pentha
Servizi Integrati per le Imprese
ANNO 16 NUMERO 277
Aderente ASSO DPO Associazione Data Protection Officer
FEDERPRIVACY Federazione Italiana Privacy
Delegazione provinciale

Cuneo, 25/10/2023

In questo numero

Il focus di questo numero

Gentili Lettori,

a seguito di un lungo periodo estivo che ci ha visti impegnati nell'analisi e successiva fase operativa legata a due importati questioni sul piano della protezione dei dati personali, torniamo a proporvi la nostra consueta rassegna.

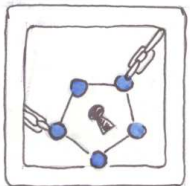
La prima grande questione estiva è legata all'approvazione del Data Privacy Framework che rende leciti i trasferimenti dei dati personali dei cittadini europei verso gli USA, sbloccando, di fatto, una situazione rimasta congelata per oltre tre anni e che ha creato non pochi grattacapi alle aziende e ai consulenti.

Certamente questa novità permette di tirare un sospiro di sollievo, soprattutto considerando quanto il mercato informatico sia fortemente permeato da prodotti americani per i quali non pare vi siano adeguati analoghi europei. Tuttavia, raccomandiamo prudenza nelle decisioni aziendali, dal momento che la storia insegna come, da un giorno all'altro, una decisione di adeguatezza possa trasformarsi nel suo opposto rimettendo tutto in discussione.

La seconda importante novità è invece relativa al D.Lgs. 24/2023 attuativo della Direttiva Europea 2019/1937 in materia di Whistleblowing e il conseguente adeguamento della protezione dei dati personali degli interessati da parte di moltissime aziende non più solamente pubbliche, bensì anche private qualora rientrino nei criteri stabiliti dalla norma e dei quali vi metteremo a parte nel secondo articolo di questa nuova newsletter.

La rassegna prosegue poi con una serie di articoli relativi alla verifica dei Responsabili del Trattamento ai quali vengono affidati i dati, sul controllo a distanza dei lavoratori e sulle modalità illecite e corrette di comunicazioni commerciali, elementi sempre più di rilievo nei controlli del garante.

Lo staff di Pentha vi augura buona lettura.



Secondo la commissione UE gli USA garantiscono misure di sicurezza adeguate alla protezione dei dati dei cittadini europei

Data Privacy Framework - trasferimento dati negli USA: evoluzione della problematica

La Commissione Europea ha ufficialmente approvato il "EU-US Data Privacy Framework", vale a dire il nuovo accordo che disciplina il trasferimento dei dati verso gli Stati Uniti e ne ripristina, pertanto, la condizione di legittimità.

Di fatto, dopo l'invalidazione dei due accordi precedenti, Safe Harbor e Privacy Shield, Bruxelles ha formalmente riconosciuto che gli elementi contenuti nel nuovo DPF (Data Privacy Framework) offrono sufficienti garanzie per la protezione dei dati personali dei cittadini dell'Unione Europea trattati negli Stati Uniti, oltreché tutele legali che limitano l'operato delle agenzie di intelligence americane.

Si chiude così, almeno temporaneamente, una situazione di incertezza giuridica che si protraeva da tre anni, gravando su aziende e pubbliche amministrazioni utilizzatrici di servizi digitali USA (Amazon, Google, ecc.).

Nell'accogliere la notizia con un sospiro di sollievo, non bisogna, però, dimenticare che nel maggio scorso lo stesso Parlamento Europeo aveva giudicato le misure statunitensi insufficienti per garantire la protezione dei dati degli europei invitando la Commissione europea a riaprire i negoziati, e che sono già pronti diversi modelli di ricorso alla Corte di Giustizia europea messi a disposizione di chi ne faccia richiesta, dall'associazione no-profit Noyb.

Ricordiamo che Noyb è un'organizzazione fondata dall'attivista Max Schrems, noto per le due sentenze della suprema Corte europea che portano il suo nome, le quali avevano invalidato i due precedenti sopra citati accordi sul trasferimento dei dati verso gli Stati Uniti d'America.

Non essendo, quindi, chiaro se e quanto a lungo questa decisione di adeguatezza potrà reggere, suggeriamo a chi avesse adottato soluzioni alternative ai prodotti/servizi americani di non abbandonarli.

Coloro che, invece, adottano e intendano mantenere strumenti targati USA devono verificare che le aziende fornitrici americane (e i loro sub responsabili) siano presenti nel data base che si trova al link Data Privacy Framework List dal quale risulti attiva la certificazione/autocertificazione di conformità al nuovo quadro sulla privacy, la relativa scadenza e per quale tipologia di servizi, e, soprattutto, per quali finalità il DPF è attivo.

Inoltre, sarà importante adeguare le informative rese agli interessati sulla presenza di eventuali trasferimenti di dati verso gli USA e la relativa base giuridica.

Fonte: Pentha S.r.l.

D.Lgs. 24/2023 Whistleblowing - adeguamento privacy essenziali

Il 30 marzo 2023 è entrato in vigore il D. Lgs. 24/2023 attuativo della Direttiva Europea 2019/1937 in materia di whistleblowing.

Nuove regole per la segnalazione degli illeciti

In sintesi, la normativa prevede che siano istituiti dei canali per accogliere eventuali notizie di illeciti segnalati da dipendenti subordinati, collaboratori e tirocinanti, liberi professionisti, persone in fase di selezione o in periodo di prova, ex dipendenti (qualora siano venuti a conoscenza di violazioni durante il periodo lavorativo), parenti delle persone interne al contesto lavorativo ed enti che siano operativi nel medesimo contesto lavorativo.

Le violazioni, intese come comportamenti, atti ed omissioni di disposizioni normative sia nazionali che dell'Unione Europea dalle quali possa derivare un danno all'interesse pubblico e all'integrità dell'amministrazione pubblica o dell'ente privato, devono, inoltre, poter essere rese note a mezzo di segnalazioni interne o esterne a personale formato e specificamente autorizzato al trattamento di questo tipo di dati, o, se del caso, tramite divulgazione pubblica.

Le segnalazioni possono essere fatte sia in forma scritta (anche con canali telematici) che orale e il Titolare del Trattamento è tenuto a rendere noti tutti i canali di segnalazione in modo chiaro e trasparente.

Entro le rispettive scadenze, i soggetti interessati dovranno, pertanto, adottare canali di segnalazione ed adeguare le procedure interne, con effetti scaglionati e con le seguenti distinzioni:

- A decorrere dal 15 luglio 2023 per tutti i soggetti pubblici e gli enti privati che hanno impiegato una media di 250 lavoratori subordinati (con contatti di lavoro a tempo determinato o indeterminato) durante l'anno o che hanno adottato modelli organizzativi in ossequio al D. Lgs 231/2001.;
- A decorrere dal 17 dicembre 2023 per le aziende che invece hanno impiegato una media uguale o superiore a 50 dipendenti durante l'anno.

In ambito privacy, vi sono diverse novità che impattano sulla compliance aziendale in materia di whistleblowing:

1. La protezione del soggetto segnalante, al quale deve essere garantita la riservatezza dell'identità, la protezione da eventuali ritorsioni e fornita specifica informativa;
2. Anche il soggetto segnalato dovrà ricevere una informativa diversa dalla precedente;
3. I dati raccolti dovranno essere conservati per il tempo strettamente necessario alla gestione della segnalazione;
4. È necessario generare una Valutazione d'impatto (DPIA) e aggiornare il Registro dei trattamenti.

I nostri uffici sono a disposizione per la gestione degli aspetti privacy della questione; la procedura per la gestione delle segnalazioni, la scelta dei canali ecc. ricade sull'azienda con il supporto dei propri professionisti di riferimento (ODV, sindaci, legali ecc.), ma vi sarebbe la possibilità, da parte nostra, di coinvolgere i nostri canali esterni, qualora fosse necessario ipotizzare una gestione completa del whistleblowing.

Fonte: Pentha S.r.l.

Il governo della filiera dei responsabili del trattamento rientra nell'accountability del titolare

Quando a trattare i dati del Titolare è un terzo soggetto è necessario controllare in maniera efficace l'attività del Responsabile Esterno

Nell'ambito di un trattamento di dati personali ci troviamo di fronte a quella che possiamo definire una "filiera dei partner" ogni qual volta le varie attività di trattamento di dati vengono effettuate da vari "soggetti privacy". Questa filiera, costituita dall'insieme di soggetti che si relazionano tra loro e che compiono varie attività nell'ambito di un trattamento di dati personali, può essere semplice o anche complessa e stratificata, a seconda di quante titolarità privacy si interpongono nella gestione di un determinato trattamento di dati e a seconda dei particolari rapporti tra essi.

Il Garante privacy con un provvedimento di fine 2022 ha sanzionato una società per essersi dimostrata incapace di controllare efficacemente la filiera dei partner che effettuavano attività di trattamento (in questo caso, per scopi di marketing) per conto della società stessa.

Il GDPR definisce i diversi ruoli dei soggetti che intervengono a vario titolo nella gestione di un trattamento: partendo dal soggetto privacy "protagonista" e sempre presente quando siamo di fronte ad un trattamento di dati, vale a dire il titolare del trattamento (articolo 4), possono poi interporsi responsabili e sub-responsabili del trattamento (articolo 28), contitolari del trattamento (articolo 26) e, infine, autorizzati al trattamento (articolo 4).

Responsabile del trattamento - In particolare, il responsabile del trattamento rappresenta quel soggetto che tratta i dati personali "per conto" del titolare in relazione a taluni trattamenti specificatamente individuati nel contratto (o altro atto giuridico a norma del diritto dell'Ue) che disciplina i rapporti tra titolare e responsabile del trattamento. L'articolo 28, GDPR prevede che il titolare del trattamento «ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato».

Il Considerando n. 81 al GDPR aggiunge che le "garanzie sufficienti" che devono presentare i responsabili del trattamento vanno letti in termini di conoscenza specialistica, affidabilità e risorse, elementi necessari in vista della messa in atto di misure tecniche e organizzative in grado di soddisfare il rispetto della normativa privacy, anche in relazione alla sicurezza del trattamento.

Anche l'Europea Data Protection Board (EDPB) con le **Linee guida n. 7/2020 adottate il 7 luglio 2021** sui concetti di titolare e responsabile del trattamento evidenzia l'essenzialità del processo di selezione dei responsabili e la necessaria contrattualizzazione del rapporto tra i due soggetti.

Il contratto deve vincolare il responsabile al titolare e specificare la materia disciplinata, la durata, la natura e la finalità del trattamento,

il tipo di dati personali oggetto del trattamento e le categorie di interessati coinvolti, gli obblighi e i diritti del titolare del trattamento.

Il contratto deve indicare che il responsabile:

- Tratti i dati personali soltanto su istruzione documentata del titolare;
- Garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (per esempio con nomine a incaricato, ad amministratore di sistema, ad addetto alla videosorveglianza ecc.)
- Adotti tutte le misure tecniche e organizzative richieste dall'articolo 32, GDPR, vale a dire pseudonimizzazione, cifratura, capacità di assicurare riservatezza, integrità, disponibilità, resilienza, ripristino dei dati, procedura di test ed efficacia delle misure adottate, risk assessment (per perdita, distruzione, modifica, divulgazione);
- Tenendo conto della natura del trattamento, assista il titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (in questo contesto può essere importante avere un risk e privacy impact assessment per dimostrare di aver adottato misure tecniche ed organizzative adeguate);
- Assista il titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, GDPR (quindi in relazione alle notifiche di data breach, alle comunicazioni di data breach agli interessati coinvolti, redazione della DPIA) tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile;
- Su scelta del titolare, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati (in partica, il titolare deve comunicare al responsabile la propria politica di data retention e cancellazione);
- Metta a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi e consenta le attività di audit, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato (pertanto il titolare ha il dovere di verificare con audit periodici le "credenziali" del responsabile del trattamento e, di converso, il responsabile ha l'obbligo di consentire l'effettuazione degli audit).

Verifiche ex ante e periodiche sul responsabile del trattamento - In generale, il titolare del trattamento è tenuto a dimostrare, in virtù del principio di accountability, di governare la filiera dei partner di trattamento.

La domanda cruciale è: come lo dimostra concretamente? La dimostrazione del corretto governo della filiera dei partner/fornitori (che poi saranno nominati "responsabili del trattamento") si esplica in momenti diversi.

Infatti, l'attività di verifica su tali soggetti va fatta sia ex ante, vale a dire dal momento della selezione del responsabile del trattamento, sia ex post considerando i controlli periodici effettuati sottoforma di audit sulla gestione dei dati effettuata dal responsabile stesso, che temporalmente vanno svolti lungo tutto il rapporto contrattuale.

Quindi, per verificare fin da subito se il responsabile può essere un soggetto che garantisce un trattamento dei dati compliance privacy, il titolare del trattamento deve procedere con la valutazione, caso per caso, del risk assessment del responsabile/fornitore fin dalla fase della selezione.

Sarebbe utile utilizzare una check-list oppure un questionario da far compilare alla società fornitrice in modo da verificare vari aspetti, che vertono, per esempio:

- Sulla verifica di un corretto "assetto privacy" (presenza, per esempio, dei seguenti documenti: registro dei trattamenti di dati personali, informative privacy, accordi, procedure per la gestione dei data breach o per la gestione dell'esercizio dei diritti degli interessati, policy di data retention);
- Sull'eventuale nomina di un DPO;
- Sulla presenza di misure tecniche ed organizzative e adeguate;
- Sulla verifica della presenza di un approccio privacy by design e by default;
- Sulla verifica di eventuali trasferimenti dati extra-Ue.

Naturalmente sarebbe molto efficace poter effettuare tali verifiche parallelamente all'analisi dell'impianto, se esistente, del Modello 231 e/o all'analisi degli asset concernenti gli obblighi antiriciclaggio.

Dopo tale fase di selezione, se il titolare del trattamento considera idoneo il fornitore sulla base del suo assetto, delle sue comprovate competenze ed esperienze, della sua affidabilità e delle risorse che mette a disposizione dovrebbe innanzitutto documentare tale decisione per poi procedere con la stipula dell'accordo ai sensi dell'articolo 28, GDPR, disciplinante tutti gli elementi sopra descritti.

Poi, come detto, durante il rapporto contrattuale il titolare del trattamento dovrà effettuare un'analisi periodica sull'attività del responsabile del trattamento nominato attraverso degli specifici audit.

Caso sanzionato dal Garante privacy - Il provvedimento sanzionatorio emanato dal Garante privacy anticipato in premessa (di cui al Registro dei provvedimenti n. 349 del 20 ottobre 2022) ci ha dato lo spunto per approfondire fin qui la tematica della filiera dei partner di trattamento e per la sua corretta governance.

La vicenda ha avuto origine dalla segnalazione di un cittadino che ha lamentato la ricezione, via e-mail, di una comunicazione indesiderata proveniente da un indirizzo di posta non direttamente ricollegabile alla società con cui l'interessato aveva avuto dei rapporti (di seguito anche "società X"), ma avente ad oggetto la promozione di prodotti offerti dalla società X stessa.

In realtà, infatti, la mail proveniva da una società di marketing che svolgeva l'attività di promozione dei prodotti della società X, la quale era la committente l'attività promozionale stessa, che, lato privacy, si configurava quale titolare del trattamento. A quest'ultimo riguardo, con riferimento ai ruoli privacy, l'Autorità di controllo nel provvedimento in commento ha ricordato sia le Linee guida dell'EDPB n. 7/2020 sia alcuni suoi provvedimenti dove ha più volte affermato che il committente di una campagna promozionale, indipendentemente dalla materiale raccolta dei dati, deve ritenersi titolare del trattamento avendo in concreto determinato, nella ricorrente prassi relativa a tale settore, le decisioni in ordine alle finalità e ai mezzi essenziali del trattamento stesso.

Il reclamante aveva avanzato una formale richiesta di chiarimenti sul trattamento dei propri dati personali alla società incaricata all'attività di marketing, la quale avrebbe dovuto essere stata nominata responsabile del trattamento ai sensi dell'articolo 28 GDPR dalla società X committente l'attività promozionale (nella fattispecie, la nomina non era stata effettuata).La società di marketing non riscontrava l'interessato, pertanto quest'ultimo inviava un reclamo al Garante privacy dichiarando di non aver mai conferito il consenso alla ricezione della comunicazione promozionale e lamentando il mancato riscontro alla richiesta di esercizio dei diritti di cui agli articoli 15, 17 e 21, GDPR.

L'Autorità di controllo chiedeva informazioni alla società titolare del trattamento, la quale dichiarava la propria estraneità in relazione alla condotta lamentata nel reclamo, precisando che i dati dell'interessato sono risultati presenti nelle liste di contatti di un'altra società di cui la società si avvaleva per la gestione dell'attività di marketing.

La società X sanzionata, ha sottolineato il Garante privacy nel provvedimento in esame, non è stata in grado di comprovare l'adozione di adeguate misure tecniche e organizzative, come richiesto dagli articoli 5, par. 2, e 24 del GDPR, norme che inquadrano le competenze del titolare in un'ottica di responsabilizzazione (accountability) finalizzata a comprovare gli adempimenti effettuati in materia di protezione dei dati personali.

In particolare, il Garante ha considerato il riscontro fornito dalla società indicativo dell'incapacità di controllare efficacemente la filiera dei partner che effettuano attività promozionale a suo vantaggio. Di conseguenza, è stata contestata alla società X la violazione degli articoli 5, par. 2, e 24, GDPR, nonché degli articoli 12, 15, 17 e 21, GDPR, non essendo stata riscontrata, nei termini richiesti, l'istanza di esercizio dei diritti formulata dall'interessato, oltre che la violazione dell'art. 6, par. 1, lett. a), GDPR e dell'articolo 130 del

Codice privacy, in ragione dell'invio all'interessato reclamante di una e-mail promozionale in assenza di un consenso libero, specifico, documentato ed inequivocabile.

Fonte: Il Sole 24 Ore (di Elisa Chizzola)

Quando è lecito controllare la posta elettronica aziendale di un dipendente senza violare la sua privacy?

È necessaria l'adozione di un disciplinare interno che indichi le regole per l'uso di Internet e della posta elettronica.

Si tratta di un tema che rimane sempre di grande attualità e di ampio contrasto tra gli addetti ai lavori rispetto al quale si richiama il **Provvedimento generale dell'Autorità Garante per la protezione dei dati personali del 1° marzo 2007** che per quanto datato è ancora valido laddove conforme al Regolamento europeo sulla protezione dei dati n. 2016/679 (GDPR), nonché la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'art. 8, Convenzione europea dei diritti dell'uomo.

Non poche, poi, sono le questioni sorte in merito alla legittimità dell'accesso da parte del datore di lavoro o dirigente alla casella di posta elettronica aziendale del dipendente.

Al fine di risolvere tali questioni è opportuno ricordare alcuni importanti concetti:

- L'equiparazione della posta elettronica alla corrispondenza tradizionale la cui libertà e segretezza viene tutelata dall'art. 15 della Costituzione;
- La legittimità del controllo della casella della posta elettronica del proprio dipendente da parte del datore di lavoro alla luce di quanto prescritto dall'attuale disciplina in tema di rapporti di lavoro, compreso lo Statuto dei lavoratori;
- La tutela della privacy alla luce di quanto stabilito dal GDPR.

La problematica non è semplice e il Garante alla luce dei principi di cui sopra è intervenuto già da tempo con un Provvedimento nel quale ha chiarito che i datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali.

Spetta al datore di lavoro definire le modalità d'uso di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali.

Ma cosa succede nel caso di messaggi inerenti al rapporto di lavoro? Anche in questo caso opera il divieto di controllo?

L'Autorità prescrive innanzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Il Garante vieta poi la lettura e la registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori (art. 4).

Viene inoltre indicata tutta una serie di misure tecnologiche e organizzative per prevenire la possibilità, prevista solo in casi limitatissimi, dell'analisi del contenuto della navigazione in Internet e

dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'azienda.

Il Provvedimento raccomanda l'adozione da parte delle aziende di un disciplinare interno, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica.

Il datore di lavoro è inoltre chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre controlli successivi sui lavoratori. Per quanto riguarda Internet è opportuno ad esempio:

- Individuare preventivamente i siti considerati correlati o meno con la prestazione lavorativa;
- Utilizzare filtri che prevengano determinate operazioni, quali l'accesso a siti inseriti in una sorta di black list o il download di file musicali o multimediali.
- PER quanto riguarda la posta elettronica, è opportuno che l'azienda:
- Renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;
- Valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;
- Preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi;
- Metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.

Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro devono essere effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.

Il Garante della Privacy ha chiesto infine particolari misure di tutela in quelle realtà lavorative dove debba essere rispettato il segreto professionale garantito ad alcune categorie, come ad esempio i giornalisti.

Con riferimento allo Statuto dei lavoratori va ricordato, però, che la giurisprudenza della Corte di Cassazione già da un po' di tempo ha iniziato a rivedere l'applicazione dell'art. 4.

Difatti, con sentenza n. 4746 del 2002 la Cassazione ha escluso l'applicabilità di detto articolo ai controlli diretti ad accertare condotte illecite del lavoratore, i c.d. controlli difensivi.

Il ragionamento della Corte, in tal senso, è chiaro: "Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 l. n. 300 citata, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o gli apparecchi di rilevazione di telefonate ingiustificate.

Successivamente, con la pronuncia n. 15892 del 2007, la Corte ha tuttavia ammesso un limite, affermando che i controlli difensivi non possono giustificare l'annullamento di ogni garanzia: "Né l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore".

Inoltre, più di recente, la stessa Corte di Cassazione con la sentenza n. 22662 dell'8 novembre 2016, ha affermato che "in tema di controllo del lavoratore, le garanzie procedurali imposte dall'art. 4, secondo comma, legge n. 300/1970, per l'installazione di impianti e apparecchiature di controllo, richiesti da esigenze organizzative e produttive, ovvero dalla sicurezza del lavoro, dai quali derivi la possibilità di verifica a distanza dell'attività dei lavoratori, trovano applicazione ai controlli, c.d. difensivi, diretti ad accertare comportamenti illeciti dei lavoratori, quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso.

Fonte: Federprivacy (Michele Iaselli – Coordinatore del Comitato Scientifico di Federprivacy)

Videosorveglianza nei luoghi di lavoro: il legittimo interesse deve essere adeguatamente documentato

Se la videosorveglianza è utilizzata per esigenze di sicurezza, il legittimo interesse deve essere documentato

All'esito dell'attività ispettiva condotta da parte dell'Autorità Garante per la protezione dei dati personali iniziata nel 2021, l'ambito della videosorveglianza ha registrato un rilevante numero di non conformità per lo più riconducibili a trasparenza, liceità e limitazione della conservazione

Per quanto riguarda il profilo di liceità è infatti bene ricordare che per un'organizzazione con lavoratori al proprio interno, l'aspetto della protezione dei dati personali incontra anche le tutele giuslavoristiche previste dall'art. 4 dello Statuto dei Lavoratori (L. 300/1970). Dunque, l'installazione di un sistema di videosorveglianza può avvenire per rispondere ad esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale "previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali" e, in mancanza, con autorizzazione da parte della sede territoriale dell'Ispettorato nazionale del lavoro.

La base più diffusa per il trattamento dei dati personali attraverso i sistemi di videosorveglianza negli ambienti di lavoro consiste nel legittimo interesse (art. 6 par. 1 lett, f) GDPR) che deve essere adeguatamente documentato e può consistere solamente in una (o più) delle ipotesi indicate dal citato articolo 4 dal momento che c'è un'espressa previsione normativa che esclude la legittimità di perseguire altri interessi. Il Purpose test, primo passaggio della valutazione di legittimo interesse (o LIA – Legitimate Interest Assessment), si può esaurire identificando l'interesse perseguito selezionandone uno di quelli indicati dalla norma e - in ottica di rendicontazione – fare riferimento al contesto concreto ed attuale e non a mere dichiarazioni generiche o di principio.

Per quanto riguarda invece lo svolgimento del secondo e del terzo passaggio, ovverosia il Necessity test e il Balancing test, sarà bene tenere conto, dell'area videosorvegliata e della sua effettiva rispondenza rispetto agli scopi dichiarati, nonché dalla quantità e tipologia di informazioni che è possibile raccogliere sugli interessati. È bene inoltre individuare anche le categorie di interessati coinvolti nelle ipotesi in cui siano ripresi soggetti ulteriori rispetto ai lavoratori (ad es. ambienti di lavoro frequentati anche da soggetti esterni). All'interno di tale valutazione è buona prassi e risponde al rispetto dei principi di privacy by design rendicontare anche le modalità operative in cui si garantiscono gli adempimenti indicati dal Garante all'interno del Provvedimento in materia di videosorveglianza - 8 aprile 2010.

Per dare evidenza al rispetto del principio di liceità il documento della valutazione del legittimo interesse assume un ruolo fondamentale, e va allegato alla proposta di accordo sindacale o altrimenti all'istanza da presentare presso l'ispettorato del lavoro. Qualora infine venga riscontato un rischio elevato per gli interessati, o si rientri nell'ipotesi di cui al punto 5 dell'allegato 1 al

provvedimento n. 467 dell'11 ottobre 2018, sarà necessario anche lo svolgimento di una valutazione d'impatto e l'allegazione della medesima

Fonte: Federprivacy (Stefano Gazzella – Delegato Federprivacy per la provincia di Gorizia)

Il Garante privacy bacchetta www.trovanumeri.com: stop agli elenchi telefonici formati tramite web scraping

È vietato creare elenchi telefonici non estratti dal DBU

Il Garante privacy ha vietato al titolare del sito web "www.trovanumeri.com" la costituzione e diffusione on line di un elenco telefonico formato "rastrellando" i dati tramite web scraping (ricerca automatizzata nel web) e gli ha ingiunto il pagamento di una sanzione di 60 mila euro. L'attuale quadro normativo non consente infatti la creazione di elenchi telefonici generici che non siano estratti dal DBU, il data base unico che contiene i numeri telefonici e i dati identificativi dei clienti di tutti gli operatori nazionali di telefonia fissa e mobile.

Numerosissime sono state in questi anni le richieste di intervento ricevute dal Garante relative alla pubblicazione non autorizzata di nominativi, indirizzi, numeri di telefono, anche di titolari di utenze riservate.

Dagli accertamenti dell'Autorità è emerso che il titolare del sito non aveva un'idonea base normativa per trattare i dati, che sul sito mancavano le indicazioni per rivolgersi al titolare del trattamento come pure assente risultava la possibilità di ottenere la cancellazione dei dati in caso di mancato funzionamento dell'apposito form. Anche nella breve informativa privacy pubblicata, non era indicato l'intestatario del sito, la cui identificazione ha richiesto lunghe indagini.

Il Garante ha dichiarato dunque illecita la raccolta, la conservazione e la pubblicazione dei dati personali ed ha comminato una sanzione di 60 mila euro. La ditta individuale aveva già subito una sanzione nel 2022 per una violazione analoga.

Nel definire l'ammontare dell'ammenda l'Autorità ha tenuto conto della gravità della violazione, dell'elevato numero di soggetti i cui dati sono stati pubblicati (circa 26 milioni di utenti), della durata della violazione e del carattere doloso della condotta dell'intestatario.

Quale unico elemento attenuante, il Garante ha considerato le dimensioni economiche del titolare, che riveste la qualifica di piccolo imprenditore.

Fonte: Garante Privacy

Soft spam: sì all'invio di proposte senza consenso ma solo tramite email a chi è già cliente

È possibile inviare proposte commerciali senza consenso solo tramite posta elettronica e per prodotti analoghi a quelli già acquistati dal cliente

Soft spam, senza consenso, ma solo per le e-mail. La normativa Ue sul marketing elettronico, risalente al lontano 2002, ammette l'invio di proposte commerciali, senza consenso, a chi è già cliente, limitatamente a prodotti analoghi, ma solo se si usa la posta elettronica. Per tutti gli altri mezzi di comunicazione elettronica, ci vuole il consenso preventivo. La regola, introdotta oltre venti anni fa, continua ad essere vigente così come è stata varata.

Tanto che il Garante della privacy (provvedimento n. 9 dell'11/1/2023) ha ammonito una società che gestisce una piattaforma di annunci on line: la sanzione pecuniaria non è scattata solo perché in concreto la società ha fatto e-mail e non altro. Resta, però, un andamento normativo a zig zag: si pensi, ad esempio, che per il marketing telefonico non ci vuole il consenso, applicandosi il registro delle opposizioni (ispirato all'opt out).

Nel medesimo provvedimento c'è, poi, la conferma della necessità, in caso di cessione di liste telefoniche, di rendere noti agli interessati (possessori delle numerazioni) le denominazioni (non la categoria) dei destinatari. Ma vediamo di illustrare le questioni.

Soft Spam - La direttiva Ue 2002/58 (articolo 13), recepita dall'articolo 130 del codice della privacy (decreto legislativo 196/2003), ammette il soft spam: non ci vuole un consenso preventivo per usare, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di prodotti o servizi, purché analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni (nel corso delle quali deve essere ripetuto l'avviso sulla possibilità di opporsi in ogni momento, in maniera agevole e gratuitamente). La e-mail, dunque, nei limiti indicati, si può fare senza consenso. E anche una telefonata, rispettando i paletti del registro delle opposizioni (legge 5/2018).

Per altri mezzi di comunicazione automatizzati ci vuole il consenso preventivo. Resta da capire cosa possa fare la differenza tra e-mail e altri tipi di messaggi elettronici, ma allo stato così è. E, anzi, va segnalata la sensibilità del Garante della privacy, che ha considerato la buona fede dell'operatore e si è limitato a una censura formale (ammonimento), senza sanzione pecuniaria.

Disclosure - Un articolo della legge 5/2018 sul telemarketing impone che, in caso di cessione a terzi di liste di numerazioni telefoniche, agli interessati siano comunicati gli estremi identificativi dei soggetti a cui i dati sono trasferiti. Qui il problema è se si possa dare notizia delle categorie di destinatari (che possono essere tantissimi) o se bisogna dare i nomi precisi di ciascuno. Nel provvedimento citato il Garante prende atto del fatto che la legge del 2018 impone l'obbligo di indicare "la denominazione specifica" dei destinatari. Anche per

questo profilo, la piattaforma coinvolta nella vicenda ha tratto vantaggio dalla correttezza dimostrata e ha rimediato un ammonimento (senza strascichi pecuniari).

Contratti - Se un operatore trasmette dati a terzi, che utilizzano tali dati per finalità promozionali, e se questi ultimi li usano per arricchire una propria banca dati o per svolgere attività promozionale per conto di propri committenti, allora tutti sono autonomi titolari del trattamento. Per questi casi il Garante ritiene che occorra inserire nei contratti apposite clausole di qualificazione dei ruoli come autonomi titolari. Il Gdpr non prevede espressamente clausole contrattuali tra titolari autonomi: prevale, però, l'esigenza di chiarezza sostanziale. Anche in questo caso la correttezza dimostrata dall'operatore economico ha scongiurato un'ingiunzione di pagamento.

Consensi - Nel provvedimento in esame il Garante ribadisce che il consenso dell'interessato alla cessione di dati a terzi per finalità promozionale vale solo nei confronti del primo acquirente e non è valido per i successivi trasferimenti.

Fonte: Fonte: Italia Oggi del 14 marzo 2023 (di Antonio Ciccio Messina)

Pentha Memo…

Memorandum sulle scadenze privacy, iniziative, eventi e servizi curati da Pentha e dalla rete di collaboratori (non è quindi esaustivo di tutti gli adempimenti contabili, fiscali, previdenziali e societari obbligatori).

Per ulteriori informazioni siamo a completa disposizione ai recapiti in calce.

Data	Da stabilire in base alle esigenze del cliente
On demand	Corsi di formazione sul Regolamento Europeo Gdpr 2016/679

Le sanzioni del GDPR

Riepilogo di alcune fattispecie di violazione riscontrate dai garanti europei e relativi provvedimenti sanzionatori dopo l'introduzione del GDPR 2016/679

Riportiamo, nella tabella che segue, una selezione di violazioni e contestazioni effettuate dal garante italiano o da quelli di altri paesi europei, con l'indicazione della relativa sanzione applicata all'ambito di attività del destinatario al fine di fornire indicazioni utili, ancorché non precise e/o senza garanzia che sarebbero ugualmente replicabili in casi analoghi, ma significative per valutare l'impatto di una eventuale violazione simile.

Sono state volutamente tralasciate le sanzioni applicate a BIG DATA (Google, Amazon, Facebook ecc.) e alle aziende multiutility (telefoniche, gas ecc.) in quanto difficilmente ripetibili e applicabili alle piccole e medie realtà nazionali.

TIPOLOGIA VIOLAZIONE	*SANZIONE PECUNIARIA*	*SANZIONE ACCESSORIA*	*DESTINATARIO*	*ANNO*
Controllo illecito sulla navigazione Internet dei dipendenti	84.000,00 €		Comune di Bolzano	2021
Mancata o tardiva nomina del Data Protection Officer (DPO)	75.000,00 €		Ministero delle finanze (MEF)	2021
Accesso indiscriminato e ingiustificato a dati sanitari	400.000,00 €		Ospedale portoghese	2020
Misure di sicurezza insufficienti	460.000,00 €		Ospedale olandese	2020
Inidonea o omessa informativa per finalità commerciali	200.000,00 €		Azienda polacca	2020
Errata base giuridica (consenso per raccolta dati nei rapporti di lavoro)	150.000,00 €		Azienda greca	2020
Misure di sicurezza insufficienti	50.000,00 €		Associazione Rousseau (M5S)	2020
Diffusione illecita di dati	30.000,00 €		Università italiana	2020
Accesso illecito a dati sanitari	30.000,00 €		Ospedale italiano	2020

TIPOLOGIA VIOLAZIONE	SANZIONE PECUNIARIA	SANZIONE ACCESSORIA	DESTINATARIO	ANNO
Diffusione illecita dati personali	10.000,00 €		Comune italiano	2020
Marketing aggressivo	200.000,00 €		Call Center italiano	2020
Diffusione di dati di c.v.	80.000,00 €		Ospedale Cardarelli Napoli	2020
Gestione errata procedure di whistleblowing	30.000,00 €		Università italiana	2020
Comunicazione illecita di dati personali particolari	20.000,00 €		Università italiana	2020
Comunicazione illecita di dati personali per bugs software FSE	150.000,00 €		ASL (con rischio di ribaltamento sanzione ai produttori del sw)	mag-21
Mancato oscuramento dati nel FSE	190.000,00 €		ASL (con rischio di ribaltamento sanzione ai produttori del sw)	giu-21
Mancata esposizione cartelli videosorveglianza	3.000,00 €		Piccolo Hotel (sanzione parametrata sul fatturato)	nov-20
Poca sicurezza nel software utilizzato e mancata nomina di sub responsabili del trattamento	20.000,00 €		Fornitore software segnalazioni Whistleblowing	lug-21
Violazione norme sui cookies	50.000,00 €		Giornale Le Figaro	ago-21
Mancata nomina di responsabili/sub responsabili	800.000,00 €	al titolare	Roma capitale	lug-21
Mancata nomina di responsabili/sub responsabili	400.000,00 €	al responsabile	ATAC spa	lug-21
Mancata nomina di responsabili/sub responsabili	30.000,00 €	al sub responsabile	Flow Bird	lug-21
Chiamate promozionali illecite (anche per acquisizione liste dati da altre società)	3.200.000,00 €		Sky Italia	ott-21
Diffusione illecita di dati personali (prescrizioni agli assistiti appese fuori dallo studio con mollette da bucato)	10.000,00 €	Pubblicazione sul sito del Garante	Medico MMG italiano	nov-21
Nomina DPO inadeguato	18.000,00 €		Azienda Lussemburghese	nov-21
Data breach a seguito di misure di sicurezza deboli	400.000,00 €		Vettore aereo olanda	nov-21
Mancata denuncia di possibile data breach (anche se poi non si è verificato) a seguito di smarrimento di un plico contenente dati personali spedito a mezzo corriere	87.000,00 €		Banca polacca	nov-21
Impedimento all'esercizio dei diritti dell'interessato, mancato riscontro alle richieste dell'interessato	150.000,00 €		Tim	dic-21
Registrazione telefonate assistenza clienti in assenza di informativa e accordo sindacale	30.000,00 €		Società di trasporto pubblico	dic-21
Utilizzo indebito dei dati dei dipendenti (finalità non dichiarate nell'informativa)	400.000,00 €		Società trasporto metropolitano francese	nov-21

TIPOLOGIA VIOLAZIONE	SANZIONE PECUNIARIA	SANZIONE ACCESSORIA	DESTINATARIO	ANNO
Dati dei dipendenti "dimenticati" su un vecchio server on line e non protetto		In via di definizione	Società trasporto metropolitano francese	dic-21
Telemarketing aggressivo	26.500,00 €		Enel Energia	gen-22
Misure di sicurezza insufficienti che hanno comportato la sottrazione e la diffusione di dati particolari	7.000,00 €		Fornitore IT (nominato REDT) di una casa di riposo italiana	dic-21
Telemarketing aggressivo: mancata nomina e vigilanza sulla catena degli appaltatori	400.000,00 €		Titolare del trattamento	feb-22
Telemarketing aggressivo: mancata nomina e vigilanza sulla catena degli appaltatori	200.000,00 €		Responsabile del trattamento (call center)	feb-22
Telemarketing aggressivo: mancata nomina e vigilanza sulla catena degli appaltatori	90.000,00 €		Sub responsabile del trattamento (che non ha risposto al Garante)	feb-22
Informativa inidonea (basi giuridiche e data retention non corrette)	7.500,00 €	Pubblicazione sul sito del Garante	ASL Frosinone	gen-22
Sistematica richiesta della fotocopia carte di identità ai propri clienti quale presupposto per esercitare i diritti dell'interessato	525.000,00 €		Società editoriale olandese	mar-22
Consenso per finalità di marketing "estorto" all'interessato e caselle pre-flaggate	2.100.000,00 €		Banca Spagnola	mar-22
Richiesta casellario giudiziale senza averne motivo	2.000.000,00 €		Amazon	feb-22
Telemarketing a numeri reperiti in rete	5.000,00 €		Agenzia immobiliare affiliata Tecnocasa	apr-22
Richiesta sproporzionata di dati per accedere al proprio account (richiesta copia bolletta luce per accedere al proprio profilo su società interinale)	240.000,00 €		Michael Page società interinale	apr-22
Discriminazione su cittadini presunti evasori fiscali	500.000,00 €		Agenzia entrate olandese	apr-22
Discriminazione su cittadini presunti evasori fiscali	2.750.000,00 €		Agenzia entrate olandese	apr-22
Riprese con telecamere di aree non di pertinenza del titolare e assenza di cartelli informativi	2.000,00 €		Circolo ricreativo privato	apr-22
Rilevazione temperatura e questionari COVID senza corretta base giuridica	200.000,00 €		Aeroporto Bruxelles	apr-22
Rilevazione temperatura e questionari COVID senza corretta base giuridica	100.000,00 €		Aeroporto Bruxelles sud	apr-22
Rilevazione temperatura e questionari COVID senza corretta base giuridica	20.000,00 €		Società che somministrava questionari	apr-22
Errata configurazione del software del whistleblowing.	40.000,00 €		Società informatica	mag-22
Mancata consegna dell'informativa ai lavoratori, mancata redazione della DPIA, trattamento non inserito del registro delle attività.	40.000,00 €		Azienda ospedaliera	mag-22
Inviso SMS di sollecito crediti al coniuge di un cliente	10.000,00 €		Finanziaria	mag-22

TIPOLOGIA VIOLAZIONE	SANZIONE PECUNIARIA	SANZIONE ACCESSORIA	DESTINATARIO	ANNO
Profilazione con informativa generica e profilazione senza consenso, mancata notifica di un data breach	2.120.000,00 €		Uber	mag-22
Violazione di un sistema informatico per scarse misure di sicurezza e software non concepito "privacy by design"	10.000,00 €	Pubblicazione sul sito del Garante	Brav s.r.l.	mar-22
Data breach riguardante dati sanitari (HIV, patologie ecc.), inadempienze nelle nomine art. 28, carenze misure di sicurezza art. 32	1.500.000,00 €		Dedalus (società francese)	feb-22
Fototrappola per documentare illeciti nel deposito di rifiuti	150.000,00 €		Comune di Taranto	apr-22
Fototrappola per documentare illeciti nel deposito di rifiuti	200.000,00 €		Gestore del servizio rifiuti	apr-22
Accesso illecito a dati personali, anche particolari, in occasione di tre mini data breach (il numero delle consultazioni riguarda 8 interessati)	50.000,00 €	Pubblicazione sul sito del Garante	INAIL	mag-22
Utilizzo di cookies analitici e di profilazione con trasferimento dati in USA		Ammonimento e 90 giorni per adeguarsi	Caffeina magazine s.r.l.	giu-22
Mancato riscontro alle richieste del garante: impianto di videosorveglianza non autorizzato e senza informative	15.000,00 €	Pubblicazione sul sito del Garante	Rebirth s.r.l. gestione di un bar	apr-22
Pubblicazione e utilizzo di numeri di telefono e nominativi non attinti dal DBU	50.000,00 €		Ditta individuale	giu-22
Mancato riscontro a richiesta dell'interessato (società telemarketing)	20.000,00 €	Pubblicazione sul sito del Garante	Società italiana	giu-22
Nomina di un DPO in conflitto di interessi con il titolare	6.000,00 €		Comune italiano	giu-22
Eccesso di "trasparenza amministrativa" – pubblicazione di dati eccedenti quelli minimi richiesti	46.000,00 €		ASL Roma 1	giu-22
Comunicazione di dati personali a persona diversa dall'interessato sui si riferiscono	100.000,00 €		Banca Intesa San Paolo	giu-22
Pubblicazione dati eccedenti di un CV nella sezione trasparenza	10.000,00 €		Comune italiano	lug-22
Invio di una mail con in cc tutti i destinatari	1.500,00 €		Scuola italiana	lug-22
Accessi abusivi al dossier sanitario dei pazienti	50.000,00 €	60 giorni di tempo per adeguare il sistema informatico	Asl FVG	lug-22
Accessi abusivi al dossier sanitario dei pazienti	70.000,00 €	60 giorni di tempo per adeguare il sistema informatico	Asl FVG	lug-22
Profilazione esagerata degli utenti e clienti di una banca tedesca (informativa privacy di 28 pagine!)	900.000,00 €		Hannoversche Volksbank	ago-22
Comunicazione di dati particolari di un paziente ad altri 2000 destinatari, assenza di protezione sulle refertazioni allegate alle mail	202.000,00 €		Azienda farmaceutica inglese	ago-22

TIPOLOGIA VIOLAZIONE	SANZIONE PECUNIARIA	SANZIONE ACCESSORIA	DESTINATARIO	ANNO
Destinatari di posta elettronica in chiaro anziché in CCN (APP diabetici)	45.000,00 €		Società statunitense	lug-22
Impianto videosorveglianza installato senza informative e con angoli di ripresa su aree private	2.000,00 €	Ingiunzione con prescrizioni	Negozio italiano	lug-22
Errore tecnico configurazione applicazione che ha comportato un piccolo data breach (500 interessati)	2.000,00 €		Banca Rumena	ott-22
SMS con operazioni bancarie inviati a destinatari errati (44 operazioni in totale)	2.000,00 €		Banca Rumena	ott-22
Comunicazione di dati personali (4 interessati) a destinatari sbagliati	1.000,00 €		Banca Rumena	ott-22
Invio messaggi pubblicitari a destinatario che si era opposto a comunicazioni commerciali	42.000,00 €		Banca Spagnola	ott-22
Invio dati correntista con relativo portafoglio a cliente sbagliato	56.000,00 €		Banca Spagnola	ott-22
Pubblicazione dati disabili partecipanti ad un concorso	20.000,00 €		Regione Abruzzo	ott-22
Dati non aggiornati: comunicazione inviata a persona deceduta nel 1995 (diritto esercitato da eredi)	100.000,00 €		Regione Lazio	ott-22
Invio newsletter senza consenso (anche con proposte di terzi) a destinatari di diversi paesi UE	600.000,00 €	In applicazione del OSS tramite CNIL	HaccorHotels	ago-22
Nomina DPO in conflitto di interessi	525.000,00 €		Azienda di e-commerce tedesca	set-22
Smarrimento copie cartacee fascicoli studenti	Ammonimento		Università italiana	set-22
Nomina DPO in conflitto di interessi (amministratore di società del gruppo)	Sanzione non trovata sul Web		Società tedesca	ott-22
Nomina DPO in conflitto di interessi (dirigente interno)	75.000,00 €		Banca belga	ott-22
Nomina DPO in conflitto di interessi (avvocato e membro del CDA)	Stop alla nomina		Azienda islandese	ott-22
Utilizzo di dati presi da registri pubblici per attività di marketing	50.000,00 €		Agente immobiliare	ott-22
Utilizzo di dati presi da registri pubblici per attività di marketing	5.000,00 €		Geometra che "passava" i dati all'agente	ott-22
Ras ha tenuto nascosto un data breach avvenuto nel 2016	8 anni carcere (rischio secondo la legge USA)		Amministratore di sistema di Uber	ott-22
Installazione rilevatori biometrici non autorizzati per la rilevazione presenze	"modesta sanzione" in quanto all'arrivo degli ispettori il dispositivo era stato disinstallato		Azienda italiana	ott-22

TIPOLOGIA VIOLAZIONE	SANZIONE PECUNIARIA	SANZIONE ACCESSORIA	DESTINATARIO	ANNO
Zia ha pubblicato foto dei nipotini senza consenso dei genitori	5.000,00 €		Persona fisica (parente dell'interessato)	ott-22
Geolocalizzazione utenti senza un consenso ed una corretta informazione (azione congiunta di 40 stati federati USA)	392 milioni di dollari		Google	ott-22
Pubblicazione di dati eccedenti rispetto alla finalità perseguita (dati del CV e permanenza on line)	10.000,00 €		Comune italiano	nov-22
Utilizzo di dispositivi indossabili (occhiali) per riconoscimento facciale e targhe		Stop all'utilizzo e richiesta di maggiori informazioni	Comune di Lecce e comune di Arezzo	nov-22
Rilevazione presenze dipendenti tramite impronte digitali	20.000,00 €		Società sportiva	dic-22
Controllo illecito sulla navigazione Internet dei dipendenti	100.000,00 €		Regione Lazio	dic-22
Cyberbullismo e revenge porn	5.000,00 €		Sedicenne spagnolo	dic-22
Dark pattern e trattamento illecito dati di minori (sanzione secondo le norme USA)	520 milioni di dollari	Restituzione acquisti indotti da dark pattern	Epic Games (USA)	dic-22
Informative privacy e cookies mischiate, elenco di trattamenti più ampio di quelli effettivamenti svolti, mancata cancellazione di dati obsoleti	1.400.000,00 €		Douglas Italia	nov-22
Messaggi incomprensibili (velocità di lettura troppo elevata con tanto di conteggio delle parole per minuto) e contatti promozionali indesiderati a fasce deboli (anziani)	500.000,00 €		Vodafone Italia	nov-22
Rimozione dei blocchi per l'accesso a dati sanitari ed istituzione di dossier sanitari senza consenso	40.000,00 €		ASL Valle d'Aosta	nov-22
Diffusione su internet di dati degli utenti (circa 533 milioni di utenti)	265 milioni di Euro		Meta (Facebook, Instagram, Whatsapp)	nov-22
Furto di dati con tecnica del phishing a causa di scarsa attenzione di un dipendente e misure di sicurezza deboli	5,1 milioni di Euro		Azienda Inglese	nov-22
Utilizzo di dati per marketing e profilazione senza consenso specifico, condivisione di dati senza inforamtiva e consenso	2 milioni di Euro	Obbligo di DPIA	Alpha Exploration per social Clubhouse	nov-22
Dati inesatti classificano come morosi utenti di distributore energia elettrica che perdono vantaggi sul libero mercato	1 milione di Euro		Areti - società distributrice energia elettrica	nov-22
Imposizione di installazione cookies a utenti di Bing	60 milioni di Euro (Garante francese)		Microsoft	dic-22
Trattamento illecito dati particolari	4,3 milioni di Euro (Garante portoghese)		Istituto nazionale di statistica	dic-22
Account posta elettronica di un dipendente cessato lasciato attivo	10.000,00 €		Costampress s.p.a.	feb-22
Mancato riscontro richiesta esercizio diritti	6.000,00 €		ASL Caltanissetta	mar-22

TIPOLOGIA VIOLAZIONE	SANZIONE PECUNIARIA	SANZIONE ACCESSORIA	DESTINATARIO	ANNO
Mancato riscontro richiesta esercizio diritti di un dipendente	50.000,00 €		Palumbo Superyacht Ancona s.r.l.	apr-22
Mancato riscontro richiesta esercizio diritti	10.000,00 €		E-Mac Professional	apr-22
Mancato riscontro richiesta esercizio diritti	40.000,00 €		Il sole 24 Ore s.p.a.	apr-22
Mancato riscontro richiesta esercizio diritti	70.000,00 €		Unicredit	giu-22
Mancato riscontro richiesta esercizio diritti	20.000,00 €		Deutsche Bank	giu-22
Invio di comunicazione a liste di destinatari acquistati senza verifiche sugli effettivi consensi	600.000,00 €		EDF	giu-22
Telemarketing senza consultare il registro delle opposizioni inglese	435.000 Sterline		5 società inglesi di telemarketing	gen-23
Geolocalizzazione utenti senza un consenso ed una corretta informazione e utilizzo di dark pattern	9,5 milioni di dollari	Invio comunicazione con istruzioni per disabilitazione geolocalizzazione e cancellazione dati	Google	gen-23
Profilazione degli utenti senza consenso ed invio di pubblicità mirata	8 milioni di Euro (CNIL Francese)		Apple	gen-23
Profilazione degli utenti senza consenso ed invio di pubblicità mirata	390 milioni di Euro		Meta (Facebook, Instagram, Whatsapp)	gen-23
Utilizzo base giuridica errata (consenso anziché esecuzione contratto)	5,5 milioni di Euro		Meta (Whatsapp Ireland)	gen-23
Profilazione non consentita degli utenti, utilizzo di un algoritmo senza informare gli utenti	55.000,00 €		3 ASL friulane, la sanzione è stata applicata ad ogni ASL	gen-23
Profilazione degli utenti anche in caso di rifiuto da parte dell'utente	3 milioni di Euro (CNIL Francese)		Voodoo (editor di videogiochi)	gen-23
Cookies difficili da rifiutare e conseguente pubblicità mirata	5 milioni di Euro (CNIL Francese)		Tik Tok	gen-23
Comunicazione di dati eccedenti la finalità perseguita e mancata nomina del DPO	5.000,00 €		Comune di Cisterna di Latina	gen-23
Furto o danneggiamento degli strumenti informatici può comportare la bancarotta semplice documentale in assenza di backup (sentenza della cassazione che esclude la forza maggiore)	-		Impresa italiana	nov-22

Fonte: Pentha s.r.l.

Pentha s.r.l. Servizi Integrati per le Imprese
Via Gobetti, 37 – 12100 Cuneo
Telefono 0171 489095 – Fax 0171 631346
Web www.pentha.eu Mail pentha@pentha.eu

http://www.facebook.com/pages/Pentha-srl-Servizi-Integrati-per-le-imprese/89151469538