Privacy: Proteggere i dati personali e rispettare le linee guida del Garante

Consapevolezza, la prima fase della sicurezza.

Cari Colleghi,

In questa seconda Newsletter, vogliamo affrontare il tema della protezione dei dati personali necessaria per garantire la sicurezza della nostra Regione.

La privacy e la riservatezza delle informazioni riguardano la capacità di controllare i dati personali (es. nome, cognome, numero di telefono, etc.), i dati finanziari, i dati sanitari e molto altro. Dunque, gestire la privacy in maniera corretta è necessario per evitare che queste informazioni vengano acquisite da criminali informatici. La protezione dei dati personali è una garanzia di liceità che l'Unione Europea, grazie al **Regolamento Generale sulla Protezione dei Dati (GDPR)**, ha deciso di regolamentare nel 2016 per ovviare ad una frammentazione degli Stati Membri in materia. Questo Regolamento impone alle aziende di mantenere un **adeguato livello di sicurezza e riservatezza delle informazioni** da garantire durante la loro attività. Ciò significa che devono adottare misure per proteggere i dati personali dei propri interessati tramite un alto standard di sicurezza e riservatezza.

Dunque, l'obiettivo è fornire informazioni e consigli utili per proteggere i dati in modo semplice e pratico, sulla base degli orientamenti del Garante italiano per la protezione dei dati personali (GDPD).

Le sanzioni del Garante

Il Garante italiano per la protezione dei dati personali, unica autorità italiana che ha il compito di tutelare i diritti fondamentali della persona in materia privacy, durante gli anni ha irrogato molte sanzioni agli enti pubblici per correggere le lacune che gli stessi avevano durante il trattamento dei dati personali dei cittadini. Di seguito riportiamo alcuni esempi:

Il Garante ha multato per 40.000 € **l'Azienda socio sanitaria territoriale nord Milano**. Nel corso dell'indagine, il Garante ha riscontrato che il coniuge di un paziente aveva ricevuto il referto di un test COVID del marito da un dipendente dell'autorità sanitaria **senza autorizzazione**.

Il Comune di Castel Goffredo è stato oggetto di una sanzione di 50.000 € dall'Autorità per **uso illecito delle registrazioni** audio-video di un colloquio intercorso presso il Comando di Polizia Locale.

L'USL Toscana ha subito una sanzione per 100.000 €. Le persone interessate **non sono state informate in modo adeguato** sul periodo di conservazione dei loro dati, sui loro diritti (in particolare i diritti di reclamo e di accesso), sulle modalità di trattamento dei loro dati e sui relativi scopi al momento di dare il consenso al trattamento. Inoltre, l'USL non ha tenuto un registro delle attività di trattamento e **non ha implementato misure tecniche e organizzative** adeguate per proteggere il trattamento dei dati. Infine, non è stata condotta una valutazione d'impatto sulla protezione dei dati (DPIA), nonostante la natura dei dati trattati (dati sanitari) richiedesse tale valutazione.

Il Garante ha multato il **Comune di Roma** per 500.000€ per il trattamento illecito dei dati personali di utenti e dipendenti. Il Comune utilizzava il sistema di prenotazione "TuPassi" per gestire appuntamenti e altri servizi dal 2015. Nel corso di un'indagine dettagliata, il Garante italiano ha riscontrato che il Comune aveva violato diverse norme sulla protezione dei dati in relazione al trattamento dei dati personali dei clienti e dei dipendenti con cui avevano fissato gli appuntamenti. Ad esempio, il Comune **non aveva informato correttamente gli interessati prima di trattare i loro dati**, né aveva adottato **misure tecniche e organizzative adeguate** per proteggere le informazioni in suo possesso.

Il Garante per la per la protezione dei dati personali ha inflitto alla **Regione Lazio** una multa di 75.000€ per non aver designato Capodarco S.r.l, la società a cui aveva affidato la gestione delle prenotazioni per i servizi sanitari nel 1999, come Responsabile del trattamento. La Regione non aveva stipulato con Capodarco S.r.l. un contratto che regolasse il suo ruolo di Responsabile del trattamento dei dati in conformità con i requisiti del GDPR. Pertanto, un contratto adeguato per il trattamento è stato stipulato solo nel 2019, il che significa che i dati **sono stati trattati illegittimamente per** un periodo di **circa 20 anni**.

Il Garante ha multato il **Ministero dello Sviluppo Economico** per 75.000€ per non aver nominato un responsabile della protezione dei dati entro il 28 maggio 2018 e per aver **pubblicato sul proprio sito web i dati personali di oltre cinque mila dirigenti**. L'Autorità ha avviato un'indagine nei confronti del Ministero, dopo aver riscontrato che i dati personali di oltre cinquemila manager, che si erano resi disponibili per consulenze su processi tecnologici e digitali, erano liberamente accessibili sul suo sito web. I dati personali (nome, cognome, codice fiscale, e-mail, curriculum vitae e, in alcuni casi, copia dei documenti di riconoscimento) erano visibili al pubblico e **potevano essere scaricati liberamente**. Sul sito web era anche possibile scaricare la delibera della direzione che aveva approvato l'elenco, che comprendeva i dati e le informazioni di tutti gli amministratori. Il Garante ha ritenuto che il trattamento fosse illegittimo e che la delibera del consiglio di amministrazione citata non costituisse una base giuridica adeguata per la divulgazione dei dati online.

Attraverso le sanzioni, il Garante mira ad infondere consapevolezza agli Enti, data l'estrema importanza dei dati che una Pubblica Amministrazione tratta: in primo luogo, i dati sanitari sono ricompresi nella categoria di dati particolari ex art.9 GDPR, che hanno obblighi più stringenti al fine di garantire la sicurezza delle informazioni di tale rilievo.
In secondo luogo, ricollegandoci alla Newsletter precedente, una minore consapevolezza dei dipendenti e di tutti gli incaricati al trattamento dei dati, fa sì che l'Ente sia **passibile di attacchi informatici** di notevole portata, che causerebbero il congelamento dei servizi essenziali al cittadino.

In ultimo, la confidenzialità, l'integrità e la disponibilità sono i pilastri imprescindibili per una corretta gestione dei dati al fine di non creare un rischio tangibile alla **continuità dei servizi al cittadino** e devono essere garantiti attraverso **misure tecniche ed organizzative adeguate.**

I consigli per la Privacy

Come accennavamo pocanzi, la protezione dei dati personali è un tema di grande rilevanza per garantire la sicurezza dei cittadini. Una guida di regole di buona condotta può essere di grande aiuto per proteggere tali informazioni. Qui di seguito alcune regole di facile attuazione, che tutti i giorni possiamo mettere in pratica durante le nostre attività:

Utilizzate sempre **password robuste** e cambiatele regolarmente. Assicuratevi che le password utilizzate per accedere ai sistemi informatici della Regione siano lunghe, complesse e cambiate regolarmente. Inoltre, evitate di utilizzare la stessa password per più account. Ricordate di non lasciate incustodite le vostre password (es. Post-it attaccati allo schermo, sotto la tastiera).

Assicuratevi di utilizzare servizi online che adottano misure di sicurezza adeguate per proteggere i dati della Regione. Verificate che il sito web sia sicuro, ad esempio attraverso l'utilizzo di un **protocollo "HTTPS"**.

In caso di risposta o inoltro di documentazione tramite mail, posta ordinaria, etc., assicuratevi che questa **non contenga dati personali che non siano pertinenti**, ed eliminate eventuali allegati se non strettamente necessari. Assicuratevi sempre che siano stati inseriti nella mail **solo i destinatari strettamente necessari** ed allegate alla mail solo i documenti strettamente necessari all'elaborazione di una richiesta.

Non parlate di informazioni riferibili alle attività lavorative in luoghi non appropriati (es. macchinette del caffè). **Non diffondete informazioni/notizie esternamente** alla Regione. Coinvolgete nelle riunioni solo il personale interessato. Nel caso in cui si venga a conoscenza di informazioni confidenziali in maniera casuale, non comunicate ad altri tali informazioni.

Tenete sulla vostra scrivania solo **i documenti necessari** a svolgere l'attività di lavoro, mentre tutti gli altri documenti non utilizzati teneteli al sicuro in una stanza, in un armadio o in un cassetto chiuso.

In caso vi assentiate dal lavoro o alla fine della giornata di lavoro, **rimuovete tutti i documenti dalla scrivania** e riponeteli in cassetti ed armadietti. Assicuratevi che tutti gli strumenti elettronici, inclusi laptop, smartphone o USB, siano spenti e chiusi in modo sicuro.

Infine, vi ricordiamo che **segnalare** al Settore "Infrastrutture Digitali e Sicurezza", al Responsabile Protezione Dati ed all'Ufficio Privacy **i comportamenti scorretti** dal punto di vista privacy ed invitare i colleghi ad adottare comportamenti conformi al quadro normativo in ambito di riservatezza delle informazioni, può aiutare a fare la differenza per proteggere la nostra Regione.

Saluti,
Settore "Infrastrutture Digitali e Sicurezza",
Responsabile Protezione Dati,
Ufficio Privacy Regione Calabria.