# NEWSLETTER PRIVACY&*COMPLIANCE*

**Formazione & *compliance***

Con le principali novità in materia di protezione dati personali, *cybersecurity*, MOG 231, *Whistleblowing*

## SOMMARIO

# PROVVEDIMENTI IN EUROPA

## POLONIA: SANZIONE AMMINISTRATIVA DI 81.000 EURO PER MANCATA ATTUAZIONE DI MISURE TECNICHE E ORGANIZZATIVE ADEGUATE A GARANTIRE LA SICUREZZA

Il 12 novembre 2024, l'Autorità polacca per la protezione dei dati ha comminato una **sanzione di € 81.000** ad un'azienda per violazioni significative del Regolamento Generale sulla Protezione dei Dati (GDPR).

La sanzione è stata inflitta a seguito di un **attacco *ransomware*** che ha compromesso i dati personali dei clienti e dei dipendenti dell'azienda. L'indagine ha rivelato che l'azienda non aveva implementato misure tecniche e organizzative adeguate per mitigare il rischio di tali incidenti. In particolare, non era stata eseguita un'adeguata analisi dei rischi e il *software* non era aggiornato.

La sanzione è stata comminata per diversi motivi:

| | |
|---|---|
| **mancata implementazione di adeguate misure di sicurezza tecniche e organizzative** | l'azienda non ha implementato misure adeguate sulla base della sua analisi dei rischi; |
| **mancata verifica che il responsabile del trattamento fornisse sufficienti garanzie** | l'azienda non ha verificato che il suo responsabile del trattamento fornisse garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate; |
| **comunicazione errata agli interessati** | l'azienda ha comunicato in modo errato la violazione dei dati agli interessati. |

Inoltre, l'autorità ha rilevato che l'azienda non aveva rispettato il **principio di *accountability*** di cui all'articolo 5, paragrafo 2, del GDPR, non avendo identificato con precisione tutti i rischi o le minacce identificabili in nessuna fase del trattamento dei dati personali.

Questo caso evidenzia l'importanza per le organizzazioni di:

- **effettuare valutazioni approfondite dei rischi**: valutare regolarmente i rischi per i dati personali e implementare misure adeguate per mitigarli;
- **implementare solide misure di sicurezza**: garantire che tutto il *software* sia aggiornato e che siano in atto misure di sicurezza adeguate, come *software,* antivirus e sistemi di rilevamento delle intrusioni.;
- **fornire una formazione completa**: offrire una formazione sulla protezione dei dati regolare e completa a tutti i dipendenti;
- **stabilire chiare procedure di risposta alle violazioni dei dati**: sviluppare e implementare procedure chiare per rispondere alle violazioni dei dati, compresa la notifica all'autorità di controllo e la comunicazione agli interessati;
- **verificare i responsabili del trattamento**: condurre una *due diligence* sui responsabili del trattamento dei dati per garantire che forniscano garanzie sufficienti per l'implementazione di misure tecniche e organizzative adeguate.

Le aziende devono essere consapevoli che il GDPR non è solo una normativa da rispettare, ma anche uno strumento per proteggere i diritti fondamentali degli individui.

L'assenza di misure preventive può avere conseguenze gravi, sia per l'azienda che per i suoi clienti e dipendenti. Pertanto, è fondamentale che le organizzazioni investano nella sicurezza informatica e nella formazione del personale per evitare simili violazioni. Le organizzazioni che non riescono a implementare misure adeguate per proteggere i dati personali rischiano, peraltro, di incorrere in sanzioni significative.

## POLONIA: BANCA SANZIONATA CON € 928.498,06 PER VIOLAZIONE DEL GDPR A SEGUITO DI INVIO ERRATO DI DATI PERSONALI.

Il Presidente dell'Ufficio per la Protezione dei Dati Personali in Polonia ha inflitto una sanzione di **€ 928.498,06** ad un istituto finanziario per violazione dell'articolo 34 del Regolamento Generale sulla Protezione dei Dati (GDPR). Questa decisione segue un incidente in cui i dati personali di alcuni clienti sono stati inviati erroneamente a un altro istituto finanziario il 30 giugno 2022.

L'incidente è stato causato da un **errore di un dipendente** di una società che trattava dati personali per conto dell'istituto finanziario. I documenti, contenenti informazioni di clienti come nomi, date di nascita, numeri di conto bancario e altri dati personali, sono stati **restituiti con la busta aperta**. Nonostante ciò, l'istituto finanziario non ha informato i propri clienti dell'incidente.


L'istituto finanziario ha giustificato la sua decisione sostenendo che i documenti erano stati inviati a un istituto "fidato", anch'esso vincolato al segreto bancario. Tuttavia, l'autorità polacca non ha accettato questa giustificazione. Secondo le Linee Guida 9/2022 del Comitato Europeo per la Protezione dei Dati (EDPB), un destinatario può essere considerato "fidato" solo se esiste una relazione diretta e permanente tra il mittente e il destinatario, e se il mittente conosce le procedure e la storia del destinatario.

L'autorità ha considerato che la possibilità di diffondere una grande quantità di dati rappresentava un **rischio significativo per le persone coinvolte**. Queste persone non sono state informate in modo da poter proteggersi dagli effetti negativi che potevano derivare dalla violazione dei loro dati.

Questo caso sottolinea l'importanza per le organizzazioni di:

- **valutare attentamente il rischio di violazioni dei dati**: considerare non solo chi ha avuto accesso ai dati, ma anche il potenziale impatto sugli interessati;
- **informare tempestivamente gli interessati:** in caso di violazione che possa comportare un rischio elevato per i diritti e le libertà degli interessati, informarli tempestivamente dell'incidente, delle possibili conseguenze e dei rimedi disponibili;
- **non presumere lo status di "destinatario fidato":** valutare attentamente se il destinatario dei dati può essere considerato "fidato" ai sensi delle Linee Guida 9/2022 del Comitato Europeo per la Protezione dei Dati (EDPB);
- **rispettare i diritti degli interessati:** il rispetto di altri segreti legalmente protetti non esenta dall'applicazione del GDPR.

La sanzione inflitta dimostra l'importanza per le organizzazioni di proteggere i dati personali e di informare tempestivamente gli interessati in caso di violazioni. La mancata osservanza di questi obblighi può comportare sanzioni significative e danni alla reputazione.

## NOYB HA PRESENTATO UN RECLAMO CONTRO *BIG TECH* CINESI ACCUSATE DI VIOLARE IL GDPR

Il 16 gennaio 2025, Noyb - l'organizzazione *non profit noyb* (*None Of Your Business*) - fondata dall'attivista per la privacy Max Schrems - ha depositato un reclamo GDPR contro alcune *Big Tech* (*TikTok*, *AliExpress*, *SHEIN*, *Temu*, *WeChat* e *Xiaomi*) per il **trasferimento illegale di dati in Cina**.

L'organizzazione ha rilevato che, mentre quattro di queste società ammettono apertamente di inviare i dati personali degli europei in Cina, le altre due dichiarano di trasferire i dati a "Paesi terzi" non specificati. Dato che nessuna delle aziende ha risposto adeguatamente alle richieste di accesso dei denuncianti, Noyb presume che questo includa la Cina.

Il GDPR consente il trasferimento di dati personali al di fuori dell'UE solo a condizione che il paese di destinazione garantisca un livello di protezione dei dati equivalente a quello europeo.

Noyb ha presentato sei reclami GDPR in cinque Paesi europei, chiedendo alle autorità di protezione dei dati di ordinare immediatamente la sospensione dei trasferimenti di dati verso la Cina e di imporre sanzioni amministrative alle aziende coinvolte.

# EDPB

## EDPB: DICHIARAZIONE SULLA GARANZIA DELL'ETÀ E *TASK FORCE* SULL'APPLICAZIONE DELL'IA.

Nel mese di febbraio 2025, il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato una **dichiarazione sulla garanzia dell'età**, sottolineando l'importanza di proteggere i minori nell'ambiente digitale.

Questo documento è parte di un impegno più ampio dell'EDPB per garantire che i servizi *online* siano sicuri e rispettosi dei diritti fondamentali, specialmente per i più giovani.

**La Dichiarazione dell'EDPB sulla garanzia dell'età.**

La dichiarazione dell'EDPB ribadisce che **la verifica dell'età** deve essere condotta in modo da bilanciare la necessità di proteggere i minori con il rispetto dei diritti degli utenti. Ciò significa che i fornitori di servizi *online* devono adottare un *framework* di *governance* chiaro, che includa politiche precise per il trattamento dei dati personali.

Questo *framework* deve garantire trasparenza, responsabilità e minimizzazione dei dati, assicurando che solo le informazioni strettamente necessarie vengano raccolte e trattate.

***Task Force*** **sull'applicazione dell'*IA*.**

L'EDPB ha anche creato una *task force* sull'applicazione dell'intelligenza artificiale (*IA*), riconoscendo il ruolo cruciale che le tecnologie *IA* possono svolgere nella verifica dell'età. Questa *task force* si concentra su come utilizzare l'*IA* in modo sicuro e conforme alle normative europee, come il GDPR. L'obiettivo è quello di garantire che l'IA sia utilizzata per migliorare la protezione dei minori senza compromettere i loro diritti fondamentali.

L'EDPB sta lavorando per creare un ambiente digitale sicuro e protetto per i minori, utilizzando tecnologie avanzate come l'IA in modo responsabile. La protezione dei minori *online* è una priorità europea, e l'EDPB gioca un ruolo fondamentale nel garantire che i diritti dei più giovani siano rispettati e protetti.

## GARANTE ITALIANO

## SANZIONE DI OLTRE 890 MILA EURO AD UNA SOCIETÀ DI FORNITURA DI SERVIZI DI LUCE E GAS PER *TELEMARKETING* ILLECITO

Il Garante per la Protezione dei Dati Personali, con provvedimento del 27 novembre 2024 n. 736, ha inflitto ad una società operante nella fornitura di servizi di luce e gas una sanzione di oltre **890mila euro** per trattamento illecito di dati personali finalizzato al *telemarketing*.

La decisione è scaturita a seguito di reclami presentati da utenti che lamentavano la ricezione di chiamate promozionali indesiderate e la mancata risposta alle loro richieste di esercizio dei diritti garantiti dal Regolamento Generale sulla Protezione dei Dati (GDPR).

I reclami presentati al Garante per la protezione dei dati personali evidenziavano come gli utenti avessero ricevuto **numerose telefonate indesiderate** a scopo promozionale da diverse società, subito dopo aver stipulato contratti per la fornitura di energia elettrica e gas con la società.

Gli interessati ritenevano che tali contatti fossero il risultato di una cessione illecita dei loro dati personali a terzi da parte della società fornitrice. In seguito alla segnalazione, gli utenti avevano richiesto alla società l'evidenza documentale dei consensi rilasciati per il trattamento dei propri dati personali.

L'indagine del Garante ha fatto emergere diverse violazioni della normativa in materia di protezione dei dati personali:

- **carenza di *accountability***: la società non ha dimostrato di aver adottato tutte le misure necessarie per evitare le violazioni riscontrate, limitandosi ad attribuire le responsabilità a terzi o a errori dei propri collaboratori e partner commerciali;
- ***telemarketing* senza base giuridica**: la società ha effettuato attività di *telemarketing* e *teleselling* in assenza di un'idonea base giuridica, in violazione degli artt. 5, 6 e 7 del GDPR e dell'art. 130 del Codice per la protezione dei dati personali;
- **inadempimento degli obblighi di formazione e monitoraggio:** la società non ha adempiuto agli obblighi di cui all'art. 2 – *quaterdecies* del Codice per la protezione dei

dati personali, riguardante l'individuazione, la formazione, la direzione e il monitoraggio dei soggetti interni all'organizzazione che trattano dati personali per conto della società;

- **violazione dell'art. 28 del GDPR**: le dichiarazioni relative al mancato riscontro a un'istanza di esercizio dei diritti, attribuito a un errore di un *partner* commerciale, hanno evidenziato una violazione degli obblighi gravanti sul titolare ai sensi dell'art. 28 del GDPR (*culpa in eligendo* e *culpa in vigilando*).

**Le Contestazioni del Garante**


Alla luce delle violazioni accertate, il Garante ha contestato alla società le seguenti violazioni:

- violazione degli artt. 5, 6, 7 e 24 del GDPR, nonché dell'art. 130 del Codice Privacy, per aver effettuato trattamenti di dati personali in contrasto con i **principi di liceità e responsabilizzazione**, in assenza di **un'idonea base giuridica** e mettendo in atto **misure tecniche e organizzative non adeguate** a garantire la conformità del trattamento al GDPR;
- violazione dell'art. 28 del GDPR, per non aver **adeguatamente vigilato** sull'operato dei propri responsabili del trattamento.

**Misure Adottate dalla Società**

In relazione alla contestata violazione dell'art. 28 del Regolamento, la società ha dichiarato di aver adottato le seguenti misure:

- procedura di accreditamento dei fornitori;
- utilizzo di *checklist* di *cybersecurity* per le verifiche ex artt. 24, 25, 28 e 32 GDPR sottoposte ai fornitori in fase di ingaggio e nel corso del rapporto;
- verifica dei contratti di servizi con i propri fornitori anche con focus privacy, accertando la necessità o meno di concludere un data processing agreement e definendo correttamente i ruoli privacy tra le parti e adeguate clausole di *audit*;

- impiego di un modello di contratto per il trattamento dei dati personali, contenente istruzioni specifiche anche rispetto alle misure tecnico organizzative che il responsabile del trattamento deve garantire;
- *training* del personale anche sul processo di contrattualizzazione che prevede l'accettazione del DPA, con le annesse misure di sicurezza, prima della contrattualizzazione del partner.

Il Garante Privacy, in precedenza, aveva già sanzionato diverse società per il trattamento illecito di dati personali a fini di *telemarketing*. Tra queste, una società fornitrice di luce e gas ha ricevuto una sanzione di **678.897 euro**. In un altro caso, due gestori di energia, sono stati sanzionati per **100.000 euro ciascuno** per aver effettuato telefonate promozionali senza il consenso degli interessati, contattando anche utenti iscritti al registro pubblico delle opposizioni (servizio pubblico gratuito che consente ai cittadini di opporsi alla ricezione di chiamate e materiale pubblicitario indesiderati).

## *TELEMARKETING: WIND TRE* SANZIONATA PER 347.520 EURO

Il Garante per la protezione dei dati personali, con Provvedimento del 12 dicembre 2024, ha imposto a *Wind Tre* S.p.A. una **sanzione di 347.520 euro** per il trattamento illecito di dati personali a fini promozionali e per la mancata adozione di misure tecniche e organizzative adeguate per proteggere la privacy dei clienti sul proprio sito *web*.

Il provvedimento è scaturito da un'istruttoria avviata dopo numerose segnalazioni di utenti che avevano **ricevuto telefonate promozionali indesiderate** e da un reclamo di un cliente che aveva visualizzato i dati personali di un altro utente nella propria area riservata.

Le indagini del Garante hanno rivelato che *Wind Tre* si era avvalsa di *partner* commerciali che utilizzavano liste di contatti raccolti in modo illecito.

Queste liste erano spesso formate da soggetti extra-UE senza garanzie adeguate, i consensi non erano sufficientemente documentati, e i tempi di conservazione dei dati erano troppo lunghi o addirittura non specificati.

Inoltre, il Garante ha accertato che le **misure tecniche e organizzative relative alla registrazione all'area riservata dei clienti erano inadeguate** e che *Wind Tre* non aveva notificato all'Autorità la violazione dei dati personali dei clienti.

Nel determinare l'importo della sanzione, il Garante ha considerato la collaborazione offerta da *Wind Tre*, le categorie di dati coinvolti (dati comuni) e le misure di sicurezza avanzate che la società aveva iniziato a implementare prima dell'istruttoria, in vista dell'adesione al Codice di condotta per il *telemarketing* e *teleselling*.

In passato, *Wind Tre* era già stata sanzionata per violazioni simili, per un importo di 600.000 euro per l'uso illecito dei dati dei clienti a fini promozionali.

## SANZIONE DI 70MILA EURO AD UNA SOCIETÀ DI RIABILITAZIONE CREDITIZIA PER VIOLAZIONI DELLE NORMATIVE SULLA PROTEZIONE DEI DATI


Il Garante per la protezione dei dati personali, con Provvedimento del 19 dicembre 2024, ha ribadito un principio fondamentale nella gestione dei dati personali: il **ruolo** di Responsabile della Protezione dei Dati (RDP o **DPO**) è **incompatibile** con quello di **rappresentante legale** di una società.

Questa posizione è stata confermata a seguito di una segnalazione della Banca d'Italia, che ha portato alla **sanzione** di una società di riabilitazione creditizia per numerose violazioni delle normative sulla protezione dei dati.

La società in questione, specializzata nella cancellazione delle segnalazioni nelle centrali creditizie, deteneva un *database* con i dati di oltre 70.000 persone.

Queste informazioni erano state raccolte da diverse aziende legate al legale rappresentante della società nel corso degli anni. Tuttavia, la società aveva **designato il proprio rappresentante legale come DPO** senza comunicarlo all'Autorità, ignorando l'incompatibilità tra i due ruoli.

L'istruttoria, condotta con la collaborazione del nucleo speciale della Guardia di Finanza, ha rivelato numerose violazioni del GDPR.

Tra queste, si segnalano:

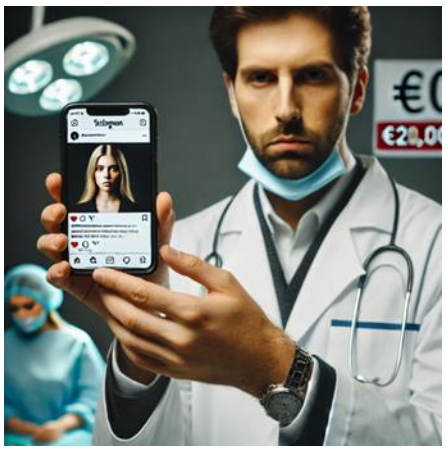
- **mancanza di tracciabilità dei dati**: nessuna funzionalità del sistema informativo consentiva di identificare quale società avesse raccolto i dati personali per ciascun cliente;
- **conservazione indifferenziata**: i dati erano conservati senza distinzione e senza fornire adeguata informazione agli interessati sui passaggi societari;
- **mancata cancellazione dei dati**: la società non cancellava i dati non più necessari dopo la cessazione dei rapporti contrattuali e non aveva definito tempistiche precise per la conservazione;
- **trattamenti non regolamentati**: alcuni trattamenti erano effettuati da soggetti terzi senza un contratto che disciplinasse i rapporti.

Il Garante ha sanzionato la società **per 70.000 euro**, considerando la gravità e la durata delle violazioni, nonché la condotta poco collaborativa.

Inoltre, sono state prescritte misure correttive per risolvere le inadempienze riscontrate.

## CHIRURGO SANZIONATO CON 20.000 EURO PER AVER PUBBLICATO FOTO DI UNA PAZIENTE SU INSTAGRAM SENZA CONSENSO.

Il Garante per la protezione dei dati personali ha inflitto una **sanzione di 20.000 euro** a un



chirurgo per **aver pubblicato sul proprio profilo *Instagram* le foto di una paziente** prima e dopo un intervento di *lifting* del volto, **senza aver ottenuto il consenso alla diffusione delle immagini.**

La decisione è stata presa in seguito al reclamo della paziente, che ha lamentato la pubblicazione di foto che la ritraevano in modo riconoscibile durante l'operazione sul profilo *social* del medico.

La paziente si è rivolta al Garante tramite il suo legale, denunciando la diffusione non autorizzata di immagini del suo volto, scattate durante un intervento di "*lifting cervico medio-facciale con blefaroplastica superiore e inferiore*". Le foto, che mostravano la paziente prima

(con cuffia operatoria) e dopo l'intervento, erano state pubblicate sulla pagina *Instagram* del dottore, con il logo del medico ben visibile.

Durante l'indagine, il chirurgo ha cercato di giustificarsi, sostenendo che le immagini fossero state scattate per uso interno e che la pubblicazione fosse dovuta a un equivoco legato alla gestione dei consensi tra i diversi professionisti coinvolti nell'intervento.

In particolare, ha affermato che la paziente aveva firmato i consensi informati della struttura e di un altro medico, ma che tali consensi erano carenti del consenso specifico alla pubblicazione delle foto.

Il medico ha inoltre aggiunto di aver chiesto alla sua segretaria di rimuovere le foto una volta venuto a conoscenza del problema.

Il Garante ha ritenuto insufficienti le giustificazioni del chirurgo, sottolineando che la pubblicazione di dati sanitari della paziente era avvenuta al di fuori delle finalità di cura e in violazione della normativa sulla privacy.

L'Autorità ha evidenziato che il trattamento dei dati personali della paziente è risultato illecito, in quanto posto in essere al di fuori delle finalità di cura per le quali il medico era legittimato al trattamento e in violazione dei principi di base di cui agli artt. 5 e 9 del Regolamento nonché dell'art. 2-septies, comma 8 del Codice.

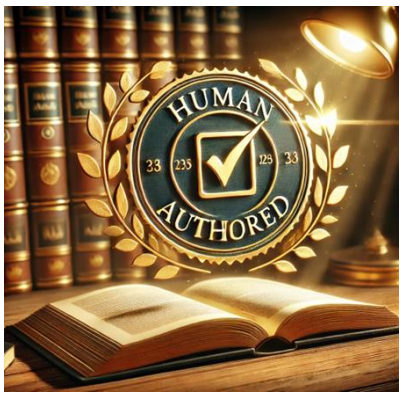
Nel determinare l'ammontare della sanzione, il Garante ha considerato la natura particolarmente sensibile dei dati personali diffusi (dati relativi alla salute) e il contesto in cui è avvenuta la violazione.

In particolare, l'Autorità ha tenuto conto dell'elevata aspettativa di confidenzialità e riservatezza della paziente, data la natura del rapporto professionale e fiduciario con il medico. È stato inoltre valutato che il Garante ha preso conoscenza dell'evento a seguito della ricezione di un reclamo della paziente.

Per questi motivi, il Garante ha ritenuto che il livello di gravità della violazione commessa fosse alto e ha inflitto una sanzione pecuniaria di **20.000 euro**.

## INTELLIGENZA ARTIFICIALE

### AUTORI UMANI CONTRO IA: NASCE IL "BOLLINO" CHE CERTIFICA LIBRI SCRITTI DA AUTORI UMANI




La *Authors Guild*, la più antica e grande organizzazione di scrittori in America, ha lanciato una certificazione denominata "*Human Authored*" per distinguere **i libri scritti da autori umani** da quelli generati da *software* **di intelligenza artificiale**.

La certificazione si presenta come un "bollino" da apporre sulla copertina del libro e sul materiale promozionale, ottenibile tramite una piattaforma *online*.

Inizialmente, questa certificazione sarebbe disponibile solo per i membri della US *Authors Guild*, ma l'associazione prevede di estendere l'iniziativa anche ai non iscritti.

L'obiettivo è quello di offrire ai lettori maggiore trasparenza sull'autenticità dell'opera. Questo permette agli autori di distinguere le proprie opere dalla crescente quantità di contenuti generati artificialmente presenti sul mercato.

La *Authors Guild* ha introdotto anche una clausola nel suo contratto di riferimento per i libri commerciali, al fine di impedire l'uso dei testi per addestrare tecnologie di intelligenza artificiale. Tale clausola vieta espressamente l'utilizzo delle opere per addestrare l'IA generativa, riservando all'autore i diritti di licenza per la formazione generativa dell'IA e lo sviluppo di modelli linguistici di *machine learning*.

## NORMATIVA

## GUIDA ACN PER LA REGISTRAZIONE AL PORTALE DEL PUNTO DI CONTATTO

La Direttiva (UE) 2022/2555 c.d. **NIS 2** è stata recepita nell'ordinamento italiano con il **decreto legislativo 4 settembre 2024, n. 138**, entrato in vigore il 16 ottobre 2024, di seguito "decreto NIS".

Al fine di favorire e semplificare gli adempimenti che i soggetti che rientrano nel suo ambito di applicazione dovranno porre in essere, l'Agenzia per la cybersicurezza nazionale, **ACN**, ha realizzato la "**Piattaforma per la gestione dei flussi di comunicazione tra ACN e i soggetti NIS e gli adempimenti previsti dalla disciplina NIS**" e rilasciato il Manuale per l'utente.

La registrazione sulla piattaforma NIS è un obbligo che i soggetti che rientrano nell'ambito di applicazione del decreto NIS sono tenuti a rispettare.

Essa è funzionale a consentire ad ACN di censire i soggetti operanti nei settori vigilati, anche al fine di fornire supporto in fase di implementazione degli obblighi.

**Il Punto di contatto**

il "Punto di contatto" è la persona fisica designata dal soggetto NIS per curare l'attuazione delle disposizioni del decreto NIS in nome e per conto del soggetto stesso.

Le funzioni del Punto di contatto possono essere svolte dal **rappresentante legale** del soggetto NIS, da uno dei **procuratori generali** del soggetto NIS o da un **dipendente** del soggetto NIS.

In tale ultimo caso, il dipendente deve essere in possesso di un titolo giuridico che ne giustifichi i poteri ovvero può essere delegato mediante il conferimento di una **delega ad hoc.**

In ogni caso, il Punto di contatto può avvalersi anche di personale esterno al soggetto NIS, quale supporto nell'esercizio delle proprie funzioni.

**Il manuale per l'utente**

Il Manuale per l'utente, realizzato dalla divisione NIS e discipline unionali del servizio regolazione, reca le indicazioni esplicative delle varie fasi in cui si articola il processo di registrazione.

Il **28 febbraio** è scaduto il termine per la registrazione sulla piattaforma ACN dei soggetti che rientrano nell'ambito di applicazione della disciplina NIS.
Tuttavia, chi non si è ancora registrato ma ha già completato il primo step, quello di censimento, potrà terminare la registrazione anche oltre il 28 febbraio. Avrà ancora dieci giorni per farlo, **fino al prossimo 10 marzo.**
ACN esprime l'auspicio che i soggetti che ritengono di essere in ambito NIS sfruttino questa ulteriore possibilità per registrarsi.

**L'applicazione del decreto NIS ai soggetti operanti in settori critici**

L'operatività del decreto legislativo n. 138/2024 ("decreto NIS") nei confronti delle entità attive nei settori a elevata criticità e in altri ambiti strategici dipende strettamente dal superamento di specifiche **soglie dimensionali.** Tali parametri sono definiti in conformità con le disposizioni della Raccomandazione 2003/361/CE.

Tuttavia, l'interpretazione dei criteri dimensionali **ha dato origine a un vivace confronto** tra giuristi e consulenti specializzati, dovuto a una possibile discrepanza tra l'interpretazione testuale della normativa e l'approccio seguito dall'Agenzia per la Cybersicurezza Nazionale (ACN). In particolare, sebbene il dettato normativo sembri indicare che sia necessario il **superamento simultaneo dei limiti dimensionali** fissati a livello europeo e nazionale, l'ACN ha adottato un'interpretazione che potrebbe portare a **conclusioni differenti,** con conseguenze dirette sulla qualificazione delle imprese soggette a tale disciplina.

**I criteri dimensionali rilevanti per l'applicazione del decreto NIS**

Il decreto NIS si applica ai soggetti che operano nei cosiddetti **"settori ad alta criticità"** e negli **"altri settori critici",** a condizione che **superino i parametri identificativi delle piccole**

**imprese,** così come delineati dall'articolo 2, paragrafo 2, dell'allegato alla Raccomandazione 2003/361/CE (di seguito "Raccomandazione").

Tale principio è sancito dall'articolo 3, comma 2, del decreto NIS, il quale stabilisce che "*il presente decreto si applica ai soggetti di cui agli allegati I e II, che superano i massimali per le piccole imprese ai sensi dell'articolo 2, paragrafo 2, dell'allegato alla Raccomandazione*".

Secondo la normativa richiamata, una **piccola impresa è definita** come un'entità che impiega **meno di 50 dipendenti** e che presenta un **fatturato annuo** o un bilancio totale **non superiori a 10 milioni di euro.**

Un'interpretazione letterale dell'articolo 3 del decreto NIS porta quindi a ritenere che l'identificazione dei soggetti sottoposti alla disciplina debba basarsi su **entrambi i criteri dimensionali: il numero di dipendenti** e almeno uno tra i **parametri finanziari (fatturato o bilancio).** Di conseguenza, affinché un'impresa rientri nell'ambito di applicazione del decreto, è sufficiente che **uno solo di questi indicatori ecceda i limiti previsti.**

## SENTENZE

### CORTE DI GIUSTIZIA UE: PROTEZIONE DEI DATI PERSONALI NEL RAPPORTO DI LAVORO

La Corte di Giustizia dell'Unione Europea ha chiarito che qualsiasi trattamento di dati personali nell'ambito del rapporto di lavoro deve rispettare integralmente le disposizioni del Regolamento Generale sulla Protezione dei Dati (GDPR).

Questa posizione è stata ribadita nella sentenza del 19 dicembre 2024 (C-65/23), che ha sottolineato l'importanza della conformità ai principi fondamentali del GDPR anche nei contratti collettivi nazionali di lavoro.

La controversia alla base della sentenza riguardava un impiegato di una società tedesca, che sosteneva di aver subito danni a causa del trattamento dei suoi dati personali effettuato dalla società. La Società aveva utilizzato un *software* per finalità contabili e successivamente aveva introdotto un altro *software*, trasferendo i dati dei dipendenti su un *server* situato negli Stati Uniti.

La Corte di Giustizia ha stabilito che le disposizioni nazionali relative al trattamento dei dati personali nei rapporti di lavoro devono rispettare i requisiti del GDPR, in particolare quelli previsti dagli articoli 5 e 6, che disciplinano i **principi di liceità** e le condizioni per un **trattamento legittimo**. Inoltre, ha precisato che i giudici nazionali possono esercitare un controllo completo sulle decisioni relative alla necessità del trattamento dei dati, anche se queste sono previste da contratti collettivi.

I **contratti collettivi nazionali di lavoro** possono prevedere norme specifiche per il trattamento dei **dati personali dei dipendenti**, ma queste devono essere **conformi ai principi del GDPR**.

Qualora un contratto collettivo violi le norme sulla protezione dei dati, **il giudice nazionale è tenuto a disapplicarlo**.

Ciò significa che le parti coinvolte nei contratti collettivi devono assicurarsi che le disposizioni relative al trattamento dei dati siano coerenti con il GDPR, altrimenti **rischiano di essere invalidate.**

## TAR LOMBARDIA: PROTEZIONE DEI DATI PERSONALI E OSCURAMENTO DELLE GENERALITÀ

Il Tribunale Amministrativo Regionale (TAR) di Milano, sezione terza, con la sentenza del 16 dicembre 2024, n. 3701, ha ribadito l'importanza della protezione dei dati personali e della tutela della dignità degli individui. In questo caso, il TAR ha disposto **l'oscuramento delle generalità del ricorrente** per salvaguardare i suoi diritti e la sua dignità, in conformità con il Decreto Legislativo 30 giugno 2003, n. 196 e il Regolamento (UE) 2016/679 (GDPR).

L'oscuramento delle generalità è una misura che può essere adottata per proteggere la privacy degli individui, specialmente in situazioni in cui la divulgazione dei loro dati potrebbe comportare rischi per la loro dignità o sicurezza. Questa pratica è coerente con i principi di minimizzazione dei dati e di necessità del trattamento, sanciti dal GDPR.

La sentenza del TAR Lombardia sottolinea l'importanza di bilanciare il diritto di accesso agli atti amministrativi con la necessità di proteggere i dati personali. L'oscuramento delle generalità rappresenta uno strumento efficace per garantire che le informazioni sensibili non vengano divulgate indebitamente, tutelando così i diritti fondamentali degli individui.

Il caso riguardava l'emersione del lavoro irregolare di un cittadino straniero. La Prefettura competente aveva inizialmente preso una decisione che non soddisfaceva le aspettative del ricorrente, portando quest'ultimo a presentare un ricorso dinanzi al TAR Lombardia. Successivamente, l'amministrazione procedente aveva riesaminato l'istanza e l'aveva accolta positivamente, determinando la cessata materia del contendere. L'oscuramento delle generalità è una misura che contribuisce a rafforzare la fiducia degli individui nelle istituzioni e a promuovere una cultura della privacy sempre più attenta e rispettosa dei diritti fondamentali.

## *CYBERSECURITY*

### SAI COSA COS'ÈLO *SPOOFING*?

Lo "***spoofing***", termine inglese traducibile con "**inganno**" o "**falsificazione**", è una tecnica utilizzata per impersonare un'altra entità nelle comunicazioni *online,* manipolando i numeri telefonici per ingannare e mascherare l'identità.

Lo *spoofing* si verifica quando un chiamante invia deliberatamente **informazioni false** per presentarsi con l'ID di un altro utente. I truffatori alterano il numero di telefono visualizzato sullo schermo del destinatario durante una chiamata, **facendo sembrare che provenga** da un'entità affidabile come una banca o un'azienda.

La maggior parte dello *spoofing* si effettua utilizzando un servizio VoIP (*Voice over Internet Protocol*) o un telefono IP con VoIP per trasmettere le chiamate su internet.

**Tecniche di *Spoofing***

Esistono diverse tecniche di *spoofing*, tra cui:

- ***caller ID spoofing***: falsificazione dell'identità del chiamante visualizzata sul *display* del telefono. I truffatori possono fingere di chiamare da un istituto bancario o da un ente di beneficenza per spingere gli interlocutori a trasferire denaro o comunicare dati personali;

- ***orange boxing***: utilizzo di un *software* che genera un segnale audio associato alla linea telefonica durante la chiamata, inducendo il ricevente a pensare che ci sia una chiamata in arrivo da un numero contraffatto;
- ***CLI Spoofing***: accorgimenti per identificare una chiamata generata tramite reti VoIP con un numero telefonico falso.

Gli obiettivi principali dello *spoofing* includono:

- ***furto di informazioni sensibili***: indurre la vittima a rivelare informazioni personali o finanziarie;
- **truffe finanziarie:** spingere gli interlocutori a trasferire denaro tramite raggiri telefonici;
- **attacchi informatici:** manipolare i dati all'interno di una rete per ottenere accessi o trasmettere file dannosi;
- ***telemarketing* aggressivo:** falsificare i numeri di telefono per effettuare chiamate promozionali indesiderate.

**Come difendersi dallo *spoofing***

- **non fidarsi dell'ID chiamante**: verificare sempre l'identità del chiamante, soprattutto se richiede informazioni personali o finanziarie;
- **non fornire informazioni personali**: non comunicare dati sensibili al telefono a meno che non si sia certi dell'identità del chiamante;
- **contattare direttamente l'ente**: in caso di dubbi, contattare direttamente l'istituto bancario o l'azienda utilizzando i canali ufficiali;
- **segnalare le chiamate sospette**: segnalare le chiamate di *spoofing* alle autorità competenti e al proprio operatore telefonico.

## SAI COSA FARE QUANDO SEI VITTIMA DI CYBERBULLISMO?

Il fenomeno del **cyberbullismo** rappresenta una delle più insidiose minacce del mondo digitale, colpendo in particolare i minori attraverso atti di molestia, diffamazione, furto d'identità e altre forme di abuso online. La **Legge n. 71 del 29 maggio 2017**, all'articolo 1, comma 2, definisce il *cyberbullismo* come "*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica*". Questa definizione sottolinea la gravità e l'ampiezza del fenomeno.


Il cyberbullismo si distingue per alcune caratteristiche peculiari:

- **pervasività**: le molestie possono avvenire in qualsiasi momento e luogo grazie alla tecnologia digitale;
- **anonimato**: spesso il cyberbullo nasconde la propria identità, rendendo difficile individuarlo;

- **volontarietà dell'aggressione**: gli attacchi sono intenzionali, sebbene il cyberbullo possa non percepire appieno le conseguenze delle sue azioni;
- **ampia diffusione**: i contenuti offensivi possono rapidamente raggiungere un vasto pubblico.

**Tipologie di cyberbullismo**

Esistono diverse modalità attraverso cui il cyberbullismo può manifestarsi:

- ***Flaming***: insulti e offese pubblicati sui social media o forum *online*;
- ***Impersonation***: furto d'identità per screditare la vittima;
- ***Trickery***: inganno per ottenere informazioni private e diffonderle online;
- ***Cyberstalking***: minacce ripetute per intimidire la vittima;
- ***Doxxing***: pubblicazione non autorizzata di dati personali sensibili;
- ***Denigration***: diffusione di pettegolezzi e insulti per danneggiare la reputazione;
- ***Cyberbashing***: registrazione e condivisione di aggressioni fisiche;
- ***Harassment***: molestie reiterate online.

**Cosa fare in caso di cyberbullismo**

Se sei vittima di cyberbullismo, puoi intraprendere diverse azioni per difenderti:

1. **segnalazione al gestore della piattaforma**: puoi richiedere la rimozione immediata dei contenuti offensivi al gestore del sito o del social network. Se sei minore di 14 anni, i tuoi genitori possono effettuare la richiesta per te.
2. **reclamo al Garante della Privacy**: se il gestore non interviene entro **48 ore**, è possibile presentare un reclamo al **Garante per la protezione dei dati personali**, che deve rispondere entro le successive **48 ore**.

3. **tutela scolastica**: ogni istituto scolastico è tenuto a promuovere l'educazione all'uso consapevole di internet e a individuare un **referente per il cyberbullismo**.
4. **azioni legali**: in caso di diffamazione, ingiuria, minacce o trattamento illecito di dati personali, è possibile **sporgere querela o denuncia** alle autorità competenti.

## ATTACCO *RANSOMWARE* A MARPOSS: ECCO COSA È SUCCESSO E COME DIFENDERSI

Nella notte di domenica 26 gennaio 2025, Marposs, azienda *leader* nel settore delle **apparecchiature di misurazione di precisione** con sede a Bentivoglio (Bologna), è stata colpita da un attacco informatico di tipo *cryptolocker* che ha compromesso alcuni *server* del sistema. Questo tipo di attacco, sempre più frequente, rientra nella categoria dei *ransomware*, in cui i criminali cifrano i dati presenti nei sistemi colpiti tramite un *virus*, richiedendo poi un riscatto per la loro decriptazione.

A seguito dell'attacco, la società ha immediatamente attivato una *task force* di esperti di *cybersecurity*, supportati da specialisti esterni, per ripristinare i sistemi compromessi e garantire la continuità operativa. L'azienda ha anche denunciato l'accaduto alla polizia postale, che ha avviato le indagini per risalire ai responsabili. Per tutelare i lavoratori e l'azienda, è stata richiesta l'attivazione della cassa integrazione ordinaria fino al 7 febbraio, applicata in modo parziale e flessibile ai comparti maggiormente colpiti.

***

L'attacco di tipo *cryptolocker* consiste nella cifratura dei dati della vittima tramite un virus informatico, con la successiva richiesta di un riscatto per "liberarli".

Il fenomeno dei *ransomware* è in forte crescita. A livello globale, nel secondo quadrimestre del 2024, sono state monitorate **1.747 rivendicazioni *ransomware***. In Italia, nello stesso periodo, si sono registrati **58 attacchi *ransomware***, con un incremento di quasi il 100% rispetto al 2022.

Per proteggere le aziende da attacchi *ransomware*, è fondamentale adottare una serie di strategie:

1. **formazione del personale**: sensibilizzare i dipendenti sui rischi derivanti da email e allegati sospetti;

2. **aggiornamenti *software***: mantenere aggiornati i sistemi operativi e i *software* per correggere le vulnerabilità;
3. ***backup* dei dati**: effettuare regolarmente copie di sicurezza dei dati per poterli ripristinare in caso di attacco;
4. **soluzioni di sicurezza**: implementare soluzioni di sicurezza avanzate, come *firewall*, antivirus e sistemi di rilevamento delle intrusioni;
5. ***incident response plan:*** sviluppare un piano di risposta agli incidenti per gestire rapidamente e efficacemente eventuali attacchi.

La crescente diffusione dei *ransomware* richiede un aumento degli investimenti in *cybersecurity* e una maggiore attenzione al fattore umano.

Adottare misure di protezione adeguate e sviluppare un piano di risposta agli incidenti sono passi fondamentali per proteggere le aziende da queste minacce.

## I RISCHI DEL *QR CODE*

Negli ultimi anni, i *QR code* sono diventati sempre più popolari, venendo utilizzati in diversi contesti, dalle transazioni finanziarie ai menu dei ristoranti. Tuttavia, dietro alla loro comodità si nascondono alcuni rischi per la nostra privacy.

**Cos'è un QR Code?**

Un *QR code* (*quick response code*) è un tipo di codice a barre bidimensionale che può essere letto da *smartphone* e altri dispositivi mobili. Questi codici possono contenere una vasta gamma di informazioni, come URL, numeri di telefono, messaggi di testo e molto altro.

**Come funzionano i *QR code*?**

Quando si scansiona un *QR code* con uno *smartphone*, il dispositivo decifra le informazioni contenute nel codice e le esegue in base al loro tipo. Ad esempio, se il codice contiene un URL, il *browser* del telefono si aprirà automaticamente su quel sito *web*.

**Rischi**

I *QR code* possono rappresentare un rischio per la nostra privacy per diversi motivi:

1. **accesso a siti web non sicuri**: se un *QR code* contiene un URL, potrebbe indirizzare l'utente a un sito *web* non sicuro o addirittura a una truffa. Questo potrebbe esporre l'utente a *malware* o *phishing*, mettendo a rischio i suoi dati personali;
2. **raccolta di dati personali**: alcuni *QR code* potrebbero essere utilizzati per raccogliere informazioni personali senza il consenso dell'utente. Ad esempio, un codice potrebbe richiedere l'accesso alla posizione o ad altre informazioni sensibili;
3. **tracciamento degli utenti**: i *QR code* possono essere utilizzati per tracciare le attività degli utenti. Ad esempio, un'azienda potrebbe utilizzare i *QR code* per monitorare chi visita il suo sito *web* o chi interagisce con i suoi prodotti;
4. ***phishing* e truffe**: i QR code possono essere facilmente contraffatti e utilizzati per ingannare le persone. Un truffatore potrebbe creare un *QR code* che sembra legittimo ma che, una volta scansionato, richiede informazioni sensibili o installa *malware* sul dispositivo.

**Come proteggersi**

Per evitare questi rischi, è importante adottare alcune precauzioni:

- **verifica l'origine**: prima di scansionare un *QR code*, assicurarsi che provenga da una fonte affidabile;
- **app sicure**: utilizzare *app* di lettura *QR code* che offrono funzionalità di sicurezza, come l'avviso di potenziali minacce;
- **non condividere informazioni sensibili**: non inserire mai informazioni personali sensibili quando richiesto da un *QR code*;
- **aggiornare il dispositivo**: sssicurarsi che il dispositivo sia aggiornato con le ultime *patch* di sicurezza.

I *QR code* possono essere strumenti molto utili, ma è fondamentale essere consapevoli dei potenziali rischi per la privacy.

## IL RUOLO DELL'ODV 231 NELLA DIRETTIVA NIS 2: COMPITI E RESPONSABILITÀ.

La Direttiva NIS 2 rappresenta un importante passo avanti nella protezione della **sicurezza informatica** delle aziende, soprattutto per quelle che operano in settori essenziali e critici. In questo contesto, l'Organismo di Vigilanza (OdV) 231 assume un ruolo cruciale nell'assicurare che le imprese rispettino i nuovi obblighi normativi in materia di *cybersecurity*.

**1. Ruolo dell'OdV 231 nell'applicazione della Direttiva NIS 2**

L'OdV 231 è responsabile della vigilanza sull'effettiva attuazione delle misure di sicurezza cibernetica previste dalla NIS 2, garantendo che queste siano integrate nel Modello di Organizzazione e Gestione (MOG 231). Ciò include la verifica che le aziende classificate come essenziali o importanti rispettino i nuovi obblighi normativi in materia di *cybersecurity*, come la registrazione obbligatoria presso l'Agenzia per la Cybersicurezza Nazionale (ACN) e la nomina del punto di contatto.

**2. Mancata applicazione della NIS 2 e responsabilità ex D.Lgs. 231/2001**

La mancata adozione di adeguate misure di sicurezza informatica da parte delle aziende che rientrano nei settori critici individuati dalla NIS 2 può configurarsi come una **colpa organizzativa**, portando alla responsabilità amministrativa dell'ente. Questo è particolarmente rilevante in caso di attacchi *cyber* con conseguenze significative, poiché il Modello 231 può essere utilizzato come causa esimente solo se adeguatamente implementato e aggiornato.

**3. Misure organizzative per la conformità alla NIS 2**

Per garantire la conformità alla NIS 2, l'OdV deve vigilare affinché nel MOG 231 siano integrate le seguenti misure:

- procedure di gestione del rischio *cyber*: *risk assessment*, gestione incidenti;

- misure di sicurezza per i sistemi IT e OT: *firewall*, crittografia, autenticazione Multi-Fattore (MFA);
- piani di risposta e *recovery* in caso di *cyberattacco*;
- formazione obbligatoria per dipendenti e dirigenti sulla *cybersecurity*.

**4. Organizzazione dell'OdV per monitorare la *compliance* alla NIS 2**

L'OdV deve aggiornare il protocollo di vigilanza includendo:

- verifiche periodiche sulla conformità alle misure di sicurezza informatica;
- *audit* sui processi di gestione degli incidenti cyber;
- analisi delle segnalazioni e dei report interni su eventi di sicurezza;
- coordinamento con il DPO, il CISO e l'IT *Security Manager*.

**5. Rischi per un'azienda che non si adegua alla NIS 2**

Le aziende che non si adeguano alla NIS 2 rischiano sanzioni fino a 10 milioni di euro o il 2% del fatturato globale annuo. Inoltre, in caso di gravi violazioni, le autorità possono imporre restrizioni operative, sospendere dirigenti responsabili e avviare procedimenti giudiziari, con impatti anche sul Modello 231.

**6. Collaborazione con il CISO**

La collaborazione tra l'OdV e il CISO è fondamentale. Il CISO fornisce dati e *report* sulla sicurezza informatica, mentre l'OdV verifica che le procedure aziendali siano conformi alla normativa. È utile prevedere incontri periodici tra l'OdV e il *team* di *cybersecurity*.

**7. Gestione delle segnalazioni di eventi *cyber***

L'OdV deve garantire che il canale di segnalazione interno preveda anche la possibilità di denunciare minacce o vulnerabilità informatiche. Tutte le segnalazioni devono essere analizzate e gestite in collaborazione con il *team* di sicurezza informatica.

**8. Aggiornamento del codice etico aziendale**

Il codice etico deve includere principi relativi alla *cybersecurity*, protezione dei dati e gestione dei rischi informatici. Il personale deve essere sensibilizzato sulla sicurezza informatica e sulle conseguenze di comportamenti negligenti.

**9. Documenti da analizzare per la compliance alla NIS 2**

L'OdV dovrebbe esaminare:

- *risk assessment* aziendale sui rischi *cyber*;
- *cyber Incident Response Plan*;
- *policy* di sicurezza IT (gestione accessi, *backup*, *encryption*);
- *report* degli *audit* di cybersecurity;
- registri degli incidenti informatici e delle azioni correttive adottate.

**10. Ruolo dell'OdV in caso di incidente informatico**

L'OdV deve verificare che l'azienda abbia seguito le procedure di *incident response* previste dalla normativa e dal MOG 231. Inoltre, deve valutare se la gestione dell'incidente evidenzi eventuali lacune organizzative che richiedono aggiornamenti al modello 231 e ai protocolli di sicurezza.

## *WHISTLEBLOWING*: QUANDO NON È APPLICABILE PER QUESTIONI PERSONALI?

Il *whistleblowing* è la possibilità per un dipendente di segnalare illeciti o irregolarità commesse dall'azienda o dall'organizzazione per cui lavora, garantendo la protezione del segnalante. Questo strumento permette ai dipendenti di segnalare violazioni di normative che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato.

Tuttavia, **l'istituto del *whistleblowing* non è utilizzabile per scopi essenzialmente di carattere personale, contestazioni o rivendicazioni inerenti al rapporto di lavoro nei confronti di superiori.**

Conflitti di questo tipo sono disciplinati da altre normative e procedure.

La normativa di tutela del dipendente che segnala illeciti altrui salvaguarda il segnalante da sanzioni disciplinari o ritorsioni, ma non lo protegge per illeciti che egli stesso abbia commesso.

In altre parole, il *whistleblowing* non può essere utilizzato per lamentele personali o richieste riguardanti la disciplina del rapporto di lavoro o i rapporti con superiori gerarchici o colleghi, poiché tali questioni sono gestite da altre procedure. La segnalazione deve essere fatta nell'interesse dell'integrità della pubblica amministrazione e non per scopi personali.

La **Corte di Cassazione, Sezione Lavoro, con sentenza del 27 gennaio 2025, n. 1880**, ha rigettato la richiesta d'impugnazione presentata da un lavoratore in materia di *whistleblowing*. La giurisprudenza ha chiarito che l'istituto del *whistleblowing* non è applicabile per scopi personali o contestazioni relative al rapporto di lavoro con i superiori.

**A CURA DI AVV. MIRIAM POLINI**

**NOVASTUDIA MILANO**

***NEWSLETTER* NOVASTUDIA MILANO**

Il presente documento è una nota di Studio. Quanto nello stesso riportato non potrà pertanto essere utilizzato o interpretato quale parere legale né utilizzato a base di operazioni straordinarie, né preso a riferimento da un qualsiasi soggetto o dai suoi consulenti legali per qualsiasi scopo che non sia un'analisi generale e sommaria delle questioni in esso affrontate.

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'articolo 13 del Regolamento (UE) 2016/679

La Newsletter di Novastudia MILANO è distribuita a mezzo e-mail - in automatico e gratuitamente - a quanti fanno richiesta di riceverla.

I dati forniti saranno utilizzati con strumenti informatici e telematici al solo fine di fornire il servizio richiesto e, per tale ragione, saranno conservati esclusivamente per il periodo in cui lo stesso sarà attivo.

La base giuridica di tale trattamento è da rinvenirsi nel consenso a ricevere comunicazioni e-mail da parte dello Studio.

Il titolare del trattamento è l'Avv. Nicola Tilli, con Studio in Milano Via Quadronno N. 4 – 20122; e-mail: **info@sltnovastudia.com**; centralino: 02 58315358.

I dati saranno trattati esclusivamente dal personale e dai collaboratori dello Studio o delle imprese espressamente nominate come responsabili del trattamento (ad es. per esigenze di manutenzione tecnologica del sito).

Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti effettuato attraverso questo servizio avvenga in violazione di quanto previsto dal Regolamento hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

**CANCELLAZIONE DEL SERVIZIO**

Per non ricevere più la Newsletter, inoltrare una e-mail a **info@sltnovastudia.com** "Cancella iscrizione". In caso di problemi tecnici, è possibile inviare una segnalazione e-mail a **segreteria@sltnovastudia.com** o telefonando al numero 02.58315358.