

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 |

| | | | | |
|--|----------------|------------------------------------|---|--------|
| 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 |
| 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 |
| 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 | | Ammonizione 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 allegare alle mail | 202.000,00 € | | Azienda farmaceutica inglese | ago-22 |
| 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 | Negoziario 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 |
| 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 | Comune di Lecce e comune di Arezzo | nov-22 |

| | | maggiori informazioni | | |
|--|--|---|---|--------|
| 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 effettivamente 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 informativa 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 |
| 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-impreses/89151469538>