ARAG
Tutela legale.
Vivi pienamente.

DIGITALnews
MAGAZINE TUTELA LEGALE

SETTEMBRE 2018
N. 9

La normativa europea in materia di Privacy (GDPR): il diritto di accesso dell'interessato.

In questo numero:

È capitato quasi a tutti di ricevere e-mail o messaggi per servizi che non ricordiamo di aver richiesto e da Società a cui non abbiamo fornito dati sensibili come il nostro numero di telefono. Finora una situazione come questa poteva essere quasi irrisolvibile. Oggi invece, in forza del nuovo Regolamento Generale sulla Protezione dei Dati (GDPR UE 2016/679), che è entrato in vigore in data 28.05.2018 e che ha sancito - tra le varie novità - il diritto di accesso, **tutti i consumatori potranno rivolgersi alle Società chiedendo di fornir loro i dettagli sui dati che hanno comunicato**, di chiarire come vengono trattati e come sono stati ottenuti i dati stessi.

> Il diritto di accesso, così come previsto dalla normativa comunitaria, si rafforza rispetto alla normativa passata tanto da acquisire il ruolo di diritto fondamentale delle persone fisiche. Questo al fine di garantire agli interessati una tutela della veridicità dei propri dati.

Ma cos'è esattamente il "diritto di accesso"?
Il diritto di accesso - disciplinato dall'art. 15 del nuovo regolamento - consiste nella possibilità per l'interessato di richiedere al titolare del trattamento (la società di telemarketing che ci assilla con le più varie proposte commerciali, ma anche qualsiasi altra società, come ad esempio la propria banca o l'azienda che ci fornisce l'energia elettrica) la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano.
In termini più generali, l'interessato può chiedere di prendere visione o estrarre copia dei vari tipi di documenti a lui riferibili. L'interessato può accedere alla propria informativa senza pagare alcuna somma. Resta ferma tuttavia la possibilità per il titolare di addebitare, in alcuni casi, un contributo spese basato sui costi amministrativi (per esempio in caso di richiesta di ulteriori copie di documenti).

Dopo aver esercitato il "diritto di accesso", cosa succede?
Una volta ricevuta da parte dell'interessato la richiesta di accedere ai propri dati, **il titolare del trattamento deve**:

- verificare l'identità dell'interessato che richiede l'accesso ai suoi dati, adottando tutte le misure necessarie per evitare che soggetti terzi possano abusivamente essere messi a conoscenza dei dati trattati;
- fornire una copia dei dati personali oggetto del trattamento che lo riguardano;
- fornire ulteriori informazioni tra cui le finalità del trattamento, le categorie di dati personali trattati, i destinatari o le categorie dei destinatari a cui i dati personali sono stati o saranno comunicati;
- informarlo della possibilità di esercitare il diritto di rettifica, o cancellazione, o di limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento.

Rispetto alla precedente normativa sulla privacy ...
... il titolare deve indicare il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per definire tale periodo nonché le garanzie applicate in caso di trasferimento dei dati verso paesi terzi. Oltre al rispetto delle prescrizioni relative alla modalità di esercizio del diritto di accesso e degli altri diritti, i titolari possono consentire agli interessati di consultare direttamente da remoto ed in modo sicuro i propri dati personali.

> Nel caso in cui l'interessato presenti la richiesta di accesso mediante mezzi elettronici (ad es.: lo smartphone o il computer), salvo sua diversa indicazione, le informazioni dovranno essere fornite in un formato elettronico di uso comune.

In collaborazione con:
Studio Legale Spagnuoli
Piazza F. Guardi 11 - 20133 Milano

Per la raccolta differenziata si devono utilizzare sacchetti trasparenti? Le regole del Garante della privacy.

La diffusione del servizio di raccolta dei rifiuti "porta a porta" sta facendo aumentare la percentuale di raccolta differenziata con conseguente riduzione di rifiuti conferiti in discarica.

Se, da una parte, la crescita della raccolta differenziata rappresenta una pratica virtuosa molto importante per la Società in cui viviamo, dall'altra bisogna considerare che può far emergere anche problematiche come quella della possibile violazione del diritto alla privacy del cittadino-utente.

Le regole dettate dai comuni

Con l'attività di raccolta differenziata della spazzatura, **molti Comuni italiani hanno imposto l'utilizzo di sacchetti trasparenti o semitrasparenti** che gli utenti devono lasciare in prossimità delle loro abitazioni in base al calendario e agli orari previsti dal Comune stesso.

Questa disposizione consente agli operatori ecologici di appurare il rispetto da parte dei cittadini delle regole previste per i rifiuti - verificando se il contenuto dei sacchetti è conforme alla frazione da ritirare - e di segnalare all'utente eventuali anomalie, attraverso degli avvisi applicati sulle buste non in regola.

È una procedura lecita o costituisce una potenziale lesione della privacy?

Tale procedura costituisce una potenziale lesione della privacy, data la possibilità di spiare facilmente cosa c'è dentro la spazzatura degli altri.

È chiaro che **nei rifiuti finiscono, infatti, molti effetti personali** (corrispondenza, fatture telefoniche con i numeri chiamati, estratti conto bancari, buste paga, scontrini, scatole di medicinali, prescrizioni mediche ecc.) - **che possono rivelare informazioni inerenti la sfera economica o le condizioni di salute di una persona**. Informazioni che, se trattate in modo non proporzionato, o in caso di abusi, possono arrecare danni alle persone.

La pronuncia del Garante della privacy

Al fine di conciliare le esigenze di tutela della privacy e l'interesse pubblico della raccolta differenziata, il Garante della privacy ha emesso un provvedimento a carattere generale (provvedimento del 14.07.2005) che risponde ai quesiti giunti da enti locali e privati cittadini e che detta una serie di regole in materia di utilizzo dei sacchetti dei rifiuti:

quando la raccolta della spazzatura avviene "porta a porta" i sacchetti trasparenti sono vietati
Si tratta infatti di una situazione che potrebbe consentire agli estranei di sapere non solo cosa contiene la busta di plastica, ma anche a chi appartiene. Secondo il Garante, tale obbligo previsto da alcuni Comuni non è proporzionato e può costituire una misura eccessiva rispetto alle normali finalità di controllo che si prefiggono gli enti locali. Pertanto, l'utilizzo di sacchetti trasparenti per verificare l'osservanza degli obblighi di raccolta differenziata è concesso solo sulla spazzatura di tipo condominiale. Nei confronti, invece, dei singoli cittadini va garantita la privacy e ciò impone la libertà di continuare a utilizzare i sacchetti neri o colorati. Il Garante della Privacy ha tuttavia fatto riferimento solo ai sacchetti trasparenti e non a quelli semi-trasparenti oggi maggiormente in uso, che dovrebbero teoricamente consentire una maggiore riservatezza, ma di fatto solo in apparenza;

sono vietate le etichette adesive nominative sui sacchi dell'immondizia o sul contenitore dei rifiuti, soprattutto se questo è posto per la strada, con nome e indirizzo del soggetto il Comune può contrassegnare il sacchetto dei rifiuti con un codice a barre, un microchip o con etichette intelligenti (Rfid), che consentono di delimitare l'identificabilità della persona solo nel caso in cui sia accertata la violazione delle norme sulla raccolta differenziata. In questo modo, precisa il Garante, "gli operatori che verificano l'omogeneità del contenuto del sacchetto (carta, vetro, plastica) non vengono a conoscenza dell'identità della persona, che rimane riservata fino alla decodifica dei codice a barre o del microchip da parte dei soggetti che applicano la sanzione";

si pongono dei limiti all'attività ispettiva finalizzata a rintracciare il produttore che avesse abbandonato i rifiuti in maniere difformi dai regolamenti: gli organi addetti ai controlli possono procedere ad ispezioni selettive solo nei casi in cui abbiano ragione di ritenere che i rifiuti siano stati lasciati senza osservare le norme in materia di raccolta differenziata e, quindi, solo nei confronti di coloro che hanno violato la normativa e quando il cittadino non sia identificabile in altro modo; sono invece vietate ispezioni generalizzate da parte del personale incaricato al fine di trovare elementi informativi per l'identificazione, presuntivamente, del conferente. La pratica delle ispezioni generalizzate è stata inoltre ritenuta non risolutiva, perché non sempre permette l'individuazione del conferente attraverso il contenuto dei sacchetti; essa è stata ritenuta anche non rispondente ai principi del Codice di protezione e, addirittura, fuorviante ai fini sanzionatori, posto che in forza di quella incertezza identificativa la sanzione eventualmente applicata, di conseguenza, potrebbe risultare comminata erroneamente. Analoga valutazione vale per le sanzioni conseguenti alla violazione del mancato rispetto dell'orario di conferimento;

i controlli e l'apertura dei sacchetti della spazzatura possono essere eseguiti esclusivamente da personale autorizzato
possono intervenire solo gli agenti della polizia municipale, ufficiali e agenti di polizia giudiziaria, dipendenti delle aziende municipalizzate e solo costoro hanno il potere di emettere sanzioni. È invece vietato il controllo e tanto più l'irrogazione di sanzioni da parte degli operatori ecologici, che sono semplici dipendenti; costoro possono semmai richiedere l'intervento della polizia locale.
E non è neanche possibile chiedere agli amministratori di condominio di controllare il comportamento dei propri condomini: è possibile chiedere loro solo di svolgere un'attività semplicemente collaborativa e di sensibilizzazione nei confronti dei proprietari delle abitazioni, senza comunque imporre alcunché.

Questo provvedimento individua un quadro di garanzie che assicura il rispetto dei diritti e delle libertà fondamentali dei cittadini e prescrive ai titolari del trattamento alcune misure necessarie e opportune per conformarsi alle disposizioni in materia di protezione dei dati personali.

In collaborazione con:
Studio Legale Associato Franciosa – Passini
Viale Mazzini, 123 - 00195 Roma

Come difendere la rete aziendale dai pirati informatici?

La sicurezza informatica è un tema caldo per tutti coloro che hanno una rete aziendale, o anche solo un sito internet da gestire.
Non esistono difese sicure al 100%: gli strumenti in mano ai criminali informatici sono sempre più numerosi ed evoluti ed è praticamente impossibile tenere tutto sotto controllo.

Quello che si può fare concretamente, è progettare bene la rete, nell'ottica di arginare quanto più possibile la possibilità di intrusioni.

Ecco 5 regole che gli esperti di sicurezza informatica suggeriscono di seguire:

1. Progetta la rete come se fosse già compromessa.

Quando si pensa alle difese di una rete, raramente si parte dal presupposto che il perimetro possa fallire e questo è errore che porta a gravi conseguenze.
La rete interna, le sue difese e i flussi di lavoro devono esser pensati sapendo che in qualsiasi momento potrebbe arrivare una "talpa" con intenzioni malevole e fare in modo che la sua vita sia difficile già dal primo momento.

2. Non creare utenti con poteri divini.

Creare degli utenti che possano accedere a tutto e abbiano pieni poteri su tutta la rete interna è uno degli errori più frequenti.
Sicuramente per chi amministra è molto più comodo avere un solo login per qualsiasi operazione, ma così si crea un'autostrada per chiunque riesca ad accedere e rubare i dati aziendali, compromettendo un utente "onnipotente".

3. Proteggi gli account privilegiati.

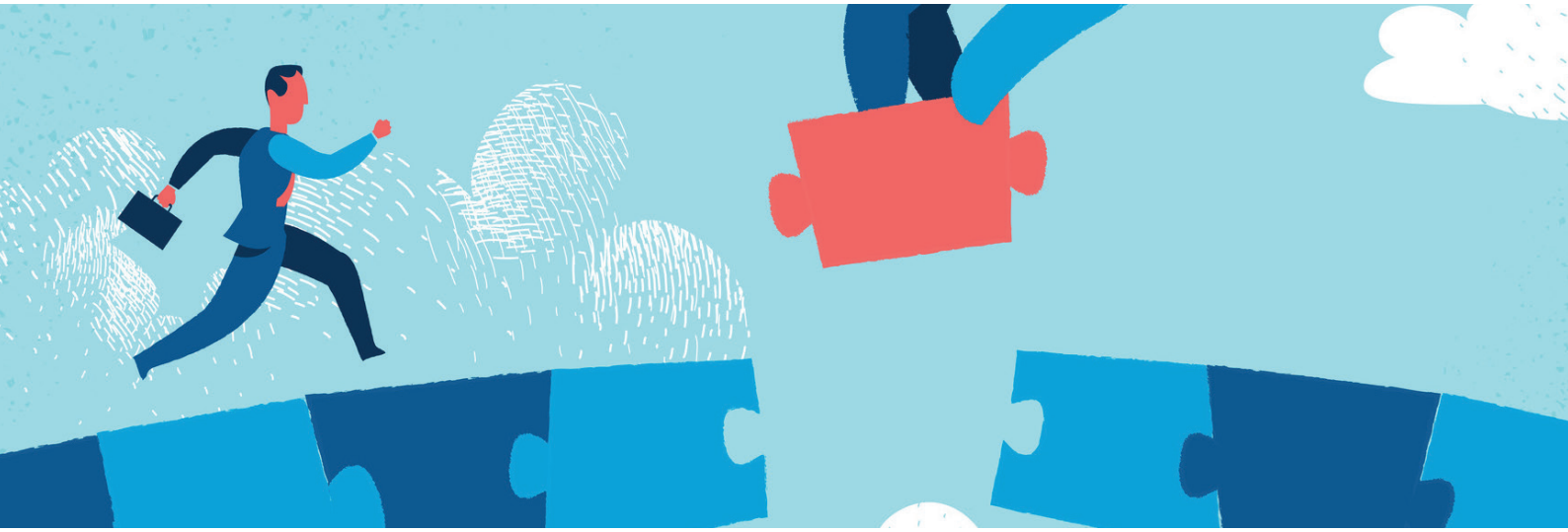
Non tutti gli utenti sono uguali e non tutti hanno bisogno delle stesse misure di sicurezza.
Quando si parla di utenti privilegiati, ovvero con poteri di amministratore più o meno forti, bisogna mettere in campo degli strumenti adatti a proteggerli adeguatamente: per un normale utente, la rotazione delle password può essere una seccatura, ma per un amministratore è assolutamente necessaria. È inoltre indispensabile prevedere autenticazioni forti, a due o più fattori, per tutta una serie di operazioni "sensibili".

4. L'Intelligenza artificiale è nostra amica.

I nuovi sistemi di intelligenza artificiale sono estremamente efficaci contro una vasta gamma di attacchi e riescono a intervenire addirittura prima che la compromissione permetta ai criminali di accedere ai dati.
I sistemi basati su *machine learning* riescono a identificare gli indicatori di compromissione prima che l'attacco giunga a buon fine scovando l'attaccante anche quando va a nascondersi in zone solitamente impossibili da analizzare.
L'idea è che "l'intelligenza artificiale" non va a caccia del'intruso nella rete, ma delle tecniche che vengono usate per portare gli attacchi e può quindi intervenire prima che l'attacco arrivi a compimento.

5. Non dimentichiamo gli endpoint.

A completare il quadro, in mezzo a tutte queste tecnologie innovative che mettono al centro utenti, flussi di lavoro e traffico di rete, non può mancare la protezione degli *endpoint* (un qualsiasi dispositivo hardware del sistema in grado di comunicare con gli altri dispositivi che fanno parte della rete; può quindi essere un computer, una stampante, un fax, un modem ecc.) per mezzo di nuovi sistemi di protezione, particolarmente attenti alla gestione delle minacce che arrivano dall'interno dell'azienda.
Pur mantenendo il proprio ruolo di protezione contro i malware inoculati tramite i soliti vettori di attacco, adesso l'endpoint è pensato anche per impedire la libera circolazione dei criminali sulle macchine.



Intermediari non più operativi per una disattenzione.

Quando non comunicare un adempimento può costare veramente caro.

In questo 2018 ricco di novità, con risvolti normativi importanti (IDD, protezione dei dati, cyber crime, ...) abbiamo anche avuto modo di conoscere un tipo di intervento da parte di IVASS, che prima era riservato a casi particolari (vedi intermediari iscritti ma non attivi): la messa in stato di inoperatività massiva.

> Per capire meglio: **quasi 4.000 iscritti sono di fatto scomparsi dalla sezione "attiva" del registro nell'arco di una notte!**
> E attenzione: nessuno di questi ha ricevuto una comunicazione individuale in merito, lasciando quindi ignari dell'evento chi non ha visto l'avviso sul sito IVASS.

Facciamo un passo indietro: **il Provvedimento IVASS n.58 del 14.03.2017** (vedi Art.8) ha ripristinato l'obbligo per gli Intermediari di comunicare all'IVASS stesso, entro il 5 febbraio 2018, l'avvenuto rinnovo della polizza di RC Professionale, secondo una modalità di invio elettronico.

Quindi, **ogni intermediario doveva tassativamente effettuare tale comunicazione pena l'indicazione automatica nel RUI come inoperativi**.
Evento poi puntualmente avvenuto: in data 5 maggio 2018 Ivass ha infatti comunicato tramite avviso lo stato di inoperatività di un numero impressionante di intermediari, oltre 800 broker (sia persone fisiche che società) e oltre 3.000 iscritti in sezione A!

Nella sezione del sito IVASS *"Per gli operatori" area "Avvisi"* sono pubblicati gli elenchi degli intermediari interessati

Tra tante cose da fare nel quotidiano, può capitare di dimenticare un adempimento. Ma...
Ora, non comunicare l'avvenuto rinnovo della polizza di RC professionale può rientrare pienamente nella categoria di quegli adempimenti che, nel turbinio di cose da fare quotidianamente in ufficio, è facile dimenticare... e se questo può essere perdonabile, non lo è però non interessarsi del ripristino della propria posizione attiva nel RUI.

Infatti, **l'intermediario divenuto "virtualmente" inoperativo deve attivarsi personalmente per ripristinare lo status corretto, che altrimenti lo vedrebbe operare al di fuori della corretta investitura del RUI**, fatto poi difficile da spiegare ad un eventuale ispettore IVASS in caso di controllo.
E non solo, dopo 3 anni di inattività l'IVASS procede alla cancellazione di ufficio dal registro, con tutto quello che ne consegue: **un intermediario particolarmente disattento potrebbe quindi cessare di esserlo per mera dimenticanza!**

In conclusione: ancora una volta è fondamentale per gli intermediari dedicare la massima attenzione alle richieste Ivass, perché esse hanno sempre un seguito.

Pubblicazione Periodica: Aut. Trib. Verona n. 1685 - 30.11.2005
Editore: ARAG SE Rappresentanza Generale e Direzione per l'Italia - Viale del Commercio, 59 - 37135 Verona - Tel. 045 8290411 - e-mail: arag@arag.it