PRIVACY DALLA A ALLA Z

PAROLE CHIAVE
PER IMPRESE E PROFESSIONISTI

BE LEGAL STUDIO

BE LEGAL STUDIO

INDICE

Caro lettore e cara lettrice,
grazie per avere dedicato del tempo per scaricare la guida.

Stai per iniziare un percorso per imparare a **orientarti tra le parole chiave della privacy**, spiegate in modo semplice e con esempi concreti, dalla **A di "accesso ai luoghi" alla Z di "zero rischi non esistono"**, per comprendere alcuni aspetti fondamentali nella gestione dei dati personali nel contesto aziendale o professionale.

Abbiamo pensato questo viaggio partendo da casi esaminati dai Garanti per la protezione dei dati personali o da qualche Autorità giudiziaria.
Per ogni lettera dell'alfabeto troverai una **parola chiave**, spiegata in tre brevi parti:

- il **principio**: cosa dobbiamo tenere a mente
- il **caso**: una vicenda reale
- il **provvedimento**: come si è espresso il Garante o il Giudice

Avete già pensato al tema della privacy nella tua realtà lavorativa? La corretta gestione dei dati personali è un diritto fondamentale delle persone e, allo stesso tempo, una responsabilità concreta per chi gestisce dati personali della propria clientela, del personale dipendente, partner o consulenti.

In un mondo sempre più digitale, trattare i dati personali in maniera conforme alla normativa non è solo una questione di compliance per evitare sanzioni, ma significa proteggere il proprio lavoro, aumentare la fiducia e la reputazione, avere cura per un elemento strategico fondamentale nelle strategie ESG di ogni attività.

Con gli strumenti giusti, anche la privacy può diventare un **vantaggio competitivo** concreto per ogni attività e **valore aggiunto per un'identità aziendale o professionale affidabile e virtuosa**.

Buona lettura!
Veronica e Ludovica

agg. 2025

I PROTAGONISTI DELLA PRIVACY

TITOLARE DEL TRATTAMENTO

È la persona fisica o giuridica, l'autorità pubblica o l'ente che determina le finalità e i mezzi del trattamento.
es. il datore di lavoro rispetto ai dati personali del suo personale.
Se sono più di uno, si parla di Contitolari del trattamento

RESPONSABILE DEL TRATTAMENTO

È la persona fisica o giuridica, l'autorità pubblica o l'ente che tratta dati personali per conto del titolare.
es. viene così qualificato il/la consulente del lavoro per il trattamento dei dati del personale delle aziende sue clienti

INTERESSATO

È la persona fisica alla quale si riferiscono i dati personali
es. se un trattamento riguarda il tuo indirizzo, il tuo C.F., la tua mail, l'interessato/a sei tu

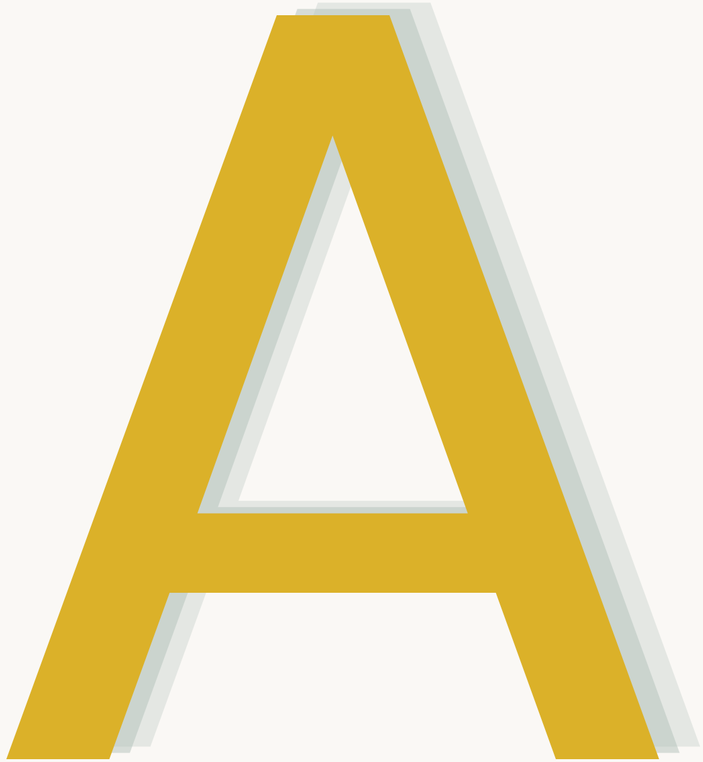
AUTORIZZATO O INCARICATO

È la persona autorizzata al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.
es. il personale dipendente che tratta i dati nell'azienda

RESPONSABILE DELLA PROTEZIONE DEI DATI

È la figura professionale che collabora con il titolare o con il responsabile del trattamento con vari compiti, tra cui fornire consulenza in merito ai loro obblighi, sorvegliare il rispetto delle norme UE, fornire pareri in alcune occasioni, cooperare con l'autorità di controllo.

ACCESSO AI LUOGHI



I sistemi di riconoscimento facciale negli stadi che memorizzano immagini degli spettatori violano le disposizioni sui dati personali e la privacy. Il consenso degli spettatori non può considerarsi libero quando l'alternativa è non poter assistere alla partita. L'obbligo imposto per entrare allo stadio che comporta il trattamento di dati biometrici è illegittimo.

IL CASO

La Liga spagnola aveva installato sistemi di riconoscimento facciale per gestire l'accesso agli stadi che consentivano la memorizzazione delle immagini di tutti gli spettatori, compresi i minori. Il sistema rendeva obbligatorio per i tifosi sottoporsi al riconoscimento facciale come condizione per entrare allo stadio e assistere alle partite.

IL PROVVEDIMENTO

Il Garante privacy spagnolo ha sanzionato la Liga per **1 milione di euro**, stabilendo che l'obbligo imposto agli spettatori violava le disposizioni sul trattamento dei dati personali e la privacy dei tifosi.
La sanzione ha chiarito che il consenso dei tifosi non poteva considerarsi libero, dato che l'unica alternativa sarebbe stata rinunciare a vedere la partita allo stadio.

ACCOUNT

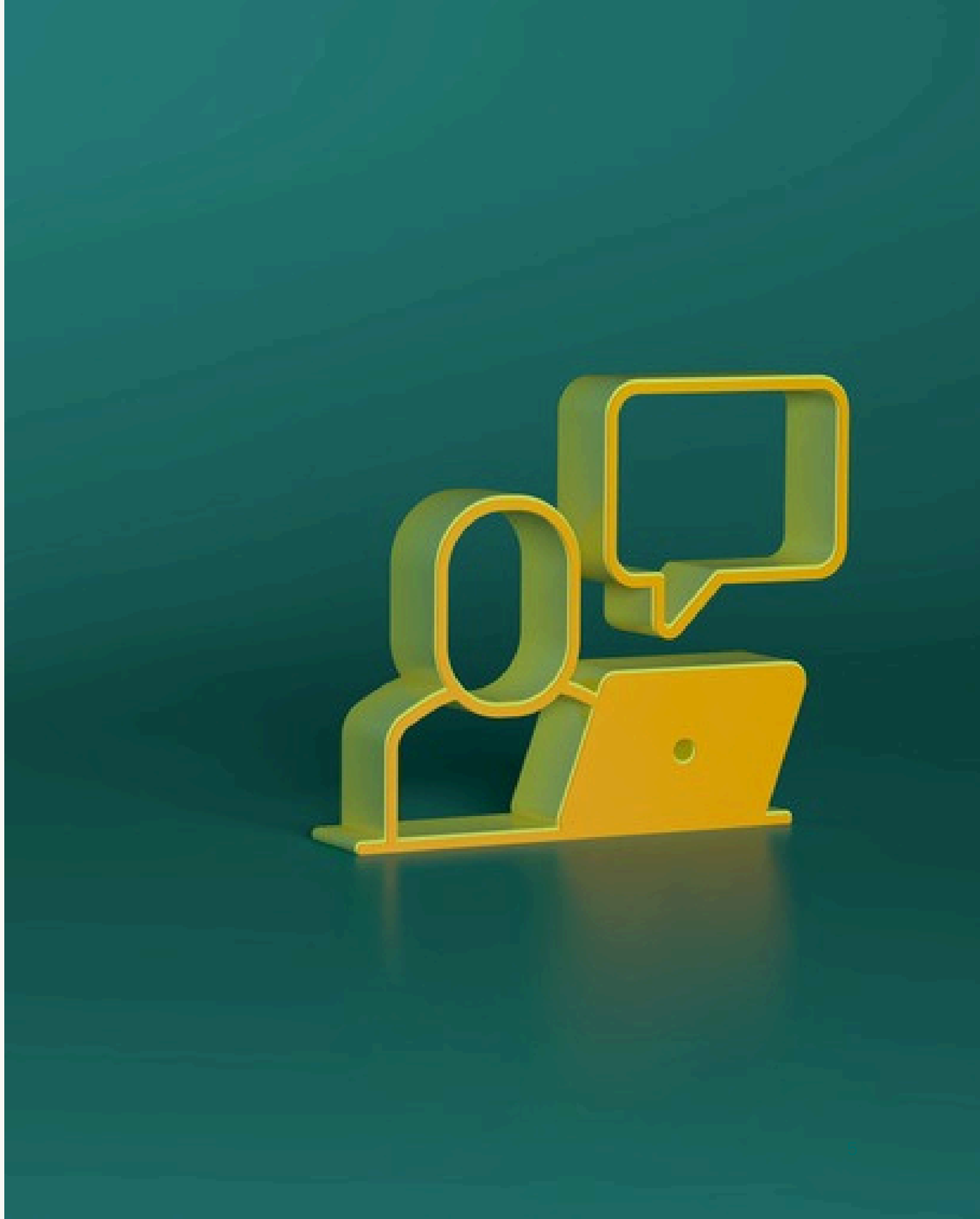
Non è legittimo l'obbligo imposto da alcuni siti di e-commerce di registrarsi anche solo per effettuare un singolo acquisto. I siti non possono obbligare la clientela a creare un account e condividere dati personali per poi utilizzarli per profilazione e invio di newsletter personalizzate. La registrazione forzata per un singolo acquisto viola il principio di minimizzazione dei dati del GDPR.

IL CASO

Un'azienda finlandese di vendite online obbligava la propria clientela a creare un account condividendo vari dati personali (nome, cognome, email, numero di telefono) per poter effettuare anche un singolo acquisto.
L'azienda utilizzava poi questi dati per la profilazione degli utenti e per l'invio di newsletter personalizzate, senza nemmeno precisare il periodo di conservazione dei dati.

IL PROVVEDIMENTO

Il Garante privacy finlandese ha sanzionato l'azienda per **856.000 euro** per violazione del GDPR: la creazione forzata dell'account non era giustificata, mancavano trasparenza e indicazioni sui tempi di conservazione dei dati.



BIOMETRIA

B

I sistemi di intelligenza artificiale per il riconoscimento facciale non sono sempre legittimi. I dati biometrici (caratteristiche fisiche, fisiologiche o comportamentali che consentono l'identificazione univoca come immagini del viso o impronte digitali) sono vietati dall'art. 9 del GDPR salvo specifiche eccezioni. È necessario prestare molta attenzione quando si introduce un sistema di riconoscimento facciale e verificare che il trattamento sia legittimo.

IL CASO

Un'Università italiana aveva adottato un sistema di supervisione "proctoring" per gli esami online che utilizzava il riconoscimento facciale per identificare gli studenti e verificarne il comportamento. Il software catturava immagini video e schermate, identificando e contrassegnando i comportamenti insoliti o sospetti mediante registrazioni e istantanee casuali, permettendo ai docenti di verificare eventuali azioni non consentite.

IL PROVVEDIMENTO

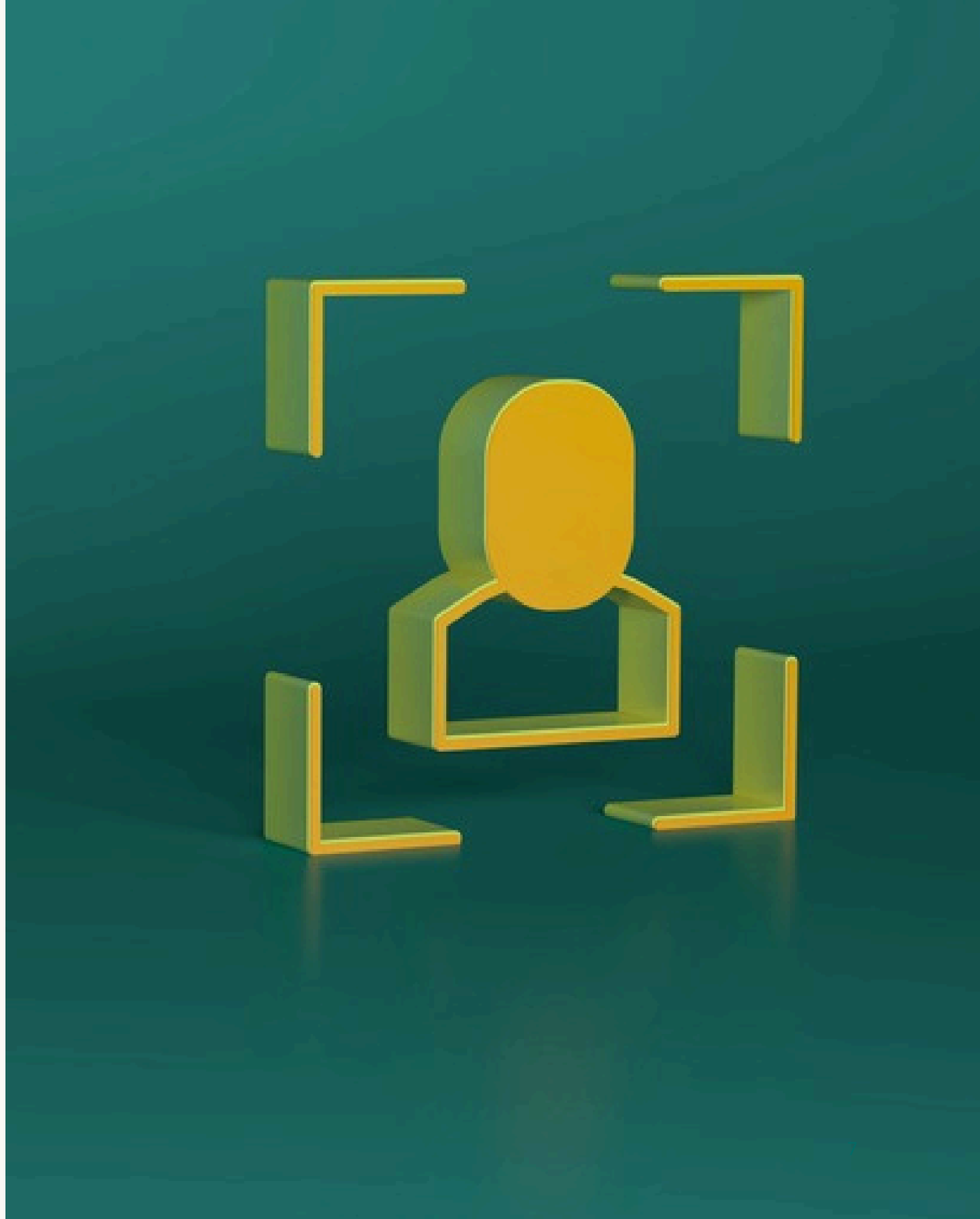
Il Garante privacy ha sanzionato per **200.000 euro** l'Università per il trattamento illegittimo di dati biometrici. La Corte di Cassazione ha confermato la sanzione, ritenendo il sistema vietato dall'art. 9 del GDPR.

BANCA DATI

La disponibilità di strumenti informatici per svolgere l'attività lavorativa non consente l'accesso indiscriminato a banche dati al di fuori della stretta necessità di compiere il proprio lavoro. Il datore di lavoro concede l'uso degli strumenti informatici in base a un rapporto di fiducia affinché il personale operi in maniera lecita e nei limiti delle esigenze lavorative. L'accesso non autorizzato ai dati dei clienti giustifica il licenziamento.

IL CASO
Un dipendente di banca è stato licenziato per aver guardato senza motivo nei conti correnti dei clienti, utilizzando impropriamente gli strumenti informatici a sua disposizione per accedere a informazioni riservate al di fuori delle necessità lavorative. Il comportamento rappresentava una violazione del rapporto di fiducia con il datore di lavoro.

IL PROVVVEDIMENTO
La Corte di Cassazione ha confermato la **legittimità del licenziamento**, stabilendo che l'accesso indiscriminato a banche dati al di fuori della stretta necessità lavorativa viola il rapporto di fiducia.



CONCORRENZA SLEALE

Il commercio online deve rispettare il GDPR, altrimenti c'è il rischio di cause per concorrenza sleale. Un'azienda può agire contro una concorrente per concorrenza sleale basando la non correttezza del comportamento sulla violazione della normativa per la protezione dei dati personali. La violazione del GDPR può costituire un vantaggio competitivo sleale rispetto ai concorrenti che rispettano le regole.

IL CASO

Una farmacia tedesca commercializzava medicinali online senza rispettare gli obblighi imposti dalla normativa privacy in relazione ai dati particolari sulla salute trattati dall'e-commerce.
Un'azienda concorrente ha agito in giudizio ritenendo questo comportamento contrario alle regole della concorrenza leale, chiedendo l'interruzione della vendita e il riconoscimento di un comportamento di concorrenza sleale.

IL PROVVVEDIMENTO

La Corte di Giustizia UE ha affermato che non esistono norme che impediscono di agire contro concorrenti per concorrenza sleale basando la non correttezza del comportamento sulla violazione della normativa privacy.

CONSENSO MARKETING

I consensi per il marketing devono essere specifici e permettere la selezione delle categorie merceologiche desiderate, non possono essere generici.

IL CASO
Un'azienda usava dei moduli privacy che prevedevano dei consensi generici che non permettevano di selezionare le categorie merceologiche desiderate (es. telefonia, energia). L'azienda inoltre ignorava le opposizioni espresse tramite il Registro delle Opposizioni e usava tecniche commerciali aggressive.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato l'azienda per **300.000 euro**, vietando ulteriori trattamenti dei dati raccolti e imponendo controlli più rigidi sulla rete vendita e sui sistemi di acquisizione dei contatti.

BE LEGAL STUDIO

DATA BREACH

D

Le organizzazioni devono adottare misure adeguate per proteggere i dati personali e prevenire violazioni, dimostrando di aver fatto tutto il possibile per migliorare la protezione dei dati.

IL CASO
L'Ordine degli Psicologi della Lombardia ha subito un attacco ransomware che ha portato al furto e pubblicazione sul dark web di dati sensibili delle persone iscritte, incluse informazioni su procedimenti disciplinari. L'Ordine si è difeso sostenendo di avere risorse limitate, ma non aveva adottato misure adeguate per rilevare tempestivamente le violazioni né per proteggere il sistema informatico vulnerabile.

IL PROVVVEDIMENTO
Il Garante Privacy ha sanzionato per **30.000 euro** l'Ordine degli Psicologi della Lombardia per non aver adottato misure adeguate a proteggere i dati personali. Ha contestato l'assenza di sistemi di rilevamento delle violazioni e l'uso di un sistema informatico vulnerabile, stabilendo che le ragioni economiche addotte dall'Ordine non erano sufficienti a giustificare l'inadeguatezza delle misure di sicurezza.

DIFFUSIONE DATI

I dati personali del personale dipendente non possono essere condivisi con soggetti non autorizzati che non abbiano necessità di trattarli per le proprie mansioni.

IL CASO
Un datore di lavoro aveva comunicato tramite e-mail a un collega non autorizzato l'utilizzo da parte di una lavoratrice dei benefici della legge 104, trattandosi di dati di particolare importanza.

IL PROVVVEDIMENTO
Il Garante privacy ha dichiarato illecito il comportamento, ribadendo che i dati personali non possono essere condivisi con persone non autorizzate al trattamento.

E

EMAIL AZIENDALE

Dopo la fine del rapporto di lavoro, è fondamentale disattivare le caselle email aziendali intestate all'ex dipendente.
La mancata disattivazione può comportare accessi indebiti a comunicazioni private o personali.

IL CASO
L'indirizzo email di una ex dipendente era rimasto attivo per mesi, senza alcun reindirizzamento informato e senza avviso alla persona. Il rischio? Che le email personali continuassero a essere consultate da altri colleghi o responsabili.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato l'azienda per **20.000 euro**, non ritenendo idoneo il motivo della continuità aziendale e evidenziando la mancata informazione ai lavoratori.

EMAIL AZIENDALE

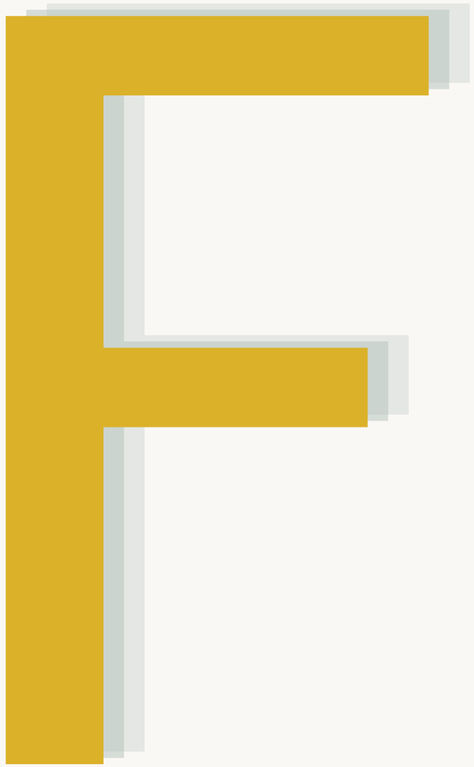
L'inoltro automatico delle mail aziendali di ex dipendenti verso altri account aziendali è illegittimo e può costare caro.

IL CASO
Un'azienda, alla cessazione di un rapporto di lavoro, ha attivato un sistema che inoltrava le mail dell'ex dipendente a un diverso indirizzo aziendale accessibile ad altre persone, invece di limitarsi al messaggio automatico informativo.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato l'azienda per **10.000 euro**, ritenendo il comportamento illegittimo e ricordando che esistono modi conformi per mantenere i contatti con la clientela.

BE LEGAL STUDIO

FOTO ESTETISTA



La pubblicazione di immagini di pazienti o clienti sui social richiede una informativa privacy completa e il consenso specifico esplicito dell'interessato.

IL CASO
Un centro di medicina estetica aveva pubblicato sul proprio profilo social un video con il volto riconoscibile di un paziente ripreso per oltre 30 secondi, senza che vi fosse il consenso della persona alla diffusione delle immagini sui social.
Il paziente si era riconosciuto e non aveva gradito.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato il centro medico per **8.000 euro** ritenendo illegittimo il trattamento dei dati sanitari.

FOTO CHIRURGO

La pubblicazione di foto di pazienti riconoscibili sui social media richiede il loro consenso specifico per la diffusione delle immagini.

IL CASO
Un chirurgo aveva pubblicato su Instagram le foto prima e dopo un intervento di lifting al volto di una paziente riconoscibile, senza aver acquisito il suo consenso alla diffusione delle immagini.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato il chirurgo per **20.000 euro**, dichiarando illecito il trattamento effettuato al di fuori delle finalità di cura.

BE LEGAL STUDIO

GEOLOCALIZZAZIONE

Le piattaforme che utilizzano i dati di geolocalizzazione dei rider devono rispettare il GDPR, evitando trattamenti automatizzati dei dati senza possibilità di contestazione. È vietato condividere dati di geolocalizzazione del personale con società terze quando l'app è in background e al di fuori dell'orario lavorativo. Il personale devono poter contestare le decisioni automatizzate del sistema e richiedere l'intervento umano per la prenotazioni dei turni e l'assegnazione degli ordini.

IL CASO

Foodinho srl, società del gruppo Glovo, effettuava trattamenti automatizzati dei dati di oltre 35.000 rider per prenotare con priorità i turni di lavoro e assegnare gli ordini, senza consentire ai rider di contestare le decisioni automatizzate o richiedere l'intervento umano. I dati di geolocalizzazione venivano inoltre condivisi con società terze anche quando l'app era in background e al di fuori dell'orario lavorativo.

IL PROVVVEDIMENTO

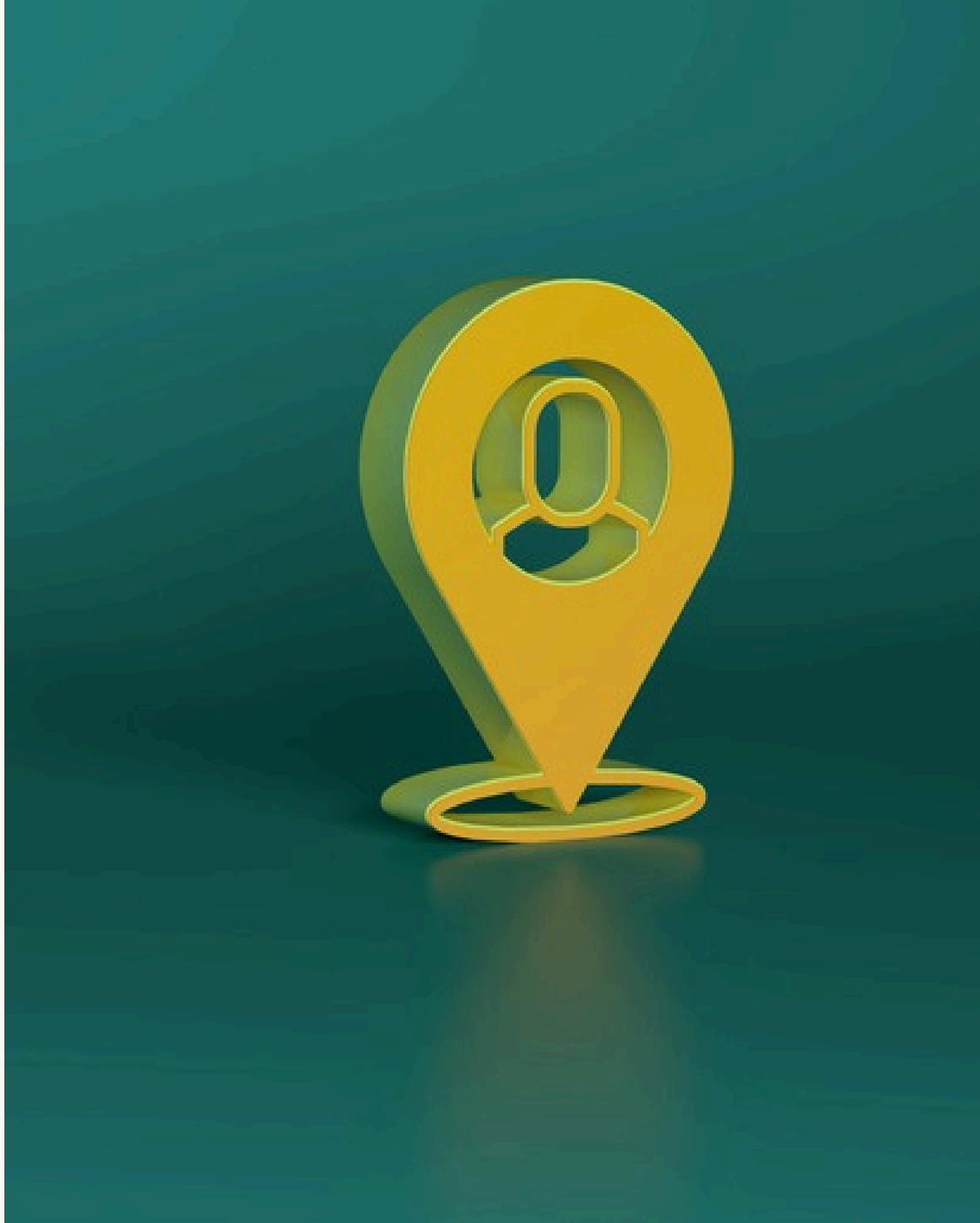
Il Garante privacy ha sanzionato la società per **5 milioni di euro** per il trattamento illecito dei dati personali dei rider in violazione del GDPR.

GPS

Il tracciamento GPS continuo dei dipendenti tramite autoveicoli aziendali viola le regole sulla privacy nei luoghi di lavoro se non rispetta le condizioni autorizzative.

IL CASO
Un'azienda di autotrasporti controllava circa 50 dipendenti tramite sistema GPS installato sui veicoli aziendali che tracciava posizione, velocità e uso dei mezzi in modo continuo.
L'informativa privacy data al personale dipendente era incompleta, i dati venivano conservati troppo a lungo e l'azienda non rispettava le condizioni previste dal provvedimento autorizzativo dell'Ispettorato del Lavoro.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato l'azienda per **50.000 euro**, ha ordinato di correggere il trattamento dei dati personali e di informare correttamente il personale dipendente.



H

HACKER

Titolari e responsabili del trattamento devono adottare misure tecniche e organizzative di sicurezza adeguate per proteggere i dati personali, anche da attacchi hacker, e per reagire tempestivamente in caso di violazioni.

IL CASO
Nel 2021 un attacco hacker, realizzato con un ransomware introdotto nel sistema attraverso un pc di un dipendente, aveva colpito il sistema sanitario del Lazio, rendendo inaccessibili dati e molti servizi sanitari (es. prenotazioni, ritiro dei referti).
Le indagini avevano evidenziato gravi carenze di sicurezza da parte dei gestori dei servizi e la mancata notifica dell'attacco al Garante privacy.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato i tre soggetti coinvolti per diverse violazioni del GDPR, legate alla gestione e alla sicurezza dei dati personali, e ha ordinato la pubblicazione del provvedimento sul sito del Garante.

INFORMATIVA

I sistemi di videosorveglianza richiedono l'esposizione di cartelli informativi obbligatori che rispettino il principio di trasparenza del GDPR.

IL CASO
Un supermercato aveva installato 6 telecamere attive senza esporre cartelli informativi sul trattamento dei dati personali. L'assenza di avvisi impediva ai clienti di sapere che stavano entrando in zona sorvegliata.

IL PROVVVEDIMENTO
Il Garante privacy ha dichiarato illecito il trattamento per violazione del principio di trasparenza, ordinando l'esposizione di idonei cartelli informativi e irrogando sanzione pecuniaria.

INFORMATIVA PRIVACY

Il GDPR prevede obblighi di chiarezza e comprensibilità. L'art. 7 del GDPR richiede che il consenso sia presentato in forma comprensibile con linguaggio semplice. L'art. 12 del GDPR stabilisce che le informazioni devono essere concise e trasparenti, prevedendo l'uso di icone standardizzate per dare un quadro d'insieme facilmente leggibile.

Per rendere le informative più accessibili, sono stati sviluppati progetti innovativi come icone e fumetti.
Il Garante Privacy ha promosso un contest "Informative privacy più chiare grazie alle icone? È possibile".
L'Istituto Italiano Privacy ha elaborato informative privacy a fumetti per migliorare la comprensibilità.

Il GDPR riconosce ufficialmente l'importanza di strumenti visivi per la comunicazione della privacy. L'art. 12 del GDPR prevede espressamente l'uso di icone standardizzate come metodo per presentare informazioni in modo intelligibile, dimostrando come rispettare gli obblighi normativi attraverso linguaggi visivi innovativi.
Il Garante privacy il 4 febbraio 2025 ha pubblicato il white paper "Rendere le informative privacy più comprensibili - il legal design come approccio rivolto all'utente".

INTELLIGENZA ARTIFICIALE

Il 13 marzo 2024 il Parlamento europeo ha approvato l'AI Act, il primo quadro giuridico organico sull'intelligenza artificiale. Il principio guida è garantire che l'innovazione rimanga sicura e rispettosa dei diritti fondamentali, applicando un approccio "risk-based" che calibra obblighi e tutele in base al livello di rischio di ciascun sistema: rischio minimo, rischio limitato, rischio alto e rischio inaccettabile.

Tra i sistemi "ad alto rischio" rientrano quelli utilizzati nei processi di selezione e assunzione del personale: pubblicazione di annunci mirati, screening automatico dei CV, valutazione delle candidature. Per queste applicazioni l'AI Act impone controlli umani, documentazione tecnica dettagliata e registri delle attività, così da evitare decisioni arbitrarie o discriminatorie.

L'AI Act è entrato in vigore dal 1 agosto 2024 e avrà un'applicazione graduale.

LESIONE DELLA PRIVACY

Le ricette mediche contengono dati personali relativi alla salute di particolare importanza che richiedono protezione speciale. Il loro trattamento deve prevenire rischi e gravi danni per i pazienti. I medici devono garantire che le ricette siano conservate in modo sicuro e ritirate dai pazienti in busta chiusa, evitando di lasciarle alla portata di chiunque.

IL CASO

Un medico lasciava le ricette per i suoi pazienti in un contenitore su un muro esterno dello studio, senza nemmeno inserirle in buste chiuse, consentendo così a chiunque di poterle leggere.
Questa pratica esponeva i dati sanitari sensibili dei pazienti a potenziali violazioni della privacy e accessi non autorizzati.

IL PROVVVEDIMENTO

Il Garante privacy ha sanzionato il medico per **20.000 euro** per violazione del GDPR. I Garante ha chiarito che le ricette mediche possono essere lasciate nelle farmacie e negli studi medici per il ritiro da parte dei pazienti, purché in busta chiusa. Lasciarle incustodite o alla portata di chiunque viola la privacy dei pazienti e comporta pesanti sanzioni.

M

MARKETING

Anche nei contratti di abbonamento per servizi di trasporto va garantito il diritto di negare il consenso per l'attività di marketing.

IL CASO
Un'azienda di trasporti usava un modulo per abbonamenti non conforme al GDPR e alla normativa privacy. Il modulo non consentiva di prestare un consenso libero, specifico e informato, non distingueva tra dati obbligatori e dati facoltativi non necessari per l'abbonamento e non segnalava il diritto di opporsi all'uso dei dati per attività di marketing diretto.
di esprimere un consenso libero, non distingueva tra dati obbligatori e facoltativi, e non segnalava il diritto di opporsi al marketing diretto.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato l'azienda per **50.000 euro**, vietando l'uso dei dati illegittimamente raccolti e imponendo la revisione delle policy aziendali sulla privacy.

NOMI VISIBILI

L'invio di mail a più persone con indirizzi mail visibili richiede attenzione particolare, specialmente per dati sanitari, e necessita di misure tecniche adeguate.

IL CASO
Una società di dispositivi medici, inviando aggiornamenti a pazienti diabetici, aveva inserito gli indirizzi in "copia conoscenza" invece che "copia conoscenza nascosta", permettendo così di far vedere gli indirizzi email della mailing-list.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato la società con due sanzioni per totali **300.000 euro** per la grave violazione della privacy e la mancata adozione di misure tecniche e organizzative adeguate a ridurre il rischio.

OBLIO

Le persone guarite da patologie oncologiche hanno diritto di non fornire informazioni né subire indagini sulla pregressa condizione patologica in specifici ambiti.

IL CASO
La legge n. 193 del 7 dicembre 2023 ha disciplinato il diritto all'oblio oncologico limitando le informazioni sanitarie che possono essere raccolte per l'accesso a servizi bancari, assicurativi, adozioni, concorsi, lavoro e formazione professionale.

IL PROVVVEDIMENTO
Il Garante privacy ha dedicato una pagina informativa sul tema con documenti di interesse, schede informative chiare e FAQ

"[...] privacy come valore attorno al quale ricostruire un nuovo patto sociale: anello di congiunzione tra pubblico e privato, precondizione di ogni altro diritto civile [...] Porre la dignità al centro dello sviluppo tecnologico significa definire i valori del futuro."

Privacy 2030: Una nuova visione per l'Europa - Giovanni Buttarelli, Garante protezione dati

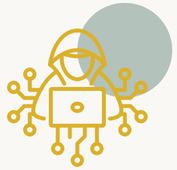
PRESENZE SUL LAVORO

P

I sistemi biometrici (es. riconoscimento facciale, impronte digitali) non possono essere utilizzati per rilevare le presenze del personale dipendente sul luogo di lavoro. Attualmente non esiste alcuna norma che consenta in generale l'uso di dati biometrici per questa finalità. Le aziende devono utilizzare sistemi meno invasivi come i tradizionali badge identificativi.

IL CASO
Alcune aziende avevano adottato un sistema di riconoscimento facciale per controllare l'accesso e le presenze del personale presso un sito di smaltimento rifiuti, ritenendo necessaria questa tecnologia per garantire un controllo efficace degli accessi.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato l'azienda per **70.000 euro** dichiarato illegittimo il sistema, precisando che le aziende avrebbero dovuto utilizzare sistemi meno invasivi per controllare le presenze (come i badge).



PHISHING

Il phishing è una tecnica illecita per appropriarsi di informazioni riservate (es. password, codici di accesso e dati bancari) con l'intento di compiere operazioni fraudolente. Le banche devono adottare misure di sicurezza adeguate e preventive per tutelare gli utenti (es. SMS-alert, autenticazione a due fattori). I clienti devono evitare di comunicare codici di accesso a sconosciuti e di cliccare su link sospetti.

IL CASO
Vittime di phishing subiscono sottrazioni di denaro dai propri conti correnti dopo aver condiviso inconsapevolmente i propri codici di accesso con truffatori. Le vittime richiedono il rimborso alle banche sostenendo che non erano state adottate misure di sicurezza sufficienti per prevenire gli accessi fraudolenti ai sistemi di home banking.

IL PROVVVEDIMENTO
La giurisprudenza ritiene generalmente che le banche non sono responsabili se i clienti hanno condiviso imprudentemente i propri codici, vanificando le misure di sicurezza adottate. Tuttavia, le banche possono essere ritenute responsabili e dover rimborsare le vittime solo se non hanno adottato misure di sicurezza adeguate per proteggere i propri clienti dai tentativi di frode.

BE LEGAL STUDIO

DIVERSI TIPI DI **FRODI INFORMATICHE**

con cui i truffatori cercano di appropriarsi dei dati e informazioni riservate con l'intento di compiere operazioni fraudolente

PHISHING	attraverso email con testi o link ingannevoli
SMISHING	con sms o chat con testi o link ingannevoli
VISHING	chiamate in cui si fingono operatori della banca o di istituzioni fidate
PHARMING	attraverso il reindirizzamento su siti web falsi

QUANTIFICAZIONE DEL DANNO

Un trattamento di dati personali non conforme al GDPR e alla normativa può dare luogo al risarcimento dei danni patrimoniali o non patrimoniali subiti.
Per ottenere il risarcimento occorre provare tre elementi: una violazione di legge, un danno e un nesso causale tra i due.

IL CASO

Un avvocato ha citato in giudizio una società che gestisce una banca dati giuridica, per avergli inviato materiale pubblicitario nonostante la revoca del consenso al marketing diretto.
Ha chiesto il risarcimento per danni patrimoniali e non patrimoniali, lamentando la perdita di controllo sui suoi dati personali. La società si è difesa sostenendo problemi organizzativi interni e negando che la sola violazione del GDPR bastasse a giustificare un risarcimento. La questione era stata rimessa davanti alla Corte europea.

IL PROVVVEDIMENTO

La Corte europea ha stabilito che chi chiede il risarcimento deve dimostrare non solo la violazione delle norme GDPR, ma anche che questa violazione ha effettivamente causato un danno. Per determinare l'importo del risarcimento non si applicano i criteri delle sanzioni amministrative, ma i criteri generali per il risarcimento dei danni, eventualmente anche basati sull'equità.

REGISTRO DELLE OPPOSIZIONI

Per fare attività di marketing telefonico serve il preventivo consenso libero, specifico, informato e inequivocabile del destinatario. Chi acquista liste di contatti deve verificare che il fornitore abbia acquisito correttamente il consenso al marketing, fornito una completa informativa sull'uso dei dati e controllato il Registro pubblico delle opposizioni. La prudenza e la necessità di verifica sono fondamentali per evitare sanzioni.

IL CASO
Un call center aveva acquistato 100.000 contatti da un list provider moldavo a cui ha fatto oltre 32.600 telefonate. Il call center non aveva però controllato che il list provider avesse acquisito il consenso al marketing, avesse dato una completa informativa privacy e avesse verificato il Registro delle opposizioni.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato il call center per **60.000 euro** per la mancata verifica sulla gestione dei dati acquistati.

SMART WORKING

S

Nel lavoro agile (smart working) il datore di lavoro può usare strumenti tecnologici per controlli a distanza del personale solo per le finalità specifiche previste dalla legge: esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale. Non è consentito utilizzare strumenti di controllo per verificare semplicemente da dove viene svolta la prestazione lavorativa, senza altre giustificazioni legittime.

IL CASO

Un'azienda obbligava i dipendenti in smart working ad attivare la geolocalizzazione tramite un'app per monitorare la loro posizione durante l'orario di lavoro. L'azienda aveva come unico scopo verificare da dove veniva svolta la prestazione lavorativa, senza altre finalità organizzative, produttive o di sicurezza che giustificassero l'uso dello strumento tecnologico di controllo.

IL PROVVVEDIMENTO

Il Garante privacy ha sanzionato l'azienda per **50.000 euro** per l'utilizzo improprio di strumenti di geolocalizzazione. Il Garante ha stabilito che lo strumento tecnologico non poteva essere utilizzato per la verifica della posizione dei lavoratori, non rientrando nelle finalità legittime previste dalla legge per i controlli a distanza nel lavoro agile.

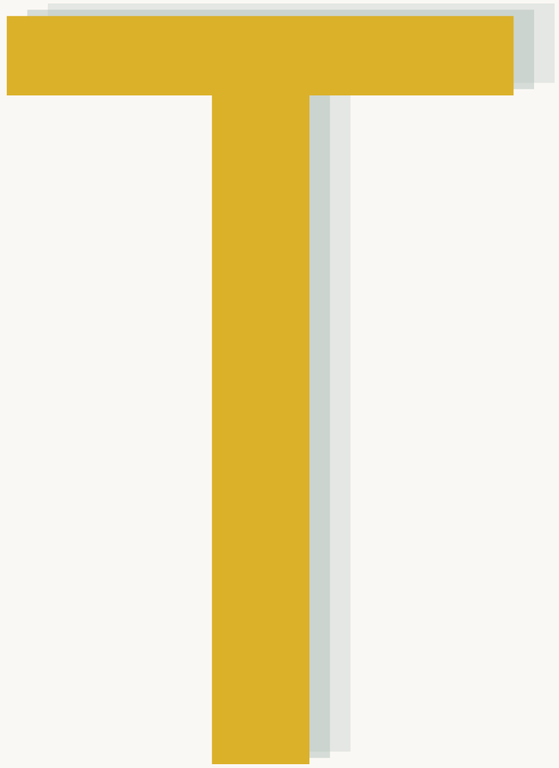
SPONSOR

I dati personali in possesso di associazioni non possono essere trasferiti a terzi per marketing senza consenso, valutando le aspettative degli interessati.

IL CASO
Un'associazione tennistica olandese aveva trasferito i dati personali delle persone tesserate (nomi, mail, indirizzi, numeri di telefono) a due sponsor senza il loro consenso. Uno degli sponsor, una società di giochi d’azzardo, li aveva poi usati per fare chiamate commerciali.

IL PROVVVEDIMENTO
La Corte di Giustizia UE ha stabilito che l'associazione avrebbe dovuto valutare le aspettative degli associati: se si aspettavano che i loro dati fossero trasferiti a terzi per fini commerciali oppure se si aspettavano che l'associazione chiedesse il loro consenso per finalità diverse da quelle associative.
La Corte ha ribadito che serve sempre il consenso per cedere dati a terzi per marketing.

TELEMARKETING



Le aziende che affidano l'attività di marketing promozionale a soggetti esterni devono vigilare sul rispetto delle regole per il trattamento dei dati personali. È obbligatorio consultare il Registro pubblico delle opposizioni prima di effettuare chiamate promozionali. Le persone fisiche possono segnalare le telefonate indesiderate tramite l'apposito canale sul sito del Garante privacy.

IL CASO

Le aziende che affidano l'attività di marketing promozionale a soggetti esterni devono vigilare sul rispetto delle regole per il trattamento dei dati personali. È obbligatorio consultare il Registro pubblico delle opposizioni prima di effettuare chiamate promozionali. Le persone fisiche possono segnalare le telefonate indesiderate tramite l'apposito canale sul sito del Garante privacy.

IL PROVVVEDIMENTO

Il Garante privacy ha sanzionato la società per **quasi 700.000 euro** per trattamento illecito di dati a fini promozionali.
La sanzione evidenzia la responsabilità delle aziende nella scelta e controllo dei fornitori esterni di servizi di marketing.

TELEMARKETING

Le attività di telemarketing devono rispettare il principio di liceità del trattamento dei dati. Contattare numeri iscritti al Registro Pubblico delle Opposizioni senza il consenso valido dell'interessato costituisce una violazione della normativa. Il GDPR richiede misure tecniche e organizzative efficaci per garantire la tracciabilità dei consensi e la conformità dell'intera filiera, compresi i soggetti esterni che operano per conto del titolare.

IL CASO
Un'azienda del settore energetico è ha effettuato chiamate promozionali a 34 utenze telefoniche iscritte al Registro delle Opposizioni. Il contatto è avvenuto senza un'idonea base giuridica. Inoltre, i controlli sui partner commerciali erano inadeguati: l'azienda non era in grado di dimostrare la legittimità dei contratti acquisiti, alcuni dei quali erano stati generati proprio a seguito di contatti illeciti. Anche le misure adottate per prevenire queste irregolarità sono risultate carenti.

IL PROVVVEDIMENTO
Il Garante ha vietato ogni ulteriore trattamento dei dati raccolti illecitamente, ha imposto l'obbligo di informare i soggetti coinvolti e di rafforzare i controlli su tutta la rete di vendita. L'azienda è stata sanzionata per **100.000 euro**.

TRASPARENZA

Chi apre un account online deve poter capire subito e con chiarezza se i suoi dati saranno usati per fini di marketing, senza dover navigare tra varie schermate. Le aziende devono rispettare sia le regole del GDPR sia quelle del Codice del consumo. La mancanza di chiarezza sull'uso dei dati personali costituisce una pratica commerciale ingannevole.

IL CASO
Una piattaforma online aveva adottato una procedura per la creazione di account che preimpostava il consenso automatico dell'utente a ricevere comunicazioni di marketing e rendeva difficile revocare questo consenso. La procedura mancava di chiarezza e trasparenza sull'uso dei dati personali inseriti dagli utenti durante la registrazione.

IL PROVVVEDIMENTO
Il Consiglio di Stato ha stabilito che preimpostare il consenso automatico per il marketing e rendere difficile la revoca viola il GDPR. Inoltre, ha chiarito che la procedura di registrazione di una piattaforma costituisce una pratica commerciale e la mancanza di trasparenza sull'uso dei dati rappresenta una pratica commerciale ingannevole contraria al Codice del consumo.

UTENZE

Le aziende devono progettare adeguati sistemi di trattamento dei dati personali e vigilare sull'operato dei propri agenti. È vietato utilizzare illegittimamente i dati delle persone per attivare contratti non richiesti con firme false e dati inesatti. Le società sono responsabili delle violazioni commesse dai loro rappresentanti e rischiano sanzioni milionarie per mancanza di controlli adeguati.

IL CASO

Agenti porta a porta di una società di fornitura di luce e gas hanno attivato per mesi contratti di fornitura non richiesti utilizzando firme false e dati inesatti di ignari clienti.
Gli agenti avevano utilizzato illegittimamente i dati personali delle persone per attivare i contratti a loro insaputa, senza alcun consenso reale.

IL PROVVVEDIMENTO

Il Garante privacy, dopo numerose segnalazioni e reclami delle persone coinvolte, ha sanzionato la società per **5 milioni di euro** per le gravi violazioni nel trattamento dei dati personali. La società non aveva progettato un adeguato sistema di controllo sul trattamento dei dati dei clienti da parte dei propri agenti.

VIDEORIPRESE DIFENSIVE

Le videoriprese sul lavoro non possono essere utilizzate come prova disciplinare se manca una corretta informazione preventiva ai dipendenti. Il personale deve essere adeguatamente informato sulle modalità d'uso degli impianti audiovisivi installati e sull'effettuazione dei controlli. La trasparenza e il rispetto del trattamento dei dati personali sono fondamentali anche nei controlli aziendali.

IL CASO
Un'azienda aveva licenziato una dipendente per furto usando le videoriprese acquisite dal sistema di videosorveglianza.
Le riprese erano però illecite perché effettuate senza informare adeguatamente il personale sulle modalità d'uso degli impianti e sui possibili controlli.

IL PROVVVEDIMENTO
La Corte di Cassazione ha annullato il licenziamento e disposto la reintegra della dipendente, ribadendo che non si possono usare le videoriprese come prova se manca una corretta informazione preventiva. La decisione conferma che le prove ottenute violando le regole sulla privacy dei lavoratori sono inutilizzabili nei procedimenti disciplinari.

VIDEOSORVEGLIANZA PER CONTROLLO A DISTANZA

L'uso di impianti audiovisivi per il controllo a distanza dei lavoratori è possibile esclusivamente per le finalità dell'art. 4 dello Statuto dei lavoratori: esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale. Quest'ultima include protezione da appropriazioni, danneggiamenti e lesioni dell'immagine aziendale. Servono accordo sindacale o autorizzazione dell'Ispettorato del lavoro e informativa GDPR completa.

IL CASO
Il caso riguardava la definizione delle finalità che giustificano l'installazione di sistemi di videosorveglianza sui luoghi di lavoro per il controllo dei dipendenti e i requisiti procedurali necessari per la loro corretta implementazione nel rispetto dei diritti dei lavoratori.

IL PROVVVEDIMENTO
La Corte di Cassazione ha stabilito che la videosorveglianza è ammessa solo per le tre finalità specifiche dell'art. 4 dello Statuto dei lavoratori. Ha chiarito che la tutela del patrimonio comprende la protezione da appropriazioni, danneggiamenti e lesioni della reputazione, richiedendo accordo sindacale o autorizzazione dell'Ispettorato e informativa GDPR.

VIDEOSORVEGLIANZA

La videosorveglianza sul lavoro richiede il rispetto dello Statuto dei Lavoratori e del GDPR, con il necessario accordo sindacale o l'autorizzazione dell'Ispettorato del Lavoro e un'informativa privacy adeguata.

IL CASO
Un Comune aveva installato una telecamera di videosorveglianza nell'atrio vicino ai dispositivi di rilevazione presenze senza rispettare le norme sui controlli a distanza, usando poi le immagini registrate per muovere delle contestazioni disciplinari.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato per **3.000 euro** il Comune perché non aveva adeguatamente informato il personale in merito all'uso delle immagini raccolte dalla videocamera e ha imposto di fornire idonea informativa a lavoratori e visitatori.

PASSWORD

La corretta gestione delle password è un aspetto cruciale per garantire la sicurezza dei dati personali e un pilastro della data protection, in conformità al GDPR. Le aziende e tutti i titolari del trattamento di dati personali devono adottare misure tecniche e organizzative adeguate e mantenerle aggiornate e verificate, per proteggere i dati da accessi non autorizzati, in conformità agli articoli 5 e 32 del GDPR.

IL CASO

Nel 2019 Meta ha conservato in chiaro circa 600 milioni di password degli utenti Facebook e Instagram, violando diverse disposizioni del GDPR e mettendo a rischio la sicurezza di milioni di persone. Non solo: dopo la scoperta, Meta ha fatto la notifica dell'errore al Garante irlandese in ritardo (va fatta senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla scoperta) e senza documentare le misure correttive adottate.

IL PROVVVEDIMENTO

Il Garante privacy irlandese ha sanzionato Meta per **91 milioni di euro**, considerando la gravità della violazione e i rischi elevati per la sicurezza degli utenti.

EX DIPENDENTI

L'accesso ai dati personali previsto dall'art. 15 del GDPR può essere limitato solo se lede diritti altrui, come il segreto aziendale.
Le aziende non possono opporre un divieto netto ma devono bilanciare i propri diritti con quelli dell'interessato.

IL CASO
Un ex dipendente ha chiesto accesso ai suoi dati personali conservati nel PC aziendale. L'azienda ha negato completamente l'accesso per tutelare i segreti aziendali, escludendo interamente la possibilità per l'ex dipendente di accedere alle informazioni che lo riguardavano.

IL PROVVVEDIMENTO
Il Garante privacy ha sanzionato l'azienda per **10.000 euro** e ha stabilito che l'azienda aveva sbagliato a escludere interamente l'accesso. L'azienda avrebbe dovuto consentire l'accesso ai dati personali dell'ex dipendente, cancellando le informazioni eccedenti che non si riferivano a lui e che avrebbero potuto compromettere i segreti aziendali.

Y

YES / NO CONSENT

Il consenso al trattamento dei dati personali, per essere valido, deve essere libero, specifico, informato e manifestato attraverso un'azione positiva e inequivocabile. L'uso di caselle preflaggate (cioè già selezionate di default) non soddisfa questi requisiti, perché non consente all'interessato di esprimere una vera scelta tra dare o rifiutare il consenso. Il GDPR vieta questa prassi in ogni contesto, per i cookie e per qualsiasi trattamento fondato sul consenso.

IL CASO
Un sito internet mostrava un banner con sei caselle preflaggate per cookie non tecnici (es. Facebook, Google Analytics, YouTube) e senza un pulsante per rifiutare facilmente i cookie. L'informativa risultava poco chiara e non conforme alle Linee guida del Garante.

IL PROVVVEDIMENTO
Il Garante ha accertato l'illiceità del trattamento e ha ammonito la società, senza sanzione pecuniaria, in considerazione dei correttivi adottati in corso di procedimento. La società ha infatti modificato il banner, permettendo così un consenso libero e granulare.

Z

ZERO RISCHI NON ESISTONO

Purtroppo anche con buone misure in atto, gli attacchi informatici evolvono rapidamente e colpiscono sia dall'esterno che dall'interno. Nessuna organizzazione può dirsi al sicuro: per questo è fondamentale per ogni organizzazione rispettare le norme e potere dimostrare in modo concreto e documentabile la conformità.

IL CASO

Il *Data Breach Investigations Report 2025* di Verizon ha analizzato oltre 22.000 incidenti, di cui 12.195 violazioni confermate. Nell'area EMEA le intrusioni sono aumentate del 53% e il 29% proviene dall'interno delle organizzazioni. Preoccupano lo sfruttamento delle vulnerabilità e il fatto che il 60% delle violazioni è legato a fattori umani. Crescono anche gli attacchi legati allo spionaggio e all'uso scorretto dell'AI.

IL REPORT

Per proteggersi, le organizzazioni devono aggiornare regolarmente sistemi e dispositivi. È fondamentale rafforzare il controllo sugli accessi e sui dispositivi non gestiti (es. BYOD). Serve maggiore vigilanza sulla supply chain, spesso coinvolta negli attacchi. La formazione del personale resta centrale, dato che l'elemento umano è presente in circa il 60% delle violazioni. Infine, è essenziale adottare una difesa multilivello e politiche di sicurezza più rigorose anche per l'uso dell'AI.

FONTI E PROVVEDIMENTI

ACCESSI AI LUOGHI - Garante privacy spagnolo - provvedimento n. EXP202315637
ACCOUNT - Garante finlandese 06.03.2024 - TSV/26/2020

BIOMETRIA - Corte di Cassazione - sentenza n. 12967/2024 del 13.05.2024
Garante privacy – provvedimento 317 del 16 settembre 2021
BANCA DATI - Corte di Cassazione - sentenza n. 2806 del 05.02.2025

CONSENSO - Garante privacy - provvedimento n. 114 del 27.02.2025
CONCORRENZA SLEALE - Corte di Giustizia UE - sentenza del 04.10.2024 Causa C-21/23

DATA BREACH - Garante privacy – provvedimento n. 271 del 29.04.2025
DIFFUSIONE DATI - Garante privacy – provvedimento n. 796 del 19.12.2024

EMAIL AZIENDALE - Garante privacy – provvedimento n. 140 del 07.03.2024
EMAIL AZIENDALE - Garante privacy – provvedimento n. 602 del 21.12.2023

FOTO ESTETISTA - Garante privacy – provvedimento n. 769 del 12.12.2024
FOTO CHIRURGO - Garante privacy – provvedimento n. 10 del 11.01.2024

GEOLOCALIZZAZIONE - Garante privacy – provvedimento n. 675 del 13.11.2024
GPS - Garante privacy – provvedimento n. 135 del 13.03.2025

HACKER - Garante privacy – provvedimenti nn. 194-195-196 del 21.03.2024

INFORMATIVA PRIVACY - Garante privacy - provvedimento n. 137 del 13.03.2025
INFORMATIVA PRIVACY - Garante privacy - "Rendere le informative privacy più comprensibili - il legal design come approccio rivolto all'utente".
INTELLIGENZA ARTIFICIALE - Regolamento (UE) 2024/1689

LESIONE DELLA PRIVACY - Garante privacy - provvedimento n. 11 dell'11.01.2024

MARKETING - Garante privacy - provvedimento n. 125 del 22.02.2024
NOMI VISIBILI - Garante privacy - provvedimento n. 62 del 08.02.2024

OBLIO ONCOLOGICO - FAQ Garante privacy

PRESENZE SUL LAVORO - Garante privacy - provvedimento n. 105 del 22.02.2024
PHISHING - Corte di Cassazione - ordinanza n. 23683 del 04.09.2024

QUANTIFICAZIONE DEL DANNO - Corte di Giustizia UE - sentenza del 11.04.2024 - C-741/21

REGISTRO DELLE OPPOSIZIONI - Garante privacy - provvedimento n. 561 del 30.11.2023

SMART WORKING - Garante privacy - provvedimento n. 135 del 13.03.2025
SPONSOR - Corte di Giustizia UE - sentenza del 04.1.2024 - C-621/22

TELEMARKETING - Garante privacy - provvedimento n. 672 del 13.11.2024
TELEMARKETING - Garante privacy - provvedimento n. 204 del 11.04.2024
TRAPARENZA - Consiglio di Stato - sentenza n. 9614 del 2 dicembre 2024

UTENZE - Garante privacy - provvedimento n. 440 del 17.07.2024

VIDEORIPRESE DIFENSIVE - Corte di Cassazione - ordinanza n. 10822 del 24.04.2025
VIDEOSORVEGLIANZA PER CONTROLLO A DISTANZA - Corte di Cassazione - sentenza n. 23985 del 06.092024
VIDEOSORVEGLIANZA - Garante privacy - provvedimento n. 234 del 11.04.2024

PASSWORD - Irish Data Protection Commission (DPC), provvedimento 27.09.2024

EX DIPENDENTI - Garante privacy - provvedimento n. 380 del 20.06.2024

YES/NO CONSENT - Garante privacy - provvedimento n. 650 del 17.10.2024

ZERO RISCHI NON ESISTONO - Data Breach Investigations Report 2025 di Verizon

CHI SIAMO

Be Legal Studio nasce dall'incontro di professioniste indipendenti con due visioni complementari: quella di Veronica, avvocata con una **solida esperienza** e una **spinta profonda a rinnovare** il modo in cui il diritto si avvicina alle persone, e quella di Ludovica, avvocata guidata da una forte **passione per la giustizia** e dal desiderio di rendere il sapere legale uno **strumento di emancipazione e consapevolezza**.

Il progetto prende forma da una esigenza condivisa: dare spazio a un **approccio più collaborativo, umano e comprensibile** per superare la rigidità della cultura giuridica tradizionale.

Be Legal Studio si vuole distinguere oggi come uno **studio che ascolta, accoglie e semplifica**, diventando un punto di riferimento per chi cerca una consulenza legale che rispecchi i propri valori.

Veronica Morlacchi

Laureata con 110/110 all'Università Cattolica di Milano, sono avvocata dal 2004 e dal 2017 sono abilitata al patrocinio per la Corte di Cassazione.
Mi occupo di contratti, privacy e protezione dati, responsabilità civile, diritto del digitale, modello 231, aspetti legali connessi a progetti per la governance della sostenibilità.
Assisto PMI ed enti nell'implementazione della compliance integrata nella loro attività.
Ho conseguito il titolo di Maestro della Protezione Dati & Data Protection Designer® dell'IIP,. Sono Legal project manager certificata dell'IILPM e socia di Federprivacy - Associazione Privacy Officer.
Sono coautrice del libro Che contratti! Progettare, scrivere, disegnare contratti semplici e chiari, Torino, ottobre 2022, G. Giappichelli.
Lavoro a progetti di legal design e sono socia di PLAIN, organizzazione che promuove la diffusione di un linguaggio chiaro nelle professioni.
Ho seguito corsi di alta formazione e master in legal tech, data protection e compliance aziendale.
Ho conseguito l'Executive Programme Legal Impact - ESG e sostenibilità d'impresa al Cottino Social Impact Campus di Torino e mi sono formata come Compliance Coach alla Ca' Foscari Challenge School.

P.IVA 02727620128

Ludovica Padovese

Laureata a pieni voti all'Università degli studi di Trieste, sono avvocata dal 2023, iscritta all'Ordine degli avvocati di Busto Arsizio.
Mi occupo di consulenza stragiudiziale a favore di imprese, studi professionali, freelance e persone private nel campo del diritto civile, in particolare in relazione a contratti, risarcimento dei danni, privacy e protezione dei dati personali, tematiche giuridiche delle nuove tecnologie.
Supporto PMI nell'integrare la compliance nelle loro attività.
In questi settori, svolgo anche attività di rappresentanza in giudizio e di assistenza nei procedimenti di mediazione e negoziazione assistita.
Ho conseguito il titolo di Maestro della Protezione Dati & Data Protection Designer® dell'Istituto Italiano per la Privacy e la Valorizzazione dei dati (IIP).
Collaboro a progetti di legal design, in particolare su contratti, policy e regolamenti aziendali.
Ho seguito formazioni specifiche nel campo del diritto delle nuove tecnologie e del legal design, tra cui il Corso di perfezionamento in Coding for Lawyers, Legal Tech, Legal Writing and Legal Design all'Università degli Studi di Milano e la Legal Design Winter School LEDS all'Università di Bologna.

P.IVA 03934250121

I NOSTRI VALORI

SEMPLICITÀ
É il nostro modo di comunicare, agire e accompagnare le persone nella complessità giuridica.
La semplificazione è per noi un valore fondamentale: complesso può non volere dire complicato.

CONCRETEZZA
Ogni nostra azione ha uno scopo chiaro, tangibile e utile. L'aggiornamento costante, la consolidata esperienza e un approccio consulenziale umano e strutturato ci permettono di dare soluzioni su misura, concrete, praticabili e comprensibili.

INNOVAZIONE
Adottiamo un approccio multidisciplinare, unendo diritto, tecnologia e strumenti innovativi per il diritto, come il legal design e il legal project management.
Soltanto considerando le reali necessità della clientela possiamo dare soluzioni efficaci.

FIDUCIA
É la base su cui costruiamo il nostro lavoro.
Partendo dall'ascolto accompagniamo le persone in un percorso chiaro: individuiamo le esigenze, raccogliamo la documentazione, approfondiamo le norme e la giurisprudenza, comunichiamo l'evoluzione del lavoro e guidiamo nei momenti di incertezza.

DI COSA CI OCCUPIAMO

CIVILE

- Contratti, controversie contrattuali e recupero crediti
- Risarcimento danni
- Rapporti patrimoniali

COMPLIANCE

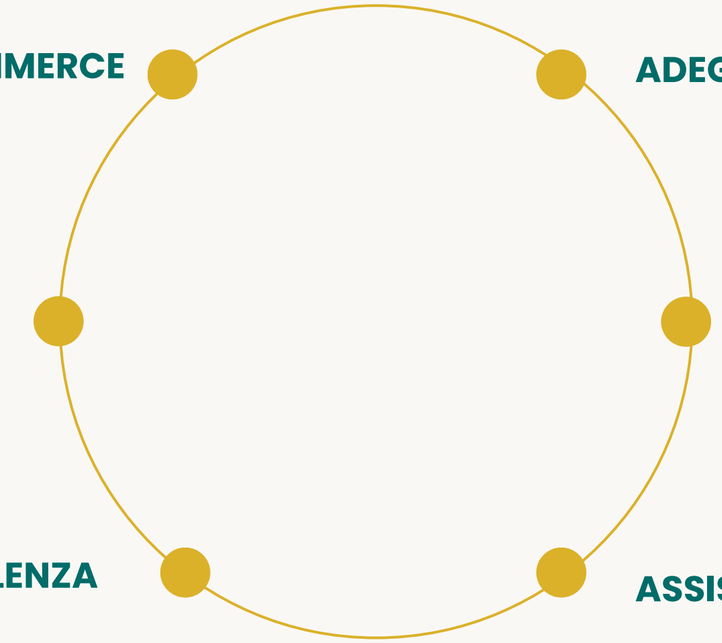
- Protezione dati e privacy
- Policy, regolamenti e modello 231
- Digitale

I NOSTRI SERVIZI PRIVACY

Assistiamo PMI, studi professionali e freelance in materia di protezione dati personali, privacy e conformità al GDPR.
La nostra visione va oltre il semplice adempimento normativo: consideriamo la privacy un **elemento strategico** fondamentale di ogni attività, per dare **valore aggiunto** a un'identità aziendale **affidabile e virtuosa**.

ADEGUAMENTO PER SITI WEB ED E-COMMERCE

ADEGUAMENTO PER IMPRESE ED ENTI



FORMAZIONE

ADEGUAMENTO PER STUDI PROFESSIONALI E FREELANCE

CONSULENZA

ASSISTENZA NEI PROCEDIMENTI AVANTI LE AUTORITÀ

Se vuoi scoprire di più sul nostro lavoro ci trovi su
www.belegalstudio.it

@belegalstudio_studiolegale

@belegalstudio

Be Legal Studio

Veronica Morlacchi

Ludovica Padovese

La newsletter
COMPLIANCE IS IN THE AIR

Vuoi ricevere novità e approfondimenti sulla **compliance nelle PMI e nelle professioni**: dai contratti alla privacy, dalle regole del digitale alla sostenibilità e al modello organizzativo 231?

ISCRIVITI QUI ALLA NOSTRA NEWSLETTER MENSILE

BE LEGAL STUDIO

Busto Arsizio (VA), via I Maggio n. 5

0331.622235

info@belegalstudio.it