro avviso, due tematiche essenziali:

A. **Divieto di inserimento obbligatorio dell'appellativo**

   La Corte chiarisce che né le aziende pubbliche né quelle private possono subordinare la formalizzazione di un contratto o l'accesso ai servizi all'obbligo di inserimento di un appellativo da parte dell'interessato/a. In questo caso, si applica il diritto dei consumatori, che riconosce il principio di libertà e di non discriminazione nell'accesso ai servizi. Sebbene questa sentenza rappresenti un precedente giurisprudenziale, è applicabile al caso specifico; pertanto, è necessario analizzare ogni situazione singolarmente.

B. **Rispetto dei principi di Privacy by Design e by Default**

La Corte sottolinea l'importanza di garantire un trattamento dei dati conforme ai principi di privacy by design e by default. Il titolare del trattamento è tenuto a individuare una base giuridica valida per il trattamento dei dati e delle informazioni che intende raccogliere, gestire e, in ogni caso, trattare. Le due principali basi giuridiche oggetto di controversia sono state il contratto e l'interesse legittimo del Titolare, previste all'articolo 6 del Regolamento (UE) 2016/679.

Da un lato, nell'ambito della qualificazione del contratto come base giuridica, la Corte ha chiarito che non vi è un obbligo di inserire appellativi specifici. Questo implica che le parti possono strutturare il contratto in modo flessibile e accessibile, senza che l'assenza di determinati termini formali di questa natura possa pregiudicare la validità della base contrattuale.

Dall'altro lato, invece, pur considerando l'interesse legittimo come una potenziale base giuridica, la Corte avverte che non può essere conferita legittimità a un trattamento in assenza di un adeguato bilanciamento degli interessi. In questo contesto, è fondamentale che gli interessi dell'interessato prevalgano su quelli del Titolare. Pertanto, la giurisprudenza sottolinea la necessità di una valutazione equilibrata che garantisca la protezione dei diritti fondamentali dell'interessato rispetto alle legittime aspettative del Titolare, affinché il trattamento possa considerarsi conforme ai principi stabiliti dal Regolamento (UE) 2016/679. Tuttavia, per avvalersi di tale base giuridica, la Corte ricorda come il titolare dovrebbe:

Indicare e motivare la base giuridica del trattamento: Prima di procedere con la raccolta dei dati, il Titolare è obbligato a fornire all'interessato un'informativa chiara e dettagliata riguardo alla base giuridica su cui fonda il trattamento. Questa indicazione non riguarda solo l'obbligo di trasparenza dettato dal Regolamento (UE) 2016/679, ma è fondamentale per consentire all'interessato di comprendere gli estremi giuridici alla luce dei quali i suoi dati verranno trattati. La motivazione dell'obbligo di indicare la base giuridica è radicata nella necessità di garantire la protezione dei diritti fondamentali degli interessati e nel rispetto dei principi di responsabilizzazione e trasparenza propri del Regolamento. Inoltre, il Titolare deve chiarire la finalità del trattamento, poiché questa informazione è indispensabile per un adeguato bilanciamento degli interessi tra il Titolare e l'interessato.

La trasparenza sui fini del trattamento consente agli interessati di valutare se il trattamento dei loro dati sia giustificato o meno e rafforza il principio di autodeterminazione informativa.

Minimizzazione del trattamento: Questo principio implica che il Titolare deve adottare misure attive per garantire che la raccolta e l'elaborazione dei dati non superino ciò che è strettamente indispensabile per raggiungere le finalità dichiarate. In tal senso, è essenziale che il Titolare effettui una valutazione preliminare riguardo alla tipologia e alla quantità di dati da raccogliere, assicurandosi di non acquisire informazioni superflue che non siano direttamente correlate alla finalità del trattamento.

La minimizzazione del trattamento contribuisce non solo a tutelare i diritti e le libertà degli interessati, ma anche a limitare i rischi associati a potenziali violazioni dei dati.

Spesso le aziende tralasciano l'importanza di questo principio che, non è soltanto una "garanzia" per gli interessati e le interessate ma anche per i Titolari stessi.

La responsabilità di attuare questo principio ricade sul Titolare, il quale deve dimostrare una chiara giustificazione per ogni dato raccolto e trattato. Inoltre, è opportuno che vengano implementate pratiche di revisione periodica per valutare se l'ammontare dei dati trattati rimanga congruo rispetto agli scopi perseguiti. La minimizzazione del trattamento non solo favorisce la conformità alle normative vigenti, ma rafforza anche la fiducia degli interessati, dimostrando un impegno autentico da parte del Titolare a rispettare e proteggere la protezione dei dati personali.

Rispetto del principio di non discriminazione: Il rispetto del principio di non discriminazione è fondamentale per garantire la piena tutela dei diritti e delle libertà degli interessati, in particolare per quanto concerne l'identità di genere. Questo principio afferma che ogni individuo ha diritto a essere trattato con rispetto e dignità, indipendentemente da caratteristiche personali o sociali. La recente sentenza in questione ha un impatto significativo sia sulla protezione dei dati personali sia sull'equità nella gestione delle relazioni con i clienti. Stabilendo un chiaro divieto di discriminazione, essa ribadisce l'importanza di adottare pratiche aziendali inclusive e paritarie (anche nei confronti dei propri Clienti e Fornitori) che non solo rispettino le diversità individuali, ma che promuovano attivamente l'integrazione e il riconoscimento di tutte le identità. L'applicazione coerente di questo principio richiede un impegno costante da parte delle organizzazioni nel rivedere e aggiornare le proprie politiche e procedure.

In conclusione, sebbene la CGUE non vieti in modo assoluto l'uso di appellativi, stabilisce chiaramente che la loro raccolta deve rispettare rigorosi parametri giuridici volti a tutelare i diritti dei consumatori e la loro dignità, segnando un passo avanti significativo nella protezione dei dati personali.

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

4 Il rischio della (re)identificazione dell'interessato/a: gli orientamenti dell'EDPB

Sintesi

La distinzione tra dati anonimi e dati pseudonimizzati rappresenta un tema di rilevante importanza nel contesto della normativa sulla protezione dei dati personali, in particolare alla luce del Regolamento (UE) 2016/679 e, dallo scorso 17 gennaio 2025, dalle Guidelines dell'EDPB 01/2025 (attualmente in fase di consultazione).

Pseudonimizzazione e anonimizzazione non sono sinonimi.

La distinzione tra dati anonimi e dati pseudonimizzati rappresenta un tema di rilevante importanza nel contesto della normativa sulla protezione dei dati personali, in particolare alla luce del Regolamento (UE) 2016/679 e, dallo scorso 17 gennaio 2025, dalle Guidelines dell'EDPB 01/2025 (attualmente in fase di consultazione).

Comprendere queste due categorie di dati o informazioni è fondamentale per garantire una gestione appropriata e conforme ai principi di protezione previsti dalla normativa europea e nazionale, specialmente gli orientamenti delle autorità nazionali competenti.

> *I dati anonimi si riferiscono a informazioni che non consentono in alcun modo l'identificazione di un soggetto specifico. Secondo il considerando 26 del GDPR, si stabilisce chiaramente che i dati anonimi non devono essere considerati dati personali, poiché "i dati anonimi non riguardano una persona identificabile e non possono, da soli o in combinazione con altre informazioni, permettere l'identificazione di un soggetto". Pertanto, qualsiasi trattamento che riguardi dati completamente anonimi non è soggetto alle disposizioni del GDPR, consentendo un uso più flessibile di tali informazioni, sempre nel rispetto delle garanzie di riservatezza e integrità. D'altra parte, i dati pseudonimizzati sono dati personali che sono stati elaborati in modo tale da ridurre il rischio di identificazione di un soggetto, ma senza evitare completamente tale possibilità.*

La pseudonimizzazione, come definita dall'articolo 4 del GDPR, è una tecnica di trattamento che prevede "l'eliminazione di alcuni elementi che potrebbero consentire di identificare l'interessato e che richiedono comunque ulteriori informazioni per permettere la re-identificazione".

Nonostante la pseudonimizzazione rappresenti una misura di sicurezza utile per tutelare i diritti e le libertà degli interessati, i dati pseudonimizzati continuano ad essere dati personali e, pertanto, sono soggetti a tutte le normative e gli obblighi previsti dal GDPR.

In questo contesto, è essenziale mettere in evidenza che la pseudonimizzazione non esonera il titolare del trattamento dai doveri di conformità. Infatti, i dati pseudonimizzati devono essere trattati nel rispetto dei principi fondamentali di protezione dei dati, come la minimizzazione, l'accuratezza e la limitazione della conservazione, oltre a garantire misure di sicurezza adeguate per prevenire o ridurre il rischio di accesso non autorizzato o di violazioni di dati.

Mentre i dati anonimi offrono una maggiore libertà d'uso, escludendo la necessità di attenersi alle rigide normative del GDPR, i dati pseudonimizzati, pur garantendo un livello di protezione, richiedono una gestione attenta e conforme alla vigente normativa sulla protezione dei dati personali. Adottare una

corretta interpretazione di queste categorie consente, da un lato, di promuovere l'innovazione e l'uso responsabile dei dati, dall'altro, di proteggere i diritti e le libertà fondamentali degli individui.

La conferma dell'EDPB riguardo l'obbligo di tutelare i dati pseudonimizzati

Nelle recentissime linee guida, l'EDPB chiarisce la definizione e l'applicabilità della pseudonimizzazione e dei dati pseudonimizzati, nonché i vantaggi della pseudonimizzazione. Nello specifico, le linee guida forniscono due importanti chiarimenti:

1. **Il dato pseudonimizzato è un dato personale.** I dati pseudonimizzati, i quali possono essere ricondotti a un soggetto identificabile mediante il ricorso a informazioni supplementari, continuano a qualificarsi come dati personali, poiché si riferiscono a una persona fisica identificabile. Infatti, nel caso in cui le informazioni possano essere ricollegate a un individuo, anche in via indiretta, esse conservano la loro natura di dati personali, come stabilito dal GDPR;

2. **la pseudonimizzazione potrebbe essere una misura di sicurezza tecnica e una strategia vincente per mitigare i rischi associati al trattamento dei dati personali.** Tale tecnica può agevolare l'impiego dell'interesse legittimo come base giuridica, ai sensi dell'articolo 6, paragrafo 1, lettera f), del GDPR, a condizione che siano adempiuti tutti gli altri requisiti stabiliti dalla normativa. Analogamente, la pseudonimizzazione contribuisce a garantire la compatibilità con lo scopo originale del trattamento, conformemente a quanto previsto dall'articolo 6, paragrafo 4, del suddetto Regolamento.

L'interesse legittimo quale base giuridica applicabile alla pseudonimizzazione

Come sopra accennato, la pseudonimizzazione è senz'altro una tecnica volta a rendere parzialmente anonimo un dato personale o un insieme di dati personali e, di conseguenza, una misura di sicurezza per il trattamento che si intende effettuare. Tuttavia, non dobbiamo dimenticare che, l'applicazione di tale tecnica comporta, anche un trattamento di dati ai sensi dell'art. 4 del GDPR:

> *un trattamento di dati personale è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.*

Alla luce di tale definizione, ogni trattamento è preceduto da una base legittimante (ex art. 6 GDPR) che autorizzi l'attività di trattamento che si intende effettuare. Le Guidelines dell'EDPB fanno riferimento all'interesse legittimo. Tuttavia, dobbiamo ricordare che, per poter avvalersi di tale base giuridica - in virtù del principio di privacy by design e by default - è necessario che il Titolare effettui, prima una Legitimate Impact Assessment (L.I.A.) al fine di verificare i presupposti e la legittimità di tale trattamento.

Consiglio

Il titolare del trattamento è tenuto ad andare oltre la semplice attività di pseudonimizzazione, considerandola come un "mezzo" finalizzato al conseguimento di specifici obiettivi, piuttosto che come un semplice esito dell'attività di trattamento che si intende effettuare. La pseudonimizzazione, infatti, non può surrogare l'applicazione di idonee misure di sicurezza, sia tecniche che organizzative, necessarie per garantire la protezione dei dati personali.

Il protagonista delle Guidelines: il rischio

Le recenti linee guida emanate dall'EDPB chiariscono che i rischi associati al trattamento dei dati sono diversificati e molteplici, tra cui figura il rischio di re-identificazione dell'interessato riguardo ai dati sottoposti a pseudonimizzazione. Il GDPR, al considerando n. 75 stabilisce che "i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare la [...] decifratura non autorizzata della pseudonimizzazione".

La pseudonimizzazione quale strumento o mezzo per lo svolgimento dell'attività statistica nel settore pubblico o nel settore sanitario risulta alquanto rilevante, una tematica non ancora affrontata nello specifico dall'EDPB (le linee guida si limitano a fornire un esempio - s.v. Example 6: Reduction of confidentiality risks).

Attualmente, si osserva un incremento significativo nella richiesta di scambio di informazioni sanitarie, anche in maniera pseudonimizzata, tra vari soggetti, inclusi i pazienti, i professionisti della salute, i ricercatori e le strutture coinvolte nei percorsi di cura sia a livello provinciale che regionale e nazionale. È opportuno sottolineare che, nei vari ordinamenti giuridici nazionali, le autorità competenti, nell'esercizio delle proprie funzioni regolatorie, possono subordinare l'effettuazione di specifici trattamenti che implicano la raccolta e la gestione di dati personali sensibili a una base giuridica precisa. Ciò può consistere, ad esempio, nell'esistenza di un Decreto Ministeriale specifico o di un'altra norma di legge nazionale che legittimi il titolare a procedere con il trattamento dei dati. La pseudonimizzazione non può essere intesa come lo strumento o il mezzo idoneo a legittimare l'attività di trattamento dei dati personali. Essa deve essere considerata come una misura di sicurezza complementare, ma non sufficiente a garantire la conformità alle disposizioni normative vigenti in materia di protezione dei dati.

Tale evoluzione nelle comunicazioni e nella condivisione dei dati impone l'adozione di misure di sicurezza adeguate, in linea con i progressi tecnologici. In questo contesto, la pseudonimizzazione dei dati sanitari si configura, a priori, come una strategia efficace per salvaguardare la riservatezza dei pazienti, mediante la sostituzione degli elementi identificativi con appositi pseudonimi (codici che non identificano, direttamente, i pazienti).

> *Diverse sono le interpretazioni della Corte di Giustizia dell'UE con sentenza del 26 aprile 2023 (causa T-557/20), che ha stabilito come un dato pseudonimizzato trasmesso ad un destinatario che non ha i mezzi per poter identificare l'interessato non è da considersi un dato personale. In questo caso, la Corte ha chiarito che la valutazione deve avvenire considerando la capacità del destinatario di (re)identificare i soggetti interessati; se quest'ultimo non dispone di informazioni aggiuntive per farlo, i dati trasmessi sono da considerarsi anonimi e quindi non soggetti alla normativa sulla protezione dei dati personali. Di conseguenza, la Corte ha annullato la decisione del Garante europeo della protezione dei dati, che aveva ritenuto i dati pseudonimizzati come dati personali, imponendo al GEPD di sostenere le spese processuali.*

Link qui per scaricare il contenuto delle nuove Guidelines dell'EDPB

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

5 Sanzione da record per E.ON: la Privacy al centro della tempesta

Sintesi

Recentemente, E.ON Energia Spa è stata colpita da una sanzione di oltre 890.000 euro emessa dal Garante per la protezione dei dati personali. Questa decisione sottolinea l'importanza cruciale di rispettare le normative vigenti in materia di privacy, evidenziando le conseguenze legali e reputazionali delle violazioni nei trattamenti di dati personali.

La sanzione deriva da due reclami di utenti che hanno segnalato pratiche di telemarketing indesiderato e il mancato rispetto dei diritti sanciti dal Regolamento Generale sulla Protezione dei Dati (GDPR). Le segnalazioni esponevano come E.ON avesse ignorato richieste legittime di esercizio dei diritti sulla privacy, portando a un'indagine approfondita da parte del Garante.

Uno dei punti critici emersi durante l'istruttoria riguarda la gestione errata dei consensi forniti dai clienti al momento dell'attivazione delle forniture di energia. L'indagine ha rivelato che i consensi erano stati registrati in modo errato, mettendo in luce gravi lacune nei sistemi interni di controllo e verifica di E.ON.

Formazione e supervisione inadeguate e utilizzo improprio dei dati

La mancanza di una formazione e supervisione efficace dei team incaricato dell'attività di telemarketing rappresenta un'altra grave mancanza individuata dal Garante. Questi aspetti sono fondamentali per garantire che le attività di trattamento dei dati siano svolte nel rispetto delle normative, minimizzando il rischio di violazioni.

Nel secondo caso sottoposto all'esame del Garante, è emerso che E.ON ha utilizzato dati raccolti tramite un form su Facebook per campagne digitali, nonostante l'interessata non avesse mai creato un account social. L'azienda non ha effettuato le necessarie verifiche sulla provenienza dei dati, evidenziando ulteriori falle nei controlli.

Quali conseguenze: sanzione e misure correttive

Oltre alla significativa multa di 892.738 euro, il Garante ha ordinato a E.ON di adottare misure adeguate per assicurare la conformità dei processi di trattamento dei dati personali con le normative vigenti. Questo include l'implementazione di controlli più stringenti e la promozione di una cultura aziendale attenta alla privacy.

Questo caso mette in evidenza l'importanza di gestire i dati personali con estrema cura e attenzione. Le aziende moderne devono considerare la privacy non solo come un obbligo legale, ma come un elemento essenziale per costruire la fiducia con i propri clienti. La mancata attenzione a questi aspetti può portare a gravi conseguenze finanziarie e danni alla reputazione aziendale. Il messaggio è chiaro: una gestione dei dati etica e conforme è essenziale per il successo a lungo termine.

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

6 Corrispondenza 2.0: la svolta della Cassazione

Sintesi

Il 14 febbraio non porterà solo con sé le celebrazioni di San Valentino, ma anche una svolta significativa nell'ordinamento giuridico italiano. La Corte di Cassazione, con la sentenza n. 1269, ha affermato che 'le chat contenute nei cellulari sono a tutti gli effetti corrispondenza', stabilendo nuove norme sulla gestione della privacy in ambito digitale.

In questo contesto, si ribadisce anche, che l'accesso al cellulare o alle conversazioni private dei propri partner non è consentito. Tale condotta è considerata una violazione della riservatezza dei dati personali, tutelata dalla normativa vigente. Pertanto, anche se l'interessato dovesse dare il proprio consenso, tale consenso non potrebbe giustificare un accesso indiscriminato a qualsiasi comunicazione del proprio partner senza un provvedimento appropriato che ne consenta esplicitamente la consultazione.

La pronuncia della Cassazione: i punti salienti

La decisione della Corte si inserisce nell'ambito di una precedente pronuncia della Corte Costituzionale, la n. 170 del 7 giugno 2023, che aveva già esteso la protezione della corrispondenza alle forme di comunicazione digitale. Non è però una novità. L'accesso a chat, screenshot e documenti presenti all'interno degli smartphone non è consentito liberamente da altri soggetti terzi nemmeno con il consenso dell'interessato stesso. La privacy diventa, sempre di più, un vero e proprio diritto oggetto di tutela. Per poter utilizzare tali informazioni, è necessario un provvedimento dall'Autorità Giudiziaria competente, analogamente a quanto previsto per le intercettazioni.

> Questo principio sottolinea l'importanza della protezione dei dati personali, che si configura come un diritto fondamentale, che deve essere considerato prioritario rispetto ad altre esigenze, comprese quelle legate a indagini preliminari. Inoltre, con questa sentenza, il cellulare del privato viene classificato come un "contenitore di corrispondenza", portando a una nuova concezione del diritto che garantisce tali comunicazioni sotto l'egida dell'art. 15 della Costituzione italiana.

L'analisi del Caso e i passaggi motivazionali più importanti

La situazione specifica analizzata dalla Corte riguardava un individuo accusato di "spaccio di sostanze stupefacenti", per il quale la prova si basava anche su messaggi tratti da WhatsApp. Tuttavia, tali messaggi si sono rivelati inammissibili in quanto acquisiti in maniera non conforme agli artt. 253 e 254 del codice di procedura penale, considerando la loro natura di corrispondenza. In questo contesto, la Suprema Corte ha dichiarato che "è indispensabile sottolineare come le garanzie a tutela della riservatezza dei dati memorizzati nel telefono cellulare, in seguito alla sentenza della Corte Costituzionale n. 170 del 2023, hanno visto ampliare il proprio raggio d'azione attraverso il riconoscimento della corrispondenza anche per le comunicazioni acquisite dopo la loro ricezione".

Di fatto, tutte le forme di comunicazione, comprese le chat, rientrano nella protezione garantita dalla Costituzione ai sensi dell'art. 15, il quale tutela la libertà e la segretezza della corrispondenza. Si

sottolinea che tale protezione può essere derogata esclusivamente mediante un provvedimento motivato dell'autorità giudiziaria.

L'analisi del Caso e i passaggi motivazionali più importanti

La situazione specifica analizzata dalla Corte riguardava un individuo accusato di “spaccio di sostanze stupefacenti”, per il quale la prova si basava anche su messaggi tratti da WhatsApp. Tuttavia, tali messaggi si sono rivelati inammissibili in quanto acquisiti in maniera non conforme agli artt. 253 e 254 del codice di procedura penale, considerando la loro natura di corrispondenza. In questo contesto, la Suprema Corte ha dichiarato che “è indispensabile sottolineare come le garanzie a tutela della riservatezza dei dati memorizzati nel telefono cellulare, in seguito alla sentenza della Corte Costituzionale n. 170 del 2023, hanno visto ampliare il proprio raggio d’azione attraverso il riconoscimento della corrispondenza anche per le comunicazioni acquisite dopo la loro ricezione”.

Tutte le forme di comunicazione, comprese le chat, rientrano nella protezione garantita dalla Costituzione (art. 15) la quale tutela la libertà e la segretezza della corrispondenza. Si sottolinea che tale protezione può essere derogata esclusivamente mediante un provvedimento motivato dell'autorità giudiziaria.

Il Principio di Diritto

Il principio di diritto stabilito dalla Corte è privo di ambiguità: “Non è valido il consenso dell’indagato – per evitare possibili abusi – a considerare legittima l’acquisizione di chat dallo smartphone in uso al medesimo, essendo necessaria un’autorizzazione preventiva da parte dell’autorità giudiziaria.”

Questo implica che non possono essere effettuati screenshot delle conversazioni, né si possono considerare tali prove come atipiche. In un sistema giuridico che segue il principio di legalità, non si può consentire alla polizia di eludere le disposizioni legislative per adottare misure non standard al fine di ottenere gli stessi risultati delle attività di acquisizione tipiche.

Il Consenso

Un aspetto di rilievo che emerge da questa sentenza è che, anche nel caso di consenso espresso da parte dell’indagato, questo non è considerato sufficiente. La Corte chiarisce che tale consenso potrebbe risultare “viziato” o estorto. È quindi fondamentale che, in situazioni simili, la polizia giudiziaria segua la procedura di sequestro del telefono senza accedere ai contenuti, onde prevenire il rischio di abusi. Il consenso deve sempre essere libero e non può essere indotto da pressioni o intimidazioni.

In conclusione, sebbene il rigetto del ricorso con conseguente condanna dell'indagato rappresenti un cambiamento significativo e di rilevante portata, esso porta con sé implicazioni non trascurabili, in particolare nel contesto delle indagini penali. Questo pronunciamento impone infatti un maggiore rispetto della privacy durante le investigazioni, richiedendo una maggiore cautela e una rigorosa osservanza delle normative a tutela dei diritti fondamentali. La sentenza n. 1269 segna quindi una tappa importante nel cammino verso la protezione della comunicazione privata nell'era digitale, dimostrando come il diritto si stia adattando alle nuove realtà sociali e tecnologiche.

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.

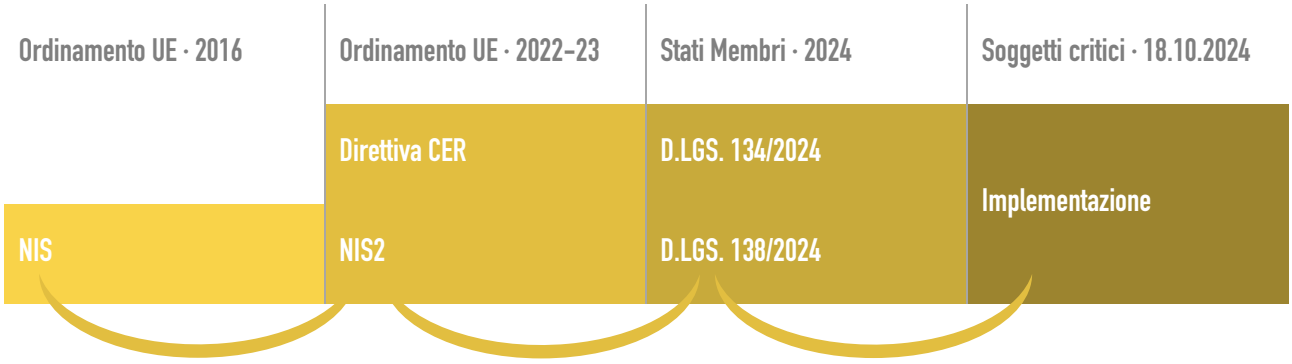
La Direttiva NIS del 2016, conosciuta come Direttiva sulla sicurezza delle reti e dei sistemi informatici, è una normativa dell'Unione Europea adottata per migliorare la sicurezza informatica all'interno degli Stati membri. Essa stabilisce requisiti di sicurezza e obblighi di reportistica per i servizi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

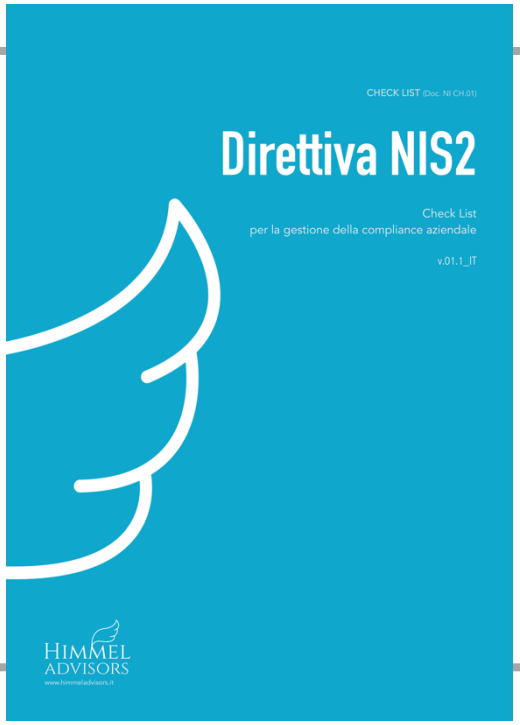


La Check List NIS2 di Himmel Advisors

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



Obbligo di registrazione all'ACN: **entro il 28 febbraio 2025!**

Nasce il *lab* di HIMMEL in materia di "Regulatory Harmonization & Simplification"

È nato in Himmel un innovativo *lab* dedicato allo studio dell'armonizzazione e semplificazione normativa, un progetto avanguardistico che riunisce clienti e stakeholder per condividere esperienze e materiali cruciali nel campo della compliance e dell'intelligenza artificiale.

Navigare l'intricata rete normativa contemporanea può essere una sfida per molte organizzazioni, che spesso faticano a distinguere tra obblighi, doveri e facoltà. Il nostro lab si propone di mitigare questa complessità: fungiamo da intermediari esperti, filtrando e razionalizzando le normative per offrire una maggiore chiarezza e supporto. Dal nostro lab sono già scaturiti strumenti essenziali, come il White Paper in ambito AI e la Check List della NIS2, che si sono rivelati risorse molto utili per i nostri Clienti volte ad affrontare le sfide della conformità normativa. Puoi trovare tutti i nostri documenti nella sezione "Publications" del nostro sito web: www.himmeladvisors.it/publications

Il nostro lab rappresenta una comunità in espansione, composta da accademici ed esperti in varie discipline. Attraverso un approccio collaborativo, integrano le loro conoscenze per sviluppare documenti operativi utili per il corretto funzionamento e il rispetto delle normative.

Se sei uno stakeholder e vuoi unirti a noi in questa iniziativa entusiasmante? La vostra partecipazione è fondamentale per creare un **dialogo costruttivo e arricchente**. Entra a far parte del nostro lab!

Unisciti a noi!	www.himmeladvisors.it/lab

La *piccola* HIMMEL ADVISORS diventa un marchio europeo

In foto la bozza progettuale elaborata da Francisco Garcia durante il processo di creazione del logo

HIMMEL®
ADVISORS
www.himmeladvisors.it

Finalmente possiamo affermare che il marchio "Himmel Advisors" è stato registrato presso l'**EUIPO**, diventando così un marchio UE!

Il nostro marchio non solo rappresenta la nostra azienda in Alto Adige, ma garantisce anche la sua protezione in tutta Europa. Questo riconoscimento non è solo un traguardo per noi, ma dimostra, anche, il nostro impegno verso i valori fondamentali che guidano la nostra mission & vision.

Il nostro logo, che rappresenta un'ala, simboleggia la libertà, un principio che riteniamo essenziale per il progresso e l'innovazione. Le ali ci permettono di elevarci sopra le sfide e di guardare al futuro con speranza e determinazione. In un mondo in continua evoluzione, la trasparenza e l'integrità sono valori imprescindibili. La nostra visione si radica nei principi democratici, i quali devono guidare non solo le nostre azioni, ma anche ispirare le generazioni future e i nostri clienti tramite soluzioni sostenibili nel ambito della compliance.

EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Pitch organizzato da Confindustria Alto Adige presso FC Südtirol: la partecipazione di HIMMEL ADVISORS

Foto realizzata in occasione dell'evento pubblico tenutosi presso FC Südtirol

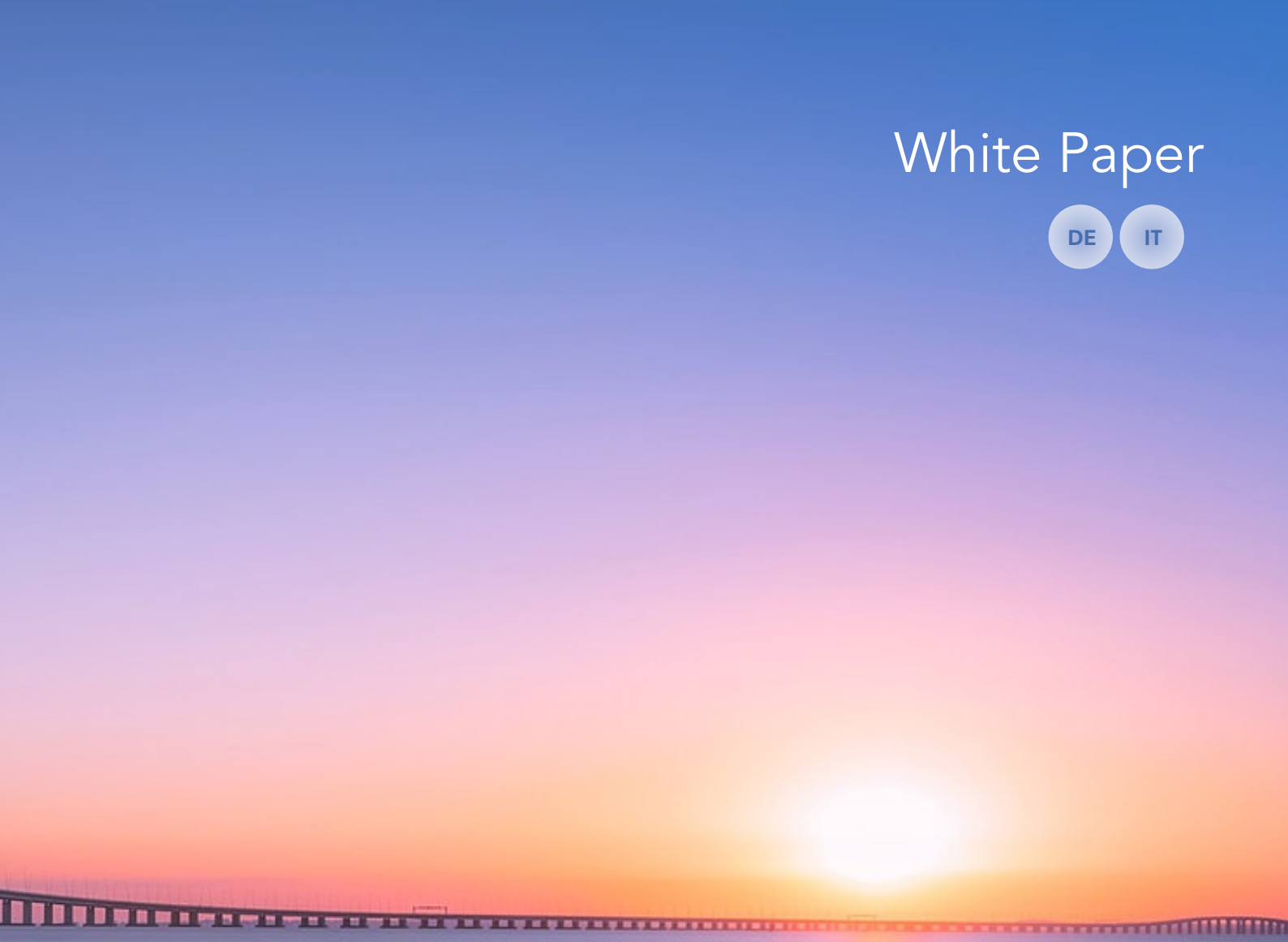
Il Südtirol è qualità. Questo è stato dimostrato dalle 10 aziende partecipanti al Pitch organizzato da Confindustria Alto Adige in collaborazione con FC Südtirol. Un'importante occasione di incontro tra realtà imprenditoriali del nostro territorio. Un territorio che si distingue per l'eccellenza, l'innovazione, lo spirito di collaborazione e il multiculturalismo.

Crediamo fermamente che il dialogo tra aziende locali sia fondamentale per elevare ulteriormente la qualità dei servizi che offriamo. Himmel nasce proprio da questa visione: garantire ai nostri clienti qualità, continuità e professionalità. Valori che riteniamo imprescindibili, così come lo è l'emozione. Nel calcio, l'emozione è il motore di ogni partita: quella che unisce squadra e tifosi, che accende la passione, che rende ogni istante indimenticabile. È proprio questa emozione che ci guida nel nostro progetto. Perché lavoriamo con il cuore, con la determinazione e l'impegno di chi vuole fare la differenza.

HIMMEL
ADVISORS
www.himmeladvisors.it

White Paper

DE IT



AI ACT

Uno sguardo ai nuovi obblighi
per società private ed enti pubblici

v.01.1_IT

Include il contributo di Himmel alla bozza di Linee Guida AGID sull'IA *in fase di consultazione*

Richiedi il nostro **White Paper** direttamente dal nostro sito web:
www.himmeladvisors.it/publications

PA e Linee Guida AGID sull'IA. Il contributo di Himmel Advisors

In foto: sede dell'Agenzia per l'Italia Digitale, a Roma

Anche Himmel Advisors ha voluto contribuire alla procedura di consultazione pubblica della "bozza di linee guida per l'adozione di IA nella pubblica amministrazione" dell'Agenzia per l'Italia Digitale (AGID).

Il nostro contributo intende fornire suggerimenti e miglioramenti alla "Bozza di Linee Guida" dell'AGID. Nello specifico abbiamo affrontato quattro temi: l'interesse legittimo come base giuridica legittimante; la procedimentalizzazione dei processi per accrescere la trasparenza nelle PA; la definizione di chiare regole di governance per un'adozione responsabile dell'IA; e la distinzione tra DPIA e FRIA per un'adeguata valutazione d'impatto. Questo approccio consapevole intende navigare tra normative ed etica per edificare una società più equa e consapevole.

Il testo è a disposizione all'interno della sezione "Publications" del nostro sito web Lingua IT – Doc 1. Public Consultation Ongoing (link qui).

“I tre porcellini” (J. O. Halliwell-Phillipps). Un’interpretazione di HIMMEL ADVISORS

Lo scorso 14 febbraio 2025, Himmel ha pubblicato la versione rivisitata del classico racconto "I Tre Porcellini", ispirato all'opera di James Orchard Halliwell-Phillipps. In questa nuova interpretazione, i tre porcellini non sono solo personaggi di una favola, ma rappresentano tre diverse organizzazioni: una società privata, una pubblica amministrazione e un ente pubblico. Ma chi è il lupo?

Questo racconto vuole rappresentare, in maniera creativa e divertente, l'importanza della preparazione e della pianificazione per affrontare ogni sfida. Sottolinea quanto sia cruciale rispettare le normative applicabili. Le scelte dei porcellini dimostrano che le decisioni hanno un impatto diretto sui risultati, proprio come i principi della compliance aziendale.

Il doc, in pdf, è a disposizione nella sezione “Publications” del nostro sito web
Lingua IT/DE/FR/EN – link qui

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

Zeitfabrik®

ein Unternehmen aus Südtirol

ZEITFABRIK


GWE B8U
Spiegelung
NB-Linda
Diese Daten durchsuchen
Einblicke erhalten
Abonnieren
Warnung festlegen
Bearbeiten
Copilot
AC
PY
ZEITFABRIK
Filter
[AC-PY]%
+19,6%
+16,2%
+203,9%
+7,4%
-75,1%
+201,0%
+21,8%
-21,2%
814 Tsd.
-370 Tsd.
-6 Tsd.
12 Tsd.
-342 Tsd.
-2 Tsd.
0 Tsd.
105 Tsd.
-31,5%
+30,4%
+18,1%
-57,6%
-61,3%
+28,3%
-100,0%
-12,3%
+0,0%
-52,2%
+19,2%
+88,4%
27 Tsd.
109 Tsd.
62 Tsd.
76 Tsd.
144 Tsd.
251 Tsd.
52 Tsd.
187 Tsd.
94 Tsd.
42 Tsd.
79 Tsd.
76 Tsd.
2024-01
2024-02
2024-03
2024-04
2024-05
2024-06
2024-07
2024-08
iiyama

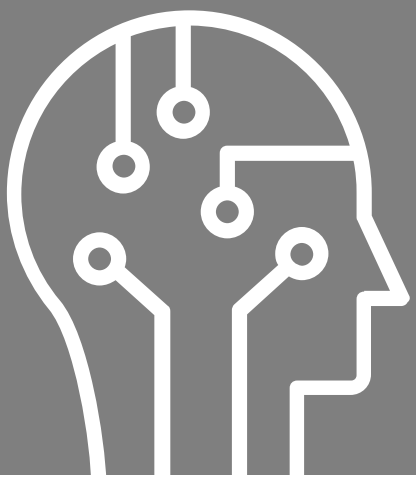
Seite 37-38: Zeitfabrik Team

Mehr Zeit

für das Wesentliche durch Business Intelligence

Datengetriebene Entscheidungen per Mausklick

In der heutigen datengetriebenen Geschäftswelt ist es wichtiger denn je, die richtigen Informationen zur richtigen Zeit zu haben. Doch wie können Unternehmer:innen aus der Flut an Daten wertvolle Erkenntnisse gewinnen? Durch Business Intelligence (BI)! Was genau ist aber Business Intelligence und welchen konkreten Nutzen hat sie für Unternehmer:innen? Lassen Sie uns einen genaueren Blick darauf werfen.

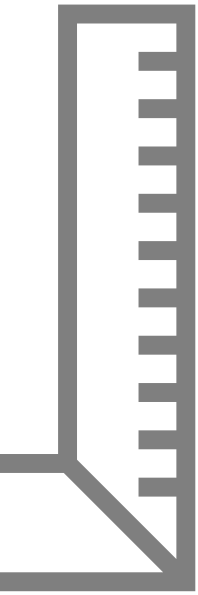


Was ist Business Intelligence?

Business Intelligence (BI) umfasst Prozesse, Technologien und Tools zur Sammlung, Integration und visuellen Darstellung von Daten. Das Ziel von BI ist es, Unternehmen dabei zu unterstützen, datenbasierte Entscheidungen zu treffen. BI-Systeme sammeln Daten weitestgehend automatisiert aus verschiedenen Quellen, verarbeiten diese und stellen sie in verständlichen Berichten, Dashboards und Visualisierungen dar. Diese Informationen helfen Ihnen, Trends zu erkennen, Probleme zu identifizieren und Ihre Ziele zu verfolgen. Menschliches Eingreifen ist in jedem Fall unerlässlich!

Weitere Informationen: https://zeitfabrik.it/services/datenvisualisierung-bi/

Was ist Ihr konkreter Nutzen von B.I.?



1. Bessere Entscheidungsfindung
BI liefert Ihnen präzise und aktuelle Informationen, die Ihnen helfen, fundierte Entscheidungen zu treffen. Anstatt sich auf Bauchgefühl oder unvollständige Daten zu verlassen, können Sie auf aussagekräftige Dashboards zurückgreifen und Entscheidungen auf Basis aktueller und genauer Daten treffen.

2. Erhöhte Effizienz
Durch die Automatisierung der Datenaufbereitung und -visualisierung sparen Sie wertvolle Zeit. Anstatt sich mit der manuellen Erstellung von Geschäftsberichten zu beschäftigen, können Sie und Ihre Mitarbeiter:innen sich auf die Analyse von Abweichungen konzentrieren. Die Goldene Regel von ZEITFABRIK® lautet: Alles, das mehr als einmal ausgewertet wird, sollte automatisiert werden!

3. Schnelle Erkenntnisse:
Interaktive Diagramme und Grafiken vereinfachen die Dateninterpretation und helfen Ihnen, schnell die Ursachen für Abweichungen zu identifizieren. Mit der Drill-Down-Funktion in Microsoft PowerBI können Sie bis auf die Belegebene navigieren und detaillierte Einblicke gewinnen.

4. Automatische Datenaktualisierungen: Automatische Datenaktualisierungen im Datawarehouse und in Power BI gewährleisten, dass Ihre Berichte stets auf dem neuesten Stand sind. Dies eliminiert die Notwendigkeit des manuellen Datenladens und reduziert Fehler. Das spart nicht nur Zeit, sondern auch Nerven. ZEITFABRIK® integriert in jedes Dashboard zusätzlich ein Infofeld zur letzten Aktualisierung, sodass jede:r Nutzer:in sofort den aktuellen Stand der Daten erkennen kann.

5. Wettbewerbsvorteil
BI hilft Ihnen, Trends und Muster in Ihren Daten zu erkennen, die sonst möglicherweise unbemerkt bleiben würden. Durch diese Erkenntnisse können Sie Marktchancen erkennen und Wettbewerbsvorteile erzielen.

Bei ZEITFABRIK® besteht ein Business-Intelligence-Projekt aus vier wesentlichen Komponenten

Datenstrategie: Die Datenstrategie bildet das Fundament einer erfolgreichen Business-Intelligence-Initiative. Hier werden zentrale Fragen geklärt, wie: Welche Daten sind für Ihr Unternehmen relevant? Wie werden diese Daten erfasst? Welche Technologien kommen zum Einsatz? Wo werden die Daten gespeichert? Diese und viele weitere Fragen werden im Rahmen der Entwicklung Ihrer Datenstrategie beantwortet.

Data Warehouse: Nach der Festlegung der Datenstrategie wird das Data Warehouse (DWH) eingerichtet. Es dient als zentraler Speicherort, in dem Daten aus verschiedenen Quellen (ERP, CRM, SharePoint, usw.) gesammelt, verbunden und für Analysen aufbereitet werden. Die sogenannte „Single Source of Truth" (SSOT) ist damit sichergestellt.

Datenvisualisierung: Die im Data Warehouse gespeicherten Daten bilden die Grundlage für die grafische Aufbereitung in einem BI-Tool, wie Microsoft PowerBI. Hier werden die Daten in interaktiven Diagrammen und Tabellen visualisiert. ZEITFABRIK® arbeitet dabei nach den International Business Communication Standards (IBCS®), einer Reihe von Richtlinien für die einheitliche Gestaltung von Geschäftsberichten, Dashboards und Präsentationen. Durch die Anwendung der IBCS® wird sichergestellt, dass aus den Daten schnell die richtigen Informationen gewonnen werden können.

Integrierte Planung: Ein umfassendes BI-Projekt bei ZEITFABRIK® schließt auch die Planung und das Forecasting mit ein. Sie können Ihre Daten direkt in Microsoft PowerBI eingeben. Die Planungsdaten werden direkt im Dashboard angezeigt und in Echtzeit in eine Datenbank im Datawarehouse geschrieben. Die integrierte Planung bildet die Grundlage für die zukünftige Datenstrategie und rundet somit den BI-Prozess bei ZEITFABRIK® ab.

Business Intelligence ist weit mehr als nur ein Trend – sie ist ein unverzichtbares Werkzeug für Ihr Unternehmen

Nutzen Sie Ihre Daten als solide Entscheidungsgrundlage und gewinnen Sie wieder mehr Zeit für das Wesentliche.

ZEITFABRIK

www.zeitfabrik.it

Arena Maurizio

"OdV e Whistleblowing"

Avvocato – Commissione Antiriciclaggio del Consiglio Nazionale Forense (membro esterno)

Maurizio Arena non è un giurista qualunque. Si distingue per la sua ampia conoscenza del diritto penale d'impresa, con particolare riguardo alla responsabilità da reato degli enti (d.lg. 231/2001), alla normativa antiriciclaggio (d.lg. 231/2007) e alla sicurezza sul lavoro.

"*Orientamenti della giurisprudenza penale sull'Organismo di vigilanza ex d.lg. 231/2001*. 2024" – il suo ultimo libro – è un volume che meriterebbe di essere incluso come lettura obbligatoria nei corsi di diritto penale di tutte le università italiane. Con uno sguardo attento alle evoluzioni legislative, Arena ci offre una comprensione approfondita della normativa antiriciclaggio, dimostrando come questa sia cruciale per garantire la legalità e la trasparenza che vivono le organizzazioni pubbliche e private nel contesto normativo odierno.

Informazioni sul CNF:
www.consiglionazionaleforense.it

> il budget dell'OdV deve tener conto […] (anche) dell'attività di esame ed approfondimento delle segnalazioni (come avvenuto sin dall'entrata in vigore del d.lgs. 231), esulando invece dai suoi compiti ogni profilo decisorio successivo (denuncia all'Autorità giudiziaria; ulteriore approfondimento investigativo; attivazione di un procedimento disciplinare) che compete agli organi gestori della società

Arena

"OdV e Whistleblowing"

Sin dall'entrata in vigore del d.lgs. 231/2001 e del sistema dei Modelli organizzativi, si è ritenuto elemento essenziale degli stessi la (regolamentazione della) possibilità di segnalazione di illeciti da parte del personale (c.d. whistleblowing).

> Il fondamento del WB veniva individuato nell'art 6 d.lgs. 231, secondo il quale il Modello deve prevedere «obblighi di informazione» nei confronti dell'Organismo di vigilanza.

Di regola i Modelli prevedevano, quale possibile oggetto della segnalazione, la commissione o tentata commissione di reati-presupposto e la violazione del Modello (ivi comprese le procedure richiamate dallo stesso e il Codice etico). L'OdV riceveva le segnalazioni tramite e-mail dedicata oppure tramite posta ordinaria e procedeva ad esaminarle ed approfondirle se ritenute pertinenti e rilevanti: all'esito, doveva riferirne all'organo amministrativo per le decisioni del caso.

In definitiva, pur in mancanza di una normativa ad hoc, la prassi di gestione del WB relativo al d.lgs. 231/2001 è consistita, per 15 anni, in tali modalità che vedevano – quasi sempre in maniera del tutto automatica e conseguente allo stesso incarico di OdV – l'OdV quale destinatario delle segnalazioni e gestore di queste ultime.

La normativa per il settore privato è intervenuta nel 2017 ed è confluita, come è noto, nel Modello organizzativo, il quale doveva indicare i canali di segnalazione e tutelare il segnalante da atti di ritorsione.

Tuttavia, la legge 179 non specificò che dovesse essere l'OdV a ricevere e gestire le segnalazioni.

> Nonostante in talune società – di dimensioni medio-grandi - si sia optato per soluzioni diverse (comitati ad hoc), non v'è dubbio che la soluzione nettamente prevalente sia rimasta quella di assegnare all'OdV la competenza a ricevere e gestire le segnalazioni interne.

Arena

"OdV e Whistleblowing"

Anche il recente d.lgs. 24/2023 non menziona esplicitamente l'OdV: esso prende posizione sull'individuazione del gestore delle segnalazioni interne che deve essere "una persona o un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero un soggetto esterno, anch'esso autonomo e con personale specificamente formato".

Certamente l'attività dell'OdV non è dedicata in via esclusiva alla gestione del WB; tuttavia, si potrebbe intendere – ed in effetti è stato inteso - l'aggettivo come riferito alla circostanza che la gestione del WB competa "esclusivamente" all'OdV.

A proposito della specifica formazione, i membri dell'OdV sono certamente tenuti a conoscere:

- la normativa in questione, con particolare riguardo a CHI può segnalare e COSA si può segnalare;
- i dettagli sull'uso del canale;
- il contenuto della procedura sulle segnalazioni;
- gli obblighi di riservatezza e le conseguenze della loro violazione.

In definitiva, a mio avviso, è possibile affidare all'OdV la ricezione e la gestione delle segnalazioni a condizione che:

- il Modello preveda tale attribuzione, la quale deve essere poi formalmente assegnata all'OdV dall'organo amministrativo dell'ente, con specifico incarico di tipo oneroso;

- sia garantita all'OdV – come, del resto, deve avvenire in generale per l'esercizio delle sue funzioni - la possibilità di ricorso a consulenti esterni per l'esame di questioni specialistiche connesse ai numerosi atti normativi le cui violazioni possono essere segnalate. Insomma, il budget dell'OdV deve tener conto di questa possibile attività;

- l'attività dell'OdV sia (precisamente ed esclusivamente) quella di esaminare ed approfondire le segnalazioni (come avvenuto sin dall'entrata in vigore del d.lgs. 231), esulando invece dai suoi compiti ogni profilo decisorio successivo (denuncia all'Autorità giudiziaria; ulteriore approfondimento investigativo; attivazione di un procedimento disciplinare) che compete agli organi gestori della società.

> Se l'OdV gestisce le segnalazioni può incorrere nella sanzione amministrativa prevista dall'art 21 d.lgs. 24 per l'omessa analisi ed approfondimento delle stesse (con sanzione dell'ANAC, compresa tra 10mila e 50mila euro).

Inoltre, è ipotizzabile a suo carico la violazione della riservatezza della segnalazione, pure sanzionata dall'art 21 e, in linea teorica, la condotta di ostacolo alla segnalazione (ad esempio, l'OdV viene contattato per verbalizzare una segnalazione e cerca di dissuadere indebitamente il dipendente).

Due ulteriori profili di responsabilità – che possono aggiungersi a quello ex art 21 di cui abbiamo appena parlato – sono invece ben noti.

L'omessa analisi della segnalazione potrebbe integrare grave inadempimento delle funzioni da parte dell'OdV e legittimerebbe l'organo amministrativo a revocargli l'incarico.

> L'omessa verifica della segnalazione potrebbe rilevare quale inefficace attuazione del Modello nella parte relativa al WB: se, per questo motivo, la società venisse sanzionata in sede penale ai sensi del d.lgs. 231, l'OdV potrebbe risponderne contrattualmente in sede civile nei confronti della società stessa.

Articolo di Maurizio Arena

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.himmeladvisors.it

HIMMEL ADVISORS
www.himmeladvisors.it

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