Newsletter

Nr. 3/2025 Luglio 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

HIMMEL® ADVISORS
www.himmeladvisors.it

benvenut*

In foto: Francisco Garcia-Garrido, Partner di Himmel Advisors

Carissimi Lettori,

È con entusiasmo e profonda gratitudine che vi presentiamo il terzo 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.

È stato un anno "accademico" ricco di sfide e di conquiste, un percorso fatto di continue prove e di approfondimenti che ci hanno permesso di crescere, di affrontare ogni ostacolo con rinnovata determinazione. Un anno in cui ogni difficoltà superata è stata un passo avanti, un'occasione di apprendimento e di rafforzamento, che ci ha portato a scoprire quanto il valore più grande risieda nella tenacia, nella capacità di reinventarsi e nella fiducia nel cammino intrapreso.

In Himmel, crediamo che il vero successo si costruisca grazie alle sfide che affrontiamo e alle soddisfazioni che condividiamo con voi. È stato un periodo di crescita condivisa, di sogni che si sono concretizzati e di obiettivi raggiunti con passione e perseveranza. Ogni vostro traguardo è per noi motivo di orgoglio e di esultanza, perché crediamo fermamente che il successo di uno sia il successo di tutti. Festeggiamo con entusiasmo i traguardi raggiunti, consapevoli che il nostro impegno, la vostra fiducia e il desiderio di miglioramento siano stati i motori di questa straordinaria avventura.

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

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 La gestione dei dati sanitari nel contesto europeo: verso un ecosistema condiviso e sicuro

Sintesi

La digitalizzazione dei dati sanitari rappresenta un'evoluzione fondamentale che può significativamente migliorare la qualità dei servizi sanitari offerti ai cittadini e cittadine europei e residenti nello SEE. Tuttavia, la creazione di uno spazio comune dei dati sanitari implica una serie di considerazioni legali, etiche e tecniche che devono essere affrontate con la massima attenzione. Ciò comprende il rispetto delle normative sulla privacy, l'interoperabilità dei sistemi e la trasparenza nei confronti dei pazienti.

La protezione della privacy dei pazienti è una priorità assoluta in qualsiasi iniziativa di condivisione dei dati sanitari. La normativa europea sul trattamento dei dati personali, rappresentata principalmente dal Regolamento Generale sulla Protezione dei Dati (GDPR), stabilisce rigorosi standard per garantire che i dati personali siano trattati in modo lecito, corretto e trasparente rispetto agli interessati. Le organizzazioni sanitarie sono chiamate a implementare solide misure di sicurezza per proteggere i dati dalla perdita, dall'accesso non autorizzato e da altre forme di trattamento illecito.

REGOLAMENTO (UE) 2025/327 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO dell'11 febbraio 2025
Scarica • 4.65MB

L'adozione del GDPR non solo assicura la protezione dei diritti degli individui, ma permette anche alle organizzazioni di affermare la propria responsabilità e trasparenza. È fondamentale stabilire un'infrastruttura di conformità solida, composta da politiche e processi che includano valutazioni d'impatto sulla protezione dei dati, formazione continua dei dipendenti e audit regolari di conformità.

In ambito sanitario vi sono però delle novità: il regolamento sullo spazio europeo dei dati sanitari, inclusivo dei dati genetici, è il Regolamento (UE) 2025/327("EHDS"), dell'11 febbraio 2025 che ha per oggetto l'accesso e la condivisione dei dati sanitari elettronici, sia a livello nazionale che infra-unionale.

Interoperabilità e Sicurezza

Un sistema di gestione dei dati sanitari efficace richiede un alto grado di interoperabilità. L'interoperabilità si riferisce alla capacità dei sistemi e delle organizzazioni diverse di funzionare insieme all'interno di un contesto comune. Questo significa che i vari sistemi informatici sanitari devono essere in grado di scambiarsi dati in modo sicuro e senza soluzione di continuità, indipendentemente dal fornitore del sistema.

Per raggiungere questo obiettivo, è necessario stabilire standard comuni, come HL7 (Health Level 7), che specificano come le informazioni cliniche debbano essere condivise. Inoltre, è cruciale implementare misure avanzate di sicurezza informatica, quali la crittografia dei dati, per prevenire accessi non autorizzati e proteggere l'integrità dei dati. Le entità coinvolte devono essere pronte a gestire i rischi associati agli attacchi informatici, adottando pratiche di sicurezza proattive e reattive.

Consenso Informato e Trasparenza

La trasparenza nel trattamento dei dati è fondamentale per costruire e mantenere la fiducia dei pazienti. Il consenso informato rappresenta un elemento chiave in questo contesto; i pazienti devono essere pienamente informati sui motivi e sulle modalità di raccolta, utilizzo e condivisione delle loro informazioni. Gli strumenti digitali possono facilitare questo processo, offrendo ai pazienti la possibilità di gestire in modo interattivo il proprio consenso, aggiornandolo e modificandolo secondo necessità.

Le organizzazioni devono garantire comunicazioni chiare e comprensibili, evitando tecnicismi eccessivi e illustrando in modo semplice i diritti dei pazienti. Devono essere predisposte procedure per consentire ai pazienti di revocare il consenso facilmente in qualsiasi momento, con conseguenti adeguamenti nell'accesso ai dati.

Tuttavia, l'implementazione di queste innovazioni comporta anche una serie di responsabilità etiche e legali. È indispensabile assicurare che le tecnologie utilizzate siano validate scientificamente e che i loro risultati siano costantemente monitorati. Le aziende e le istituzioni che sviluppano e utilizzano queste tecnologie devono attingere a team interdisciplinari, compresi esperti legali, etici e di sicurezza informatica, per garantire che tutti gli aspetti siano presi in considerazione.

Collaborazione e sviluppo sostenibile

Infine, la creazione di un ecosistema di dati sanitari richiede una forte collaborazione tra le diverse entità coinvolte, tra cui ospedali, cliniche, aziende tecnologiche, istituzioni di ricerca e organismi di regolamentazione. Tale cooperazione deve andare oltre la semplice condivisione dei dati e includere lo scambio di conoscenze, metodologie e tecnologie innovative.

Un approccio collaborativo permette di affrontare al meglio le sfide comuni, come la standardizzazione dei protocolli e la definizione di linee guida comuni per il trattamento dei dati. Inoltre, è importante coinvolgere i pazienti e le associazioni di pazienti nel processo di sviluppo e attuazione delle politiche sui dati sanitari. La loro partecipazione può contribuire a garantire che le politiche siano incentrate sui bisogni reali degli utenti e rispettino il loro diritto alla privacy.

La sostenibilità dell'ecosistema di dati richiede anche investimenti in infrastrutture e tecnologie adeguate. Le istituzioni sanitarie devono pianificare investimenti a lungo termine per l'aggiornamento delle tecnologie, la formazione del personale e l'implementazione di sistemi di monitoraggio e valutazione. Questo approccio garantisce che il sistema possa adattarsi alle mutate esigenze della società e affrontare le sfide emergenti nel settore della salute.

Il ruolo della ricerca e dello sviluppo

La ricerca rappresenta un elemento chiave nel progresso dell'ecosistema di dati sanitari. L'accesso a un'ampia varietà di dati può facilitare studi clinici, sperimentazioni e ricerche epidemiologiche, consentendo agli scienziati di sviluppare nuovi trattamenti e terapie. Tuttavia, la ricerca deve avvenire nel rispetto della privacy e dei diritti dei pazienti. È necessario sviluppare politiche di accesso ai dati che garantiscano il bilanciamento tra l'innovazione scientifica e la protezione della privacy. L'uso di tecnologie di anonimizzazione e pseudonimizzazione dei dati può giocare un ruolo cruciale facilitando l'accesso ai dati senza compromettere la riservatezza. Su tale argomento torneremo a breve. Per il momento è importante tenere in considerazione quanto specificato nel nuovo quadro normativo di riferimento: la ricerca dovrebbe essere condotta in modo etico e con la supervisione di comitati di revisione indipendenti. Questo aiuta a garantire che gli studi siano condotti in conformità con i principi etici e giuridici, tutelando gli interessi dei partecipanti e della comunità nel suo complesso nonché la protezione dei dati dei pazienti.

Implicazioni globali e cooperazione internazionale

L'argomento della gestione dei dati sanitari trascende le frontiere nazionali. La globalizzazione e la natura interconnessa della sanità globale richiedono una cooperazione internazionale per affrontare le difficoltà legate alla gestione dei dati. Le epidemie e le malattie infettive dimostrano chiaramente l'importanza di avere accesso a dati sanitari in tempo reale a livello globale.

Le organizzazioni sanitarie internazionali, come l'OMS, possono giocare un ruolo fondamentale nell'elaborazione di linee guida e normative per la gestione dei dati sanitari. Inoltre, la condivisione di dati tra paesi può fornire informazioni cruciali per la prevenzione e il controllo delle malattie, contribuendo a una risposta sanitaria globale più coordinata e tempestiva. La cooperazione internazionale deve includere anche questioni di equità. È essenziale garantire che i paesi in via di sviluppo possano accedere alle tecnologie e alle infrastrutture necessarie per la gestione dei dati sanitari. Le iniziative collaborative, come programmi di scambio e partnership tra istituti di ricerca, possono aiutare a colmare questi divari e a promuovere un approccio globale e giusto alla salute.

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

2 Un campanello d'allarme nel mondo digitale Il ransomware Medusa

Sintesi

Immaginate di essere comodamente seduti con una tazza di caffè, di controllare le vostre e-mail e all'improvviso... non funziona più nulla. Sul vostro schermo appare un messaggio minaccioso che vi chiede di pagare un riscatto per riavere accesso ai vostri dati. Benvenuti nel terrificante mondo del ransomware Medusa! Questo minaccioso software si è rivelato una delle armi informatiche più sofisticate e distruttive del nostro tempo.

Secondo una nuova ricerca di Elastic Security Labs, il driver dannoso, denominato ABYSSWORKER, viene distribuito insieme a un packer-as-a-service chiamato HeartCrypt per distribuire il ransomware Medusa.

Il predatore digitale dal nome Medusa

Medusa, che prende il nome dalla figura mitologica che trasformava in pietra chiunque la guardasse negli occhi, attacca i vostri dati con un effetto paralizzante simile. Penetra in profondità nei vostri sistemi con driver dannosi, aggirando elegantemente anche i sistemi EDR ben protetti. Ma forse la cosa più preoccupante è che Medusa è riuscita ad attaccare la sicurezza di piattaforme su cui facciamo affidamento ogni giorno: Gmail e Outlook.

Perché preoccuparsi?

Immaginate se qualcuno avesse il controllo di tutte le vostre comunicazioni digitali, sia professionali che personali. Questa idea non è più solo una finzione. Medusa non è una minaccia solo per le grandi organizzazioni, ma anche per i singoli che potrebbero non avere le risorse per proteggersi adeguatamente. Invece di adottare un approccio attendista al disastro, dovremmo diventare proattivi.

Il percorso verso la sicurezza digitale

C'è speranza! Utilizzando i moderni meccanismi di protezione, possiamo resistere alla minaccia. Iniziate aggiornando i vostri protocolli di sicurezza e assicurandovi che siano presenti password forti e uniche e l'autenticazione a più fattori. E a proposito di creatività, avete mai pensato di appassionare i vostri colleghi alla sicurezza informatica? Organizzate workshop, create sfide di sicurezza o premiate i comportamenti sicuri!

È necessario un approccio collettivo

Nel nostro mondo connesso, nessun problema è troppo grande se agiamo insieme. Tutto inizia con il rendersi conto dei rischi e agire prima che sia troppo tardi. Istruitevi, ampliate le vostre conoscenze e condividetele generosamente: la vostra comunità vi ringrazierà per questo.

Riflessioni finali

Medusa è un campanello d'allarme. Ci ricorda che dobbiamo rimanere vigili e rafforzare le nostre linee di difesa digitali. Attrezziamoci e agiamo per proteggere la nostra esistenza digitale. E ricordate: buone misure di sicurezza non sono un peso, ma una porta d'accesso alla libertà, alla creatività e al progresso nell'era digitale.

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

3 Dati sanitari elettronici "personali" e "non personali" alla luce del Regolamento (UE) sullo Spazio Europeo dei Dati Sanitari

Sintesi

Il Regolamento (UE) 327/2025 rappresenta un passo significativo verso la costruzione di uno Spazio Europeo dei Dati Sanitari (in inglese "EHDS"), concepito per facilitare l'accesso e la condivisione dei dati sanitari a livello "transnazionale", promuovendo al contempo la ricerca e l'innovazione nel settore della salute. Ne parlavamo in occasione del nostro articolo del mese di marzo (leggi qui). Un aspetto cruciale di questo regolamento è la chiara distinzione tra due concetti nuovi: i dati sanitari elettronici "personali" e i dati sanitari elettronici "non personali". Provvediamo ad analizzare questa distinzione.

I dati sanitari elettronici personali, come definiti dalla normativa, sono quelli che concernono una persona fisica identificata o identificabile, e quindi sono soggetti a tutela secondo il Regolamento (UE) 2016/679. L'art. 15 dell'EHDS fornisce un elenco delle categorie prioritarie dei dati sanitari elettronici personali, tra cui:

- profili sanitari sintetici dei pazienti
- prescrizioni elettroniche
- dispensazioni elettroniche
- esami diagnostici per immagini e relativi referti di immagini
- risultati degli esami medici, compresi i risultati di laboratorio e altri risultati diagnostici e relativi referti
- lettere di dimissione

Ricordiamo che, secondo l'articolo 4, paragrafo 1, del GDPR, un "dato personale" è qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente. Il trattamento di questi dati deve essere effettuato in conformità ai principi di liceità, correttezza e trasparenza, come delineato nell'articolo 5 dello stesso regolamento. È fondamentale riconoscere che i dati sanitari personali includono informazioni relative alla salute fisica o mentale di un soggetto, alla fornitura di servizi sanitari e all'uso di prodotti di salute (es. medicinali, apparecchiature mediche, ecc), tutti aspetti che conferiscono a tali dati una particolare sensibilità in fase di raccolta e gestione.

D'altro canto, il Regolamento (UE) 327/2025 introduce un concetto di dati sanitari elettronici nuovo, "i dati sanitari elettronici non personali", probabilmente un concetto ispirato alla necessità e doverosità di semplificare l'applicazione delle disposizioni dettate dal Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea. I dati sanitari elettronici non personali sono definiti dal nuovo EHDS come quei dati sanitari elettronici che non rientrano nella categoria dei dati sanitari elettronici personali, includendo sia i dati che sono stati anonimizzati in modo da non riferirsi più a una persona fisica identificata o identificabile («interessato»), sia i dati che non si sono mai riferiti a un interessato. Questi dati comprendono informazioni che sono state sottoposte a un processo di anonimizzazione, cioè che è stata effettuata una trasformazione tale da escludere definitivamente la possibilità di risalire all'identità del soggetto interessato.
Ai sensi del considerando 26 del GDPR, i dati anonimi non si qualificano come dati personali e quindi non sono soggetti alle normative di protezione dei dati. Ma attenzione! L'anonimizzazione non solo è una

tecnica o misura di sicurezza bensì un trattamento di dati personali. Per questo motivo, il quadro normativo applicabile stabilisce che i metodi di anonimizzazione devono essere sufficientemente rigorosi da garantire che non ci sia alcun modo per re-identificare gli individui attraverso tecniche di de-anonimizzazione o combinazione di dati.

I dati sanitari elettronici non personali possono anche includere dati che non si sono mai riferiti a un soggetto specifico (tecnica dell'anonimizzazione by default o alla fonte). Un esempio potrebbe consistere in dati aggregati ottenuti da studi clinici o da database sanitari che forniscono informazioni generali su un gruppo di popolazione, senza identificare quelli che fanno parte dell'insieme selettivo (i record sono esclusi in quanto contengono dati pseudonimizzati). Questi approcci si rivelano fondamentali per garantire che i sistemi sanitari possano sfruttare informazioni preziose per la pianificazione, il monitoraggio epidemiologico e la programmazione strategica a livello provinciale, regionale, nazionale ed UE della governance della salute pubblica, senza compromettere la riservatezza dei singoli individui.

Un altro aspetto di notevole importanza è la distinzione tra dati anonimi e dati pseudonimizzati, che riveste un ruolo centrale nel contesto della normativa sulla privacy. Questa distinzione è espressamente richiamata nel quadro definitorio dell'EHDS. Secondo l'articolo 4, paragrafo 5, del GDPR, i dati pseudonimizzati sono dati personali che non possono più essere attribuiti a un soggetto specifico senza l'uso di informazioni aggiuntive. Nonostante tale misura riduca i rischi di identificazione, i dati pseudonimizzati continuano a essere trattati come dati personali e, pertanto, godono delle stesse protezioni previste per i dati sanitari elettronici personali. Questo significa che, alla data odierna, i dati sanitari elettronici pseudonimizzati sono soggetti a condizioni di trattamento più rigorose e devono essere gestiti in conformità con i principi stabiliti dal GDPR.

La regolamentazione dei dati sanitari elettronici deve tenere conto non solo della mera categorizzazione (sopra richiamata), ma anche delle implicazioni più ampie che queste distinzioni comportano per gli individui e per le organizzazioni nel suo complesso. La corretta gestione dei dati sanitari è essenziale non soltanto per garantire la protezione dei dati personali ai sensi del GDPR e dell'EHDS, ma anche per favorire una cultura del rispetto e della responsabilità nella manipolazione delle informazioni sanitarie, ad esempio, nell'ambito ricerca scientifica. In un contesto in cui la digitalizzazione pervade ogni aspetto della vita, la sfida principale risiede nella praticità e nella capacità di bilanciare l'innovazione tecnologica con la protezione dei diritti fondamentali.

Il quadro normativo fornito dal Regolamento (UE) 327/2025 ci invita a riflettere su un'altra questione fondamentale: come possiamo garantire che l'uso dei dati non personali per scopi di ricerca e analisi non comprometta mai la possibilità di recuperare informazioni sensibili su individui specifici? Questo interrogativo porta alla luce la necessità di implementare sia procedure che tecnologie adeguate per l'anonimizzazione e la pseudonimizzazione, mantenendo nel contempo un forte impegno verso la trasparenza e la responsabilità. Non si può ignorare il potenziale positivo della condivisione dei dati, soprattutto nel contesto della salute pubblica e della ricerca scientifica e medica. L'accesso a dati aggregati o anonimi può accelerare le scoperte scientifiche, migliorare gli studi epidemiologici, e potenziare le risposte alle potenziali crisi sanitarie ovvero allo sviluppo di un progetto di ricerca futuro. Tuttavia, è cruciale che i ricercatori e le istituzioni pubbliche comprendano appieno le differenze tra i vari tipi di dati, in modo da adottare pratiche corrette e responsabili, sin dalla progettazione.

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

4 Trasparenza e Privacy: la sentenza della Corte di Giustizia UE nella causa C-33/22

Sintesi

Durante la pandemia da Covid-19, la gestione delle informazioni pubbliche è diventata un tema cruciale. Un caso significativo nasce nella Repubblica Ceca, dove un cittadino ha richiesto documenti al Ministero della Salute in merito all'acquisto di test diagnostici. Il Ministero ha fornito tali documenti oscurando nomi, email e firme, richiamandosi al GDPR e all'impossibilità di contattare preventivamente le persone coinvolte.

I giudici cechi hanno chiesto alla Corte di Giustizia dell'UE se tali informazioni, usate professionalmente, restano dati personali e se una legge nazionale può condizionare la trasparenza alla comunicazione preventiva agli interessati. La risposta della Corte è stata chiara: anche nell'ambito professionale, questi dati restano comunque dati personali. Tuttavia, la tutela della protezione dei dati personali non deve impedire l'obbligo di trasparenza.

- Sentenza della CGUE (Grande Sezione) 16 gennaio 2024 / Österreichische vs. WK

Le nazioni possono prevedere garanzie, purché mantengano il principio della proporzionalità. Ogni situazione deve essere esaminata singolarmente per determinare se l'accesso ai dati serve un interesse pubblico prevalente, come il controllo sull'uso dei fondi pubblici. Questo è possibile, a condizione che sia stata:

- verificata la possibilità di informare gli interessati;
- effettuata una valutazione di impatto (ex art. 35 GDPR).

In casi come le indagini su programmi sanitari pubblici, potrebbe essere essenziale rivelare il nome di un medico per garantire trasparenza, sempre rispettando le garanzie stabilite. Il GDPR non proibisce la divulgazione di dati personali, ma richiede un bilanciamento responsabile tra diritti. La sentenza impone alle amministrazioni pubbliche di giustificare chiaramente le loro scelte di oscuramento o divulgazione e di dimostrare l'avvenuto tentativo di contatto con le persone coinvolte.

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.

Per cittadini e giornalisti, questa sentenza apre a maggior accesso a informazioni di interesse pubblico legittimo. La Corte promuove una cultura della trasparenza avanzata, in cui privacy e trasparenza si integrano come diritti complementari. Si supera così il concetto di "riservatezza assoluta", permettendo una convivenza equilibrata tra privacy e l'accesso all'informazione.

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

5 Intelligenza Artificiale e Risorse Umane: efficienza, inclusione e compliance nell'era della trasformazione digitale

Sintesi

Nel panorama contemporaneo, l'intelligenza artificiale (IA) non rappresenta più un'innovazione di nicchia ma una tecnologia fondamentale, capace di ridefinire profondamente il ruolo delle Risorse Umane (HR) e della funzione Compliance. La diffusione di strumenti di IA nei processi di recruiting, HR Management, formazione e valutazione delle performance apre opportunità straordinarie in termini di efficienza, personalizzazione ed equità. Tuttavia, emergono anche sfide rilevanti sul fronte della protezione dei dati personali, della trasparenza decisionale e della gestione dei rischi di discriminazione. Il ruolo dell'HR & Compliance Officer diventa quindi centrale: governare l'adozione dell'IA assicurando il rispetto dei diritti dei lavoratori, la correttezza procedurale e l'allineamento normativo.

Recruitment "smart": l'IA accelera e migliora i processi

Le soluzioni di smart-recruitment basate su Natural Language Processing consentono oggi di analizzare grandi volumi di CV, lettere motivazionali e profili social, generando uno scoring oggettivo dei candidati.

Secondo l'Osservatorio HR Innovation Practice del Politecnico di Milano, il 32% delle aziende italiane utilizza almeno una soluzione di IA in ambito HR. Piattaforme come Clutch o HireVue sfruttano l'analisi semantica per estrarre competenze chiave e misurare l'affinità dei profili rispetto ai requisiti richiesti, riducendo fino al 70% i tempi di screening preliminare. Anche lato candidato, l'adozione è crescente: secondo un'indagine citata da Avvenire, il 26% dei candidati utilizza strumenti di IA generativa (ad es. ChatGPT) per scrivere o ottimizzare il proprio CV e la lettera di motivazione, percentuale che sale al 57% tra i giovani della Generazione Z.

Parallelamente, l'impiego di chatbot HR automatizza il primo contatto con il candidato, fornendo risposte immediate su policy aziendali, benefit e modalità di onboarding, migliorando la candidate experience e liberando risorse umane per attività a maggior valore aggiunto. Tuttavia, gli HR devono garantire un monitoraggio umano ("human-in-the-loop") delle shortlist generate dall'IA, per prevenire il rischio di bias impliciti basati su genere, etnia o età. Dal punto di vista privacy è importante tenere in considerazione l'orientamento dell'Autorità Garante nonché la normativa privacy applicabile sui processi decisionali automatizzati.

Evoluzione del mercato del lavoro nell'Eurozona: IA come driver di cambiamento

L'introduzione massiva dell'IA non è neutrale rispetto alla composizione occupazionale. Secondo uno studio di ING Bank, tra il 2015 e il 2025 la quota di lavoratori occupati in settori ad alta complementarietà con l'IA (sanità, servizi professionali, attività tecniche) nell'Eurozona è salita dal 32% al 35%.

In parallelo, la quota dei lavoratori in ruoli più manuali, come edilizia o ospitalità, è scesa dal 28% al 25%.

Il Nord Europa (Paesi Bassi, Belgio, Francia, Germania) presenta percentuali di lavori "AI-ready" superiori al 39%, mentre nel Sud (Italia, Spagna) il 50% delle occupazioni resta concentrato in attività a basso impatto tecnologico. Questa polarizzazione potrebbe ampliare i divari produttivi tra Nord e Sud, rallentando la convergenza economica nell'Eurozona. Per le organizzazioni italiane è essenziale investire ora in formazione digitale, upskilling e riconversione delle competenze per cogliere le opportunità offerte dalla trasformazione AI.

Employee Analytics e Formazione personalizzata: la nuova gestione delle risorse

Oltre al recruiting, l'IA sta trasformando la gestione dei dipendenti lungo tutto il loro ciclo di vita. Piattaforme di employee analytics analizzano dati aggregati su performance, produttività, presenze, engagement e sentiment, supportando decisioni data-driven su promozioni, piani di successione e talent retention.

L'adozione di sistemi di adaptive learning permette di creare percorsi formativi su misura per ogni lavoratore, adattando contenuti e modalità di erogazione in base ai bisogni formativi reali, migliorando engagement e risultati. Secondo i dati citati da IPSOA, oltre l'80% delle aziende globali ha già incrementato il budget destinato all'apprendimento e allo sviluppo per favorire la costruzione di workforce agili, capaci di collaborare con i nuovi sistemi intelligenti.

Privacy e protezione dei dati personali: una sfida cruciale per gli HR

Il trattamento di dati personali tramite sistemi di IA nei processi HR pone questioni fondamentali di compliance al GDPR. Molte applicazioni di IA utilizzano dati altamente sensibili (ad esempio etnia, condizioni di salute, orientamento religioso o politico), sia in fase di selezione che nella gestione della vita lavorativa. Come evidenzia l'Associazione Italiana Formatori, è essenziale per gli HR Manager:

- Identificare correttamente la base giuridica del trattamento (consenso, obblighi contrattuali o legittimo interesse)
- Applicare rigorosi principi di minimizzazione e limitazione della conservazione dei dati
- Realizzare valutazioni d'impatto sulla protezione dei dati (DPIA) ogni volta che si introduce un trattamento automatizzato significativo
- Garantire la trasparenza verso candidati e dipendenti, mediante informative chiare e accessibili
- Coinvolgere il DPO e il Comitato Etico HR (ove presente) nella validazione dei progetti IA e durante la conduzione della relativa FRIA.

Una gestione superficiale potrebbe esporre l'azienda a pesanti sanzioni amministrative (fino a 20 milioni di euro o il 4% del fatturato globale annuo) e danni reputazionali.

Il quadro regolamentare: verso l'AI Act europeo

Con il prossimo (applicazione dal 2026) AI Act dell'Unione Europea, i sistemi di IA applicati a processi di selezione del personale, valutazione delle performance o gestione contrattuale saranno classificati come "ad alto rischio".

Questo implica per le aziende l'obbligo di effettuare rigorose valutazioni d'impatto sulla conformità, implementando sistemi di gestione dei rischi e governance AI. Inoltre, sarà necessario adottare misure di trasparenza ed explainability degli algoritmi e garantire auditabilità e possibilità di intervento umano sui processi automatizzati. La funzione HR dovrà quindi cooperare strettamente con la funzione Legale, IT Security e DPO per assicurare il rispetto delle nuove disposizioni.

Governance dell'IA in azienda: raccomandazioni operative

Per garantire un'adozione etica e conforme dell'IA in ambito HR, è opportuno:

- Definire policy interne chiare sull'uso di algoritmi nei processi decisionali
- Formare manager, recruiter e responsabili HR sulle implicazioni tecniche e giuridiche dell'IA
- Istituire Comitati AI interfunzionali per supervisionare i progetti più sensibili
- Adottare modelli di explainability per rendere interpretabili i criteri alla base delle decisioni automatizzate
- Promuovere una cultura della responsabilità condivisa, valorizzando il contributo umano nella supervisione dei processi decisionali

Inoltre, è essenziale progettare percorsi di reskilling e upskilling per preparare tutti i lavoratori (non solo quelli tecnici) ad affrontare i cambiamenti derivanti dalla trasformazione digitale.

Conclusioni

L'Intelligenza Artificiale offre al mondo HR strumenti potentissimi per attrarre, gestire, sviluppare e fidelizzare i talenti. Tuttavia, senza una governance consapevole, senza un impegno concreto sulla compliance normativa e sull'etica dei dati, il rischio di derive discriminatorie o di danni reputazionali diventa reale. Il futuro del lavoro non sarà dominato dalle macchine, ma da un nuovo equilibrio tra intelligenza artificiale e intelligenza umana: un equilibrio che la funzione HR & Compliance ha il compito – e l'opportunità – di costruire sin d'ora.

Autore: A. Sticchi (Avv. e Compliance Officer presso Himmel Advisors)

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

6 Modelli 231 inadeguati: la decisione della Corte di Cassazione

Sintesi

La Corte di Cassazione, attraverso la decisione n. 4535/2025, ha accolto il ricorso di una società contro l'imposizione di una misura interdittiva di un anno dai rapporti con la PA. Il fulcro della sentenza riguarda la non retroattività di una violazione amministrativa collegata a un reato.

La società ha contestato la decisione del Tribunale del riesame, sostenendo che i giudici avevano erroneamente valutato un illecito secondo il D.Lgs. n. 231/2001, nonostante il fatto che il reato presupposto fosse stato incluso solo con l'art. 5 del D.Lgs. n. 75 del 2020. La condotta della società era avvenuta prima di questa modifica legislativa, il che violerebbe il principio di irretroattività. La società ha anche argomentato che, essendo trascorsi oltre cinque anni dalla fine delle attività ascrivibili al potenziale reato fino al primo atto interruttivo (la richiesta della misura cautelare), l'illecito risulterebbe prescritto ai sensi dell'art. 22 del D.Lgs. n. 231/2001.

La Cassazione ha chiarito che non si può sanzionare un ente per un illecito inesistente al momento della supposta attività fraudolenta. Ha anche precisato che le attività post 2020, considerate dal Tribunale come continuità dell'illecito, non costituiscono di per sé un illecito amministrativo a meno che non siano state inizialmente pianificate per nascondere un inadempimento doloso.

A sostegno di tale affermazione la Corte sottolinea i seguenti elementi che rappresenterebbero il carattere inadeguato del MOG adottato:

- Mancanza di una mappatura completa del rischio reato;
- Assenza di documentazione comprovante lo svolgimento di controlli da parte dell'Organismo di Vigilanza;
- Limitatezza del budget affidato all'OdV per lo svolgimento dei suoi compiti (pari a 2.500 Euro annui);
- Inadeguatezza della composizione monocratica dell'OdV.

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

7 Conservi i metadati oltre 7 giorni e, lo sai...

Sintesi

"La valigia sul letto" per un viaggio spensierato dove "la cintura" balla "despacito" intorno ad una "barbacoa" con gli amici, alle Canarie. Dopo un anno di compliance, i titolari si meritano, anche, un po' di "chiringuito" e "playa". Tuttavia, l'Autorità Garante ha stabilito - con rigore inflessibile - di fare ordine anche quest'estate, turbandone i sonni alla Regione Lombardia. Pur considerando che la Commissione Europea stia presa in un processo che mira a semplificare il Regolamento Generale sulla Protezione dei Dati (GDPR), soprattutto per lenire i gravami amministrativi sopportati dalle Piccole e Medie Imprese, questa iniziativa ha scatenato una molteplicità di reazioni che vanno dal cauto ottimismo a dubbi e timori diffusi. Parallelamente, e forse anche lontani dalla semplificazione verso cui punta la Commissione Europea, l'Autorità Garante italiana per la Protezione dei Dati Personali, con il provvedimento n. 243 del 29 aprile 2025, ha fatto luce su un aspetto particolarmente delicato: il trattamento dei metadati, in particolare, all'interno delle Pubbliche Amministrazioni.

Che cosa sono i metadati?

I metadati, un termine che fino a poco tempo addietro suscitava perplessità e scetticismo, sono stati posti al centro del dibattito giuridico e tecnologico dal Provvedimento di indirizzo del 6 giugno 2024 del Garante italiano. Questo documento ha avviato una discussione più ampia sui programmi e servizi informatici di gestione della posta elettronica e sul trattamento dei metadati dei dipendenti, comparto che era fino ad allora oscuro a molti, salvo che agli addetti ai lavori più tecnici.

Dal punto di vista tecnico-legale, i metadati si configurano come informazioni che descrivono altri dati: essi forniscono dettagli e contesto che migliorano la gestione, l'accessibilità e l'utilizzo di file, documenti, immagini o database. Ciò nonostante, dal punto di vista della privacy, la loro gestione introduce problematiche significative per molti titolari del trattamento, costretti a misurarsi con nuove ed esigenti regolamentazioni sulla gestione delle e-mail e metadati legati alle attività dei lavoratori.

Perché si torna a parlare dei metadati?

Il provvedimento del 2024 non rappresenta un debutto assoluto nel panorama delle responsabilità a carico dei titolari del trattamento di adeguarsi al GDPR e alle normative giuslavoristiche vigenti. Tali obblighi erano già ben consolidati dal momento in cui il GDPR e il Codice Privacy sono entrati in vigore. La novità, semmai, risiede nell'intensità con cui le aziende e le PA debbono adesso confrontarsi con questi vincoli regolatori più stringenti, rispolverando una certa trascuratezza nel loro approccio ai metadati sino alla data odierna.

Nel frattempo, la recente attenzione del Garante su questi dettagli operativi rimette in discussione non solo la consapevolezza diffusa delle imprese e delle PA rispetto alle loro funzioni e obblighi, ma anche il ruolo perpetuo delle autorità di vigilanza nel guidare e, quando necessario, correggere il modo in cui tali obblighi vengono interpretati e attuati. L'efficacia di queste riforme resta un nodo critico, mentre il

trattamento dei metadati si rivela un campo in bilico tra l'atemporalità del diritto e l'evoluzione inesorabile della tecnologia.

Premesse sul nuovo provvedimento del Garante in materia "metadati"

Il recente provvedimento n. 243 del 29 aprile 2025 esamina un'indagine svolta dal Garante per la protezione dei dati personali sui trattamenti di dati personali da parte della Regione Lombardia, con particolare enfasi sui log di navigazione in Internet e sui metadati di posta elettronica utilizzati nell'ambito lavorativo. Di seguito un brevissimo sunto del Provvedimento.

Oggetto e attività istruttoria

L'indagine del Garante è stata avviata per valutare il rispetto delle norme in materia di protezione dei dati personali, in particolare per quanto riguarda i trattamenti di dati effettuati nel contesto del lavoro agile. Gli accertamenti si sono concentrati sull'uso di strumenti informatici da parte del personale regionale e sulle modalità di gestione e conservazione dei dati generati.

Normativa Applicabile

Il quadro normativo di riferimento comprende il Regolamento UE 2016/679 (GDPR) e il Codice Privacy italiano. Elemento chiave è l'articolo 4 della Legge 300/1970, che disciplina i controlli a distanza sui lavoratori. Altre disposizioni rilevanti includono gli articoli 5 (principi applicabili al trattamento di dati personali), 6 (liceità del trattamento), 25 (protezione dei dati fin dalla progettazione e per impostazione predefinita), e 35 (valutazione d'impatto sulla protezione dei dati) del GDPR.

Esito dell'Attività Istruttoria

Metadati di Posta Elettronica:

- I metadati delle e-mail sono stati conservati per 90 giorni, senza un accordo collettivo con le rappresentanze sindacali, il che viola le normative sui controlli a distanza previsti dallo statuto dei lavoratori.
- È stato stabilito che questo tipo di conservazione prolungata rende possibile il controllo indiretto delle attività lavorative, imponendo pertanto l'adozione di garanzie procedurali previste dalla legge.

Log di Navigazione Internet:

- La raccolta e la conservazione sistematica dei log di navigazione Internet possono includere dati non pertinenti, rappresentando una violazione del principio di proporzionalità del GDPR.
- L'indagine ha posto in evidenza la mancanza di un accordo sindacale sui controlli a distanza e ha determinato che la tecnologia utilizzata potrebbe portare a un monitoraggio non giustificato del personale.

Gestione delle Richieste di Assistenza Tecnica:

- I dati legati alle richieste di assistenza tecnica sono stati conservati per periodi estesi oltre quanto necessario, violando i principi di limitazione della conservazione.
- Il sistema di assistenza tecnica, particolarmente il sistema "OTRS" in fase di dismissione, non era regolamentato in conformità con il GDPR durante il trattamento transitorio.

A seguito dell'indagine, il Garante:

- Ha imposto una sanzione pecuniaria di 50.000 euro complessivi, suddivisa in tre parti: 20.000 euro per la violazione relativa ai metadati di posta elettronica, 25.000 euro per i log di navigazione, e 5.000 euro per la gestione delle richieste di assistenza tecnica.

- Ha disposto una serie di misure correttive per rendere conformi i trattamenti, tra cui la riduzione dei periodi di conservazione dei dati e l'adozione di nuovi accorgimenti tecnici e organizzativi per minimizzare i rischi per i diritti e le libertà fondamentali dei dipendenti.

- Ha richiesto alla Regione di presentare una relazione documentata delle azioni intraprese per rimediare alle violazioni, da inviare entro 30 giorni dalla notifica del provvedimento.

L'intervento intende garantire un adeguamento strutturale delle procedure di trattamento dei dati personali all'interno della Regione Lombardia, promuovendo la trasparenza e la sicurezza nella gestione delle informazioni dei dipendenti.

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.

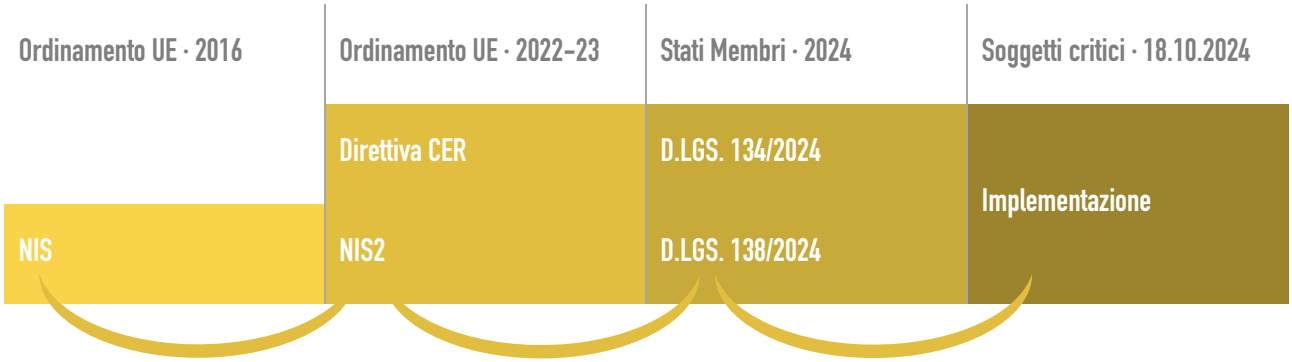
La Direttiva NIS del 2016, conosciuta come Direttiva sulla sicurezza delle reti e dei sistemi informatici, è una normativa dell'Unione Europea adottata per migliorare la sicurezza informatica all'interno degli Stati membri. Essa stabilisce requisiti di sicurezza e obblighi di reportistica per i servizi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

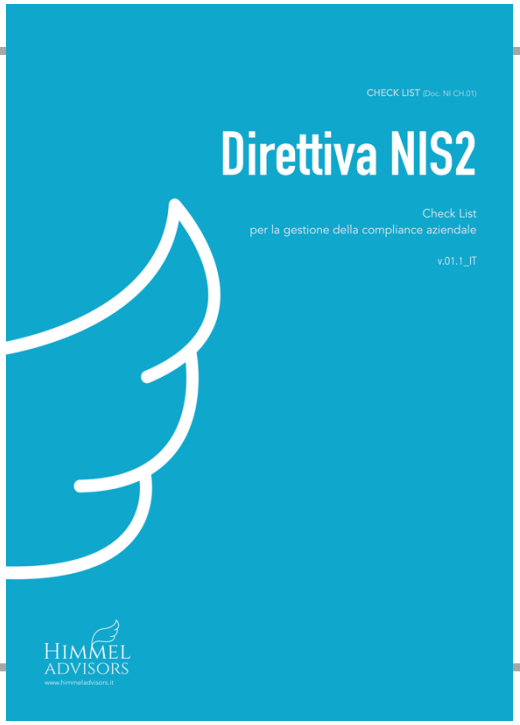


La Check List NIS2 di Himmel Advisors

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



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.

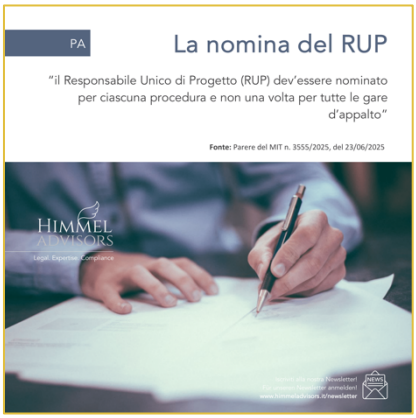
Navigare l'intricata rete normativa contemporanea può essere una sfida per molte organizzazioni, che spesso faticano a distinguere tra obblighi, doveri e facoltà. Il nostro lab si propone di mitigare questa complessità: fungiamo da intermediari esperti, filtrando e razionalizzando le normative per offrire 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

Bites: 30-sec compliance



HIMMEL ADVISORS

Sappiamo che non hai tempo. Ma siamo qui per aiutarTi!

Nel mondo frenetico di oggi, spesso la compliance viene trascurata o sottovalutata. Siamo qui per cambiarlo! Le "30-sec compliance bites" di Himmel Advisors offrono aggiornamenti rapidi e incisivi su temi cruciali per ispirare i lettori a riscoprire il valore della compliance. Con un approccio fresco e una comunicazione immediata, miriamo a sensibilizzare e stimolare azioni concrete all'interno delle organizzazioni.

Queste pillole sono solo un punto di partenza. Per una comprensione approfondita, consulta il tuo consulente o la tua consulente o i professionisti di fiducia. Scopri come la compliance può diventare il motore di un cambiamento positivo!

Accedi alle nostre Bites

AI+ Healthcare Certificate: in HIMMEL, la formazione al primo posto

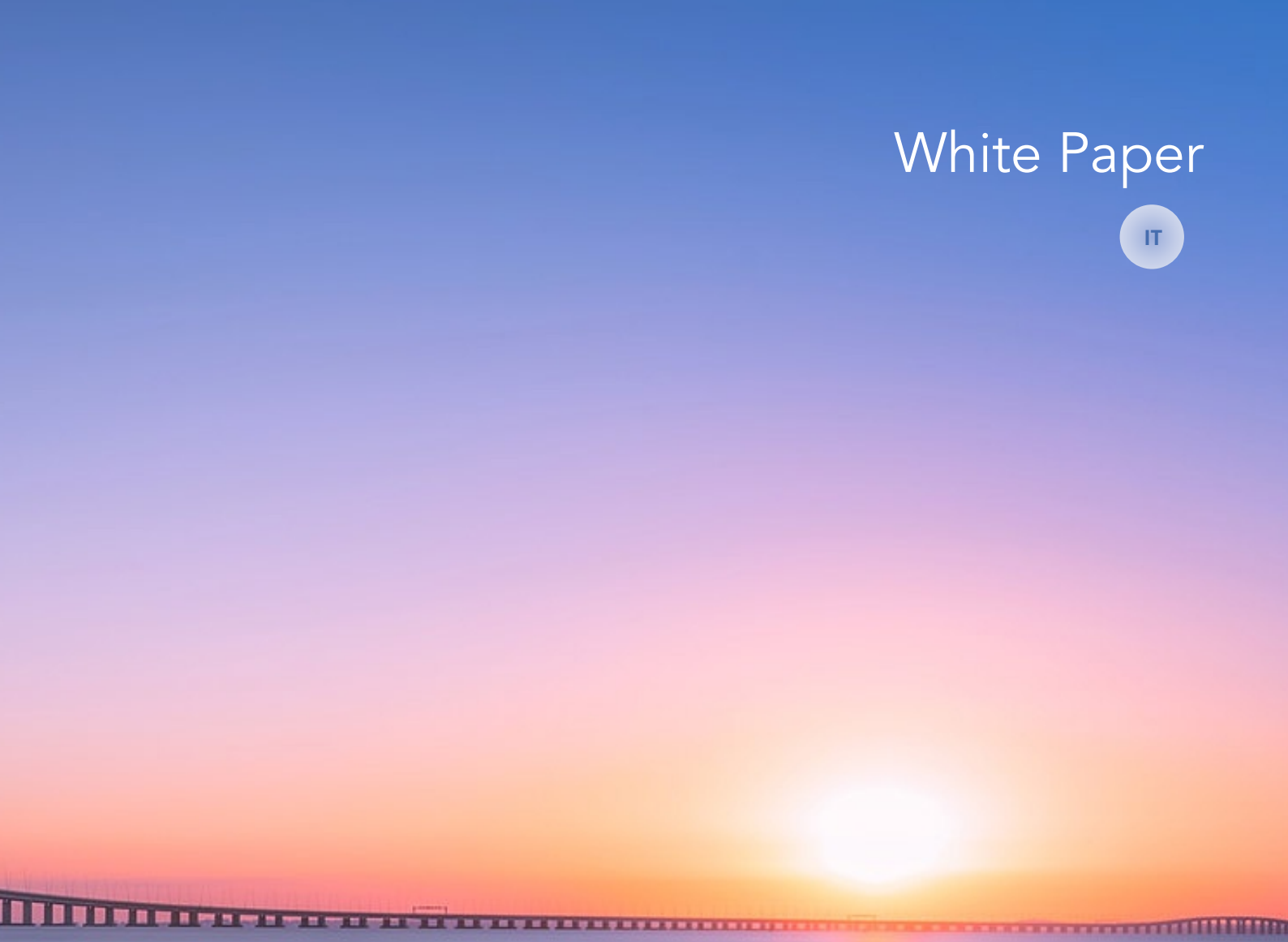
Immagine del sito: https://www.itsmhub.com/pages/ai-certs

Siamo entusiasti di annunciare che abbiamo ottenuto la certificazione in Specializzazione AI+ Healthcare dall'Istituto AI CERTs™. I progressi nella tecnologia dell'intelligenza artificiale offrono opportunità senza precedenti per rivoluzionare l'assistenza sanitaria, rendendola più efficace, accessibile ed economicamente sostenibile. Promuovendo l'integrazione dell'AI attraverso politiche adeguate, possiamo migliorare l'equità, l'assistenza e garantire che le innovazioni tecnologiche, i nuovi trattamenti e farmaci portino benefici concreti a tutta la società.

Nella diagnostica, l'AI aumenta la precisione e consente diagnosi più precoci, spesso aprendo la strada a opzioni terapeutiche meno invasive e più convenienti. I piani di trattamento personalizzati, basati sull'AI, integrano approcci tradizionali, offrendo cure più mirate ed efficaci, migliorando i risultati per i pazienti e contribuendo a ridurre i costi del sistema sanitario.

White Paper

IT



AI ACT

Uno sguardo ai nuovi obblighi
per società private ed enti pubblici

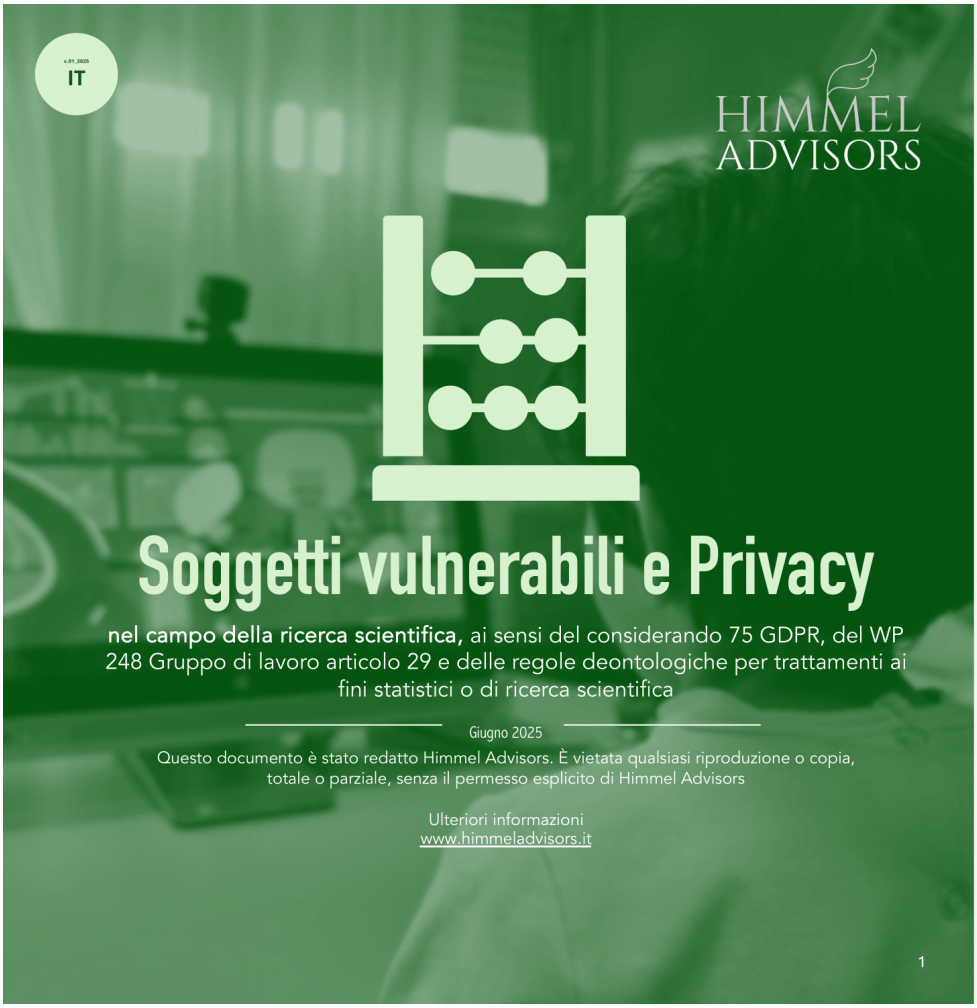
v.01.1_IT

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

HIMMEL
ADVISORS
www.himmeladvisors.it

Soggetti vulnerabili e Privacy nel campo della ricerca scientifica



Copertina del materiale di studio: Soggetti vulnerabili e Privacy

Nel contesto della ricerca scientifica, la tutela dei soggetti vulnerabili e la protezione della privacy costituiscono pilastri imprescindibili per garantire un approccio #etico e legalmente conforme. Gli strumenti normativi di riferimento, tra cui il #Regolamento (UE) 2016/679, stabiliscono principi di ampio respiro riguardanti obblighi e doveri in capo alle #università ed i #centri di ricerca in occasione della raccolta, il trattamento e la conservazione dei dati personali di soggetti #vulnerabili, come #minori, persone con #disabilità o soggetti in condizioni di #fragilità che partecipano ad un #progetto di #ricerca.

Il documento è a disposizione all'interno della sezione "Publications" del nostro sito web (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

Attenzione agli utenti di Microsoft!
Sotto attacco!

Immagine CC Copyrights

“Da giorni alcuni hacker criminali stanno portando avanti una serie di attacchi informatici a livello globale, sfruttando una falla ‘sistemica’ di Microsoft, in particolare di SharePoint, software di gestione del noto sistema operativo. Compromesse agenzie e enti governativi negli USA, università, aziende di telecomunicazione. Maccari (Sielte): “Mantenere aggiornati tutti i sistemi di sicurezza”.

Nonostante le evidenti vulnerabilità, Microsoft non ha ancora rilasciato patch specifiche, lasciando i server a rischio. Questi attacchi, classificati come 'zero-day', hanno generalmente coinvolto server interni (non il cloud), e potrebbero permettere ai cybercriminali di sottrarre dati sensibili o password. La sicurezza informatica in USA è sotto scrutinio, anche a causa di recenti cambiamenti amministrativi che hanno rallentato le risposte. Esperti consigliano di mantenere aggiornati tutti i sistemi, attivare sistemi di monitoraggio e response, e adottare strategie multilivello per ridurre i rischi. Il CSIRT italiano ha raccomandato di aggiornare subito i prodotti vulnerabili di SharePoint e di seguire le indicazioni di sicurezza fornite, tra cui il monitoraggio di traffico anomalo e l’attivazione di strumenti di difesa come IoC e scansioni antimalware.

Fonte: https://www.washingtonpost.com/technology/2025/07/20/microsoft-sharepoint-hack/

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

Fragalà Giovanna

"Regolamento EDHS: obblighi chiave dei titolari del trattamento"

Legal Counsel, AI & Data Protection

Giovanna Fragalà è Head of privacy & AI dpt. presso RCS MediaGroup.

Professionista esperta in protezione dei dati personali e intelligenza artificiale con una vasta esperienza sia in studi legali che in aziende.

In qualità di membro del gruppo di esperti dell'EDPB, co-chair dell'IAPP Milan Knowledgenet chapter e chair di Women in AI Governance a Milano, Giovanna contribuisce a rilevanti dibattiti sulla privacy nonché in relazione governance dell'intelligenza artificiale. È anche una relatrice esperta in forum di primo piano, autrice di vari articoli online e Auditor ISO/IEC 27001:2022.

"I titolari e/o gli utenti dei dati sanitari possono essere soggetti a sanzioni amministrative pecuniarie fino a 10.000.000 EUR o al 2% del fatturato mondiale annuo, se superiore, in caso di non conformità quali, ad esempio, rifiuto intenzionale di fornire dati, il mancato rispetto dei termini, nonché uso secondario vietato di Dati

Fragalà

"Regolamento EDHS: obblighi chiave dei titolari del trattamento"

Il regolamento UE 2025/327 ("Regolamento") mira a migliorare l'accesso delle persone fisiche ai propri dati sanitari elettronici ("Dati") e il loro controllo su di essi per l'assistenza sanitaria ("uso primario"), e al contempo facilitare l'utilizzo di tali Dati per finalità di interesse pubblico come ricerca, innovazione e politiche sanitarie ("uso secondario").

Il trattamento dei Dati rimane soggetto al Regolamento (UE) 2016/679 ("GDPR") e al Regolamento (UE) 2018/1725 per le istituzioni dell'UE, a cui tra le altre cose, si rimanda anche per la definizione di titolare del trattamento. Il Regolamento introduce una serie di obblighi specifici per diversi soggetti che a seconda dei casi possono operare come titolari del trattamento.

Chi sono i titolari del trattamento?

Ai sensi del GDPR, titolare del trattamento è colui che determina mezzi e finalità del trattamento. Secondo il Regolamento le categorie di soggetti che operano come titolari del trattamento in generale sono:

- titolare dei dati sanitari;
- organismo responsabile per l'accesso ai dati ("HDAB").

Nel contesto dell'uso secondario, ai sensi dell'art. 74 del Regolamento:

- titolare dei dati sanitari è il titolare del trattamento per la messa a disposizione dell'HDAB dei Dati richiesti.
- HDAB è il titolare del trattamento per la preparazione e la messa a disposizione dei Dati nonché tutti gli altri compiti previsti dal Regolamento.
- L'utente dei dati sanitari è il titolare del trattamento quando tratta i Dati per l'uso secondario e all'interno dell'ambiente di trattamento sicuro.
- I titolari di dati sanitari affidabili (se designati dagli Stati membri per una procedura semplificata) agiscono come titolari del trattamento per la fornitura

dei Dati e come responsabili del trattamento per l'utente dei dati quando forniscono dati tramite un ambiente sicuro.

Obblighi per i titolari nel contesto dell'uso primario

I titolari dei dati sanitari e più in generale i prestatori di assistenza sanitaria devono garantire:

(i) accesso ai dati sanitari elettronici dei pazienti: i pazienti devono accedere gratuitamente e immediatamente tramite servizi di accesso elettronico nonché scaricare una copia elettronica in un formato europeo comune. I prestatori non possono ostacolare la trasmissione dei Dati ad altri prestatori di assistenza sanitaria scelti dal paziente.

(ii) (ii) registrazione e aggiornamento dei dati: i prestatori sono tenuti a registrare i Dati pertinenti all'interno di un sistema di cartelle cliniche elettroniche nonché garantire che i Dati siano aggiornati con le informazioni relative all'assistenza sanitaria prestata.

(iii) (iii) rettifica dei dati: su richiesta delle persone fisiche, devono verificare l'accuratezza delle informazioni per la rettifica di Dati errati, coinvolgendo un professionista sanitario competente se necessario.

(iv) (iv) identificazione nelle cartelle cliniche: i sistemi di cartelle cliniche elettroniche devono identificare il professionista sanitario e il prestatore che ha effettuato la registrazione o l'aggiornamento dei dati, e l'ora di tale operazione.

Obblighi per i Titolari nel contesto dell'uso secondario

Le microimprese e le persone fisiche, compresi i singoli ricercatori, sono gli unici titolari dei dati sanitari generalmente esentati, a meno che gli Stati Membri non estendano loro i seguenti obblighi:

- messa a disposizione di categorie minime di dati: devono rendere disponibili all'HDAB le categorie di Dati richieste, in conformità con un'autorizzazione ai Dati rilasciata, entro un termine massimo di tre mesi dal ricevimento della richiesta, prorogabile di altri tre mesi in casi giustificati;

- descrizione e aggiornamento dei dataset: devono fornire all'HDAB una descrizione del dataset che detengono, verificandone l'accuratezza e l'aggiornamento nel catalogo nazionale almeno una volta all'anno;

- proprietà intellettuale e segreti commerciali: devono informare l'HDAB su eventuali Dati protetti da diritti di proprietà intellettuale o segreti

commerciali, specificando le parti interessate e giustificando la necessità di protezione;

- segnalazione di risultati significativi: se informati da un utente dei dati sanitari di risultati significativi relativi alla salute di una persona fisica (derivanti dall'uso secondario), devono informare la persona interessata o il professionista sanitario che la cura, a meno che non sia stato esercitato il diritto di non essere informati.

E gli utenti di dati sanitari?

Gli utenti dei dati sanitari devono trattare Dati per l'uso secondario solamente sulla base di un'autorizzazione ai dati rilasciata o di una richiesta di Dati approvata. Inoltre:

- non devono fornire l'accesso ai Dati a terzi non inclusi nell'autorizzazione ai Dati;
- non re-identificano e non cercano di re-identificare le persone fisiche a cui si riferiscono i Dati ottenuti;
- rendono pubblici i risultati o gli esiti dell'uso secondario, comprese le informazioni pertinenti per la prestazione di assistenza sanitaria, nonché citano le fonti dei dati, specificando che sono stati ottenuti nel quadro dello spazio europeo dei dati sanitari.

Sanzioni e misure di esecuzione

I titolari e/o gli utenti dei dati sanitari possono essere soggetti a sanzioni amministrative pecuniarie fino a 10.000.000 EUR o al 2% del fatturato mondiale annuo, se superiore, in caso di non conformità quali, ad esempio, rifiuto intenzionale di fornire dati, il mancato rispetto dei termini, nonché uso secondario vietato di Dati. In caso di violazioni ripetute, l'HDAB può escludere (i) il titolare dei dati dalla presentazione di domande di accesso ai Dati per un massimo di cinque anni, pur mantenendo l'obbligo di rendere accessibili i dati (ii) l'utente dei dati sanitari dall'accesso ai Dati nonché revocare autorizzazione rilasciata e/o interrompere trattamento di Dati. Inoltre, violazioni più gravi, quali l'estrazione di dati da ambienti di trattamento sicuro ad opera degli utenti dei dati sanitari nonché re-identificazione e tentativo della re-identificazione di persone fisiche sono sanzionati con importi fino a 20.000.000 EUR o il 4% del fatturato mondiale annuo.

Articolo di Giovanna Fragalà

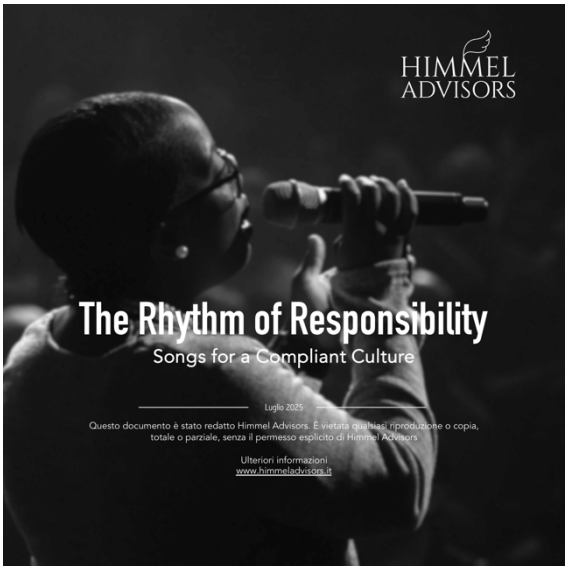
Le immagini incluse in questa newsletter sono soggette a diritti d'autore e sono utilizzate da HIMMEL ADVISORS secondo le licenze Creative Commons©. In particolare, le immagini o i ritratti presenti nelle sezioni Amber e Purple, che ritraggono persone fisiche nonché altri identificativi, sono state utilizzati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

Music & Business sono due mondi separati? Ascolta la nostra Playlist!



In Himmel Advisors abbiamo preparato una playlist speciale che unisce le note alle tematiche più hot di compliance: dal #whistleblowing alle note di avanguardia sulla #cybersecurity, ogni canzone ha il suo messaggio per ispirarci a #migliorare, #innovare e fare sempre del nostro meglio. Swipe, ascolta, lasciati ispirare!

Spotify®

Link Himmel Playlist
(privo di virus)

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