Newsletter
NOTIZIARIO
ANNO XX
WWW.GARANTEPRIVACY.IT

NEWSLETTER N. 444 del 10 settembre 2018

Telemarketing aggressivo: 600 mila euro di sanzione a Fastweb

Fastweb dovrà pagare 600.000 euro per aver condotto campagne di telemarketing senza il consenso delle persone contattate e per aver adottato modalità di profilazione non corretta dei propri clienti.

Questa la **decisione del Garante della privacy [doc. web n. 9040267] (/garante/doc.jsp?ID=9040267)**che ha emesso un'ordinanza ingiunzione relativa alle violazioni già rilevate in un provvedimento adottato prima dell'entrata in vigore del nuovo Regolamento europeo in materia di protezione dei dati personali.

L'Autorità, grazie anche ad apposite ispezioni in loco, aveva accertato che i call center che lavoravano per la società spesso contattavano clienti o potenziali clienti senza il loro consenso a ricevere proposte commerciali, chiamando più volte anche chi si era già opposto al trattamento dei propri dati per finalità di marketing. La compagnia telefonica, inoltre, aveva proceduto alla profilazione di alcune categorie di clienti (ad esempio quelli anziani o basso spendenti) senza aver prima acquisito il loro consenso informato e senza avere effettuato una notificazione completa al Garante.

Altre criticità, emerse nel corso dell'istruttoria, erano riferibili allo scarso controllo posto in essere da Fastweb sulle pratiche di telemarketing aggressivo adottate dalla propria rete di vendita.

All'esito dell'accertamento, il Garante aveva contestato alla compagnia telefonica sia le violazioni relative all'informativa, al consenso e alla profilazione, sia l'ipotesi di maggiore gravità, in quanto commesse in relazione a banche dati di particolare rilevanza e dimensione.

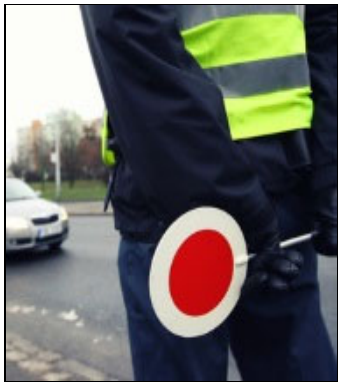
In merito alle prime violazioni, Fastweb si è avvalsa della facoltà di estinguere il procedimento sanzionatorio, pagando autonomamente, in forma ridotta, l'importo previsto dal Codice privacy, ossia il doppio del minimo edittale per ciascuna delle condotte illecite accertate.

Il Garante ha quindi adottato l'ordinanza ingiunzione con la quale ha

applicato la sanzione prevista per l'aggravante non oblabile. L'importo è stato inizialmente quantificato in 150.000 euro tenendo conto della molteplicità delle condotte illecite commesse, dei numerosi procedimenti sanzionatori già subiti dalla società stessa e dell'ingente numero di persone i cui dati sono stati trattati in violazione della normativa.

La somma da pagare è stata poi quadruplicata dal Garante a 600.000 euro, in considerazione della circostanza che le particolari condizioni economiche dell'operatore telefonico ne avrebbero altrimenti reso inefficace l'effetto sanzionatorio.

Forze di polizia,sicurezza sui luoghi di lavoro: Garante, si allo schema di decreto



Parere favorevole del Garante privacy [doc. web n. 9040242] (/garante/doc.jsp?ID=9040242) sull'applicazione del decreto in materia di tutela della salute e della sicurezza nei luoghi di lavoro per Forze di Polizia, Vigili del fuoco, protezione civile ed altre categorie affini.

L'Autorità privacy, pur non rinvenendo particolari criticità sotto il profilo della protezione dei dati personali, ha ritenuto però necessario fornire alcune precisazioni volte a perfezionare il testo dello schema di decreto, tenendo conto delle specifiche esigenze connesse all'impiego e alla formazione del personale, alla tutela delle informazioni sull'efficienza e la funzionalità delle strutture organizzative, nonché delle specifiche attività istituzionali.

Alla luce del principio di proporzionalità, ad esempio, il Garante ha chiesto al Ministero dell'interno di valutare la necessità del doppio regime di comunicazione delle segnalazioni e delle trasmissioni dei documenti del personale dell'amministrazione civile dell'Interno, sia alle ASL che agli organi di vigilanza interni.

Sotto altro profilo, sebbene al personale delle Forze di polizia e al personale delle Forze armate non trovi applicazione la disciplina in materia di assicurazione obbligatoria contro gli infortuni sul lavoro che presuppone trattamenti in capo all'INAIL, lo schema di decreto prevede comunque, la trasmissione all'INAIL dei dati relativi agli infortuni e alle malattie professionali del personale, attraverso il sistema informativo nazionale per la prevenzione nei luoghi di lavoro (SINP) "a fini statistici, in forma anonima e aggregata".

Il Garante ritiene in particolare che la trasmissione dei dati di tale personale debba avvenire per le sole finalità di cui all'art.8 comma 1 decreto 81. Tali finalità sono volte ad orientare, pianificare e valutare l'efficacia della prevenzione degli infortuni e delle malattie professionali, relativamente ai lavoratori iscritti e non iscritti agli enti assicurativi. Il decreto dovrà rispettare le indicazioni già fornite dall'Autorità privacy con due precedenti pareri, armonizzandosi con le specifiche modalità di partecipazione al sistema da parte delle Forze armate e di polizia e applicando tecniche di anonimizzazione dei dati che non consentano l'identificabilità delle persone fisiche interessate.

Rilascio dei visti, il bilancio dei controlli privacy

L'Autorità ha recentemente concluso una complessa attività di verifica sulla legittimità del trattamento dei dati personali effettuati nelle procedure di rilascio dei visti e nel Sistema di informazione visti (Visa Information System , VIS). Nell'ambito dell'attività, il Garante ha effettuato accertamenti ispettivi presso la sede del Ministero degli Affari Esteri e della Cooperazione internazionale e presso una sede consolare all'estero, verificando, in quest'ultima occasione, oltre all'operatività dell'Ufficio visti del consolato, anche la sede di una società esterna che fornisce al consolato, in outsourcing, alcuni servizi per i visti.

All'esito dei controlli, che hanno evidenziato nel complesso una situazione di sostanziale conformità al quadro normativo di riferimento, **l'Autorità ha adottato un provvedimento [doc. web n. 9040249] (/garante/doc.jsp?ID=9040249)** con il quale ha indicato al Maeci una serie di misure che consentiranno di migliorare ulteriormente la sicurezza e, più in generale, la conformità alle disposizioni sul trattamento dei dati personali effettuato dal Ministero nell'ambito del VIS.

In particolare, le prescrizioni hanno riguardato l'individuazione di tempi di conservazione dei dati nel sistema nazionale N-VIS, diversificati in relazione alla tipologia del visto e a specifiche esigenze (es. eventuale contenzioso), l'introduzione di meccanismi di cancellazione automatica dei dati in relazione ai termini stabiliti, l'indicazione di specifici requisiti per la gestione e l'analisi dei file di log. Verificate anche la gestione documentale e il funzionamento dei sistemi informativi, nonché il sistema di interfaccia specificamente dedicato ai trattamenti di dati da parte dei fornitori esterni di servizi.

Per gli aspetti tecnici e di sicurezza, gli approfondimenti hanno riguardato, tra l'altro, lo scambio di dati tra sistemi, la gestione delle utenze di accesso ai sistemi, la tenuta dei registri dei file di log, le modalità e i tempi di conservazione dei dati.

Il VIS è un sistema di scambio di dati tra i paesi dell'Unione europea relativi ai visti d'ingresso nello Spazio Schengen, che contiene i dati, anagrafici e biometrici, di tutte le persone tenute a chiedere il visto d'ingresso per soggiorni di breve durata, istituito con la Decisione del Consiglio dell'Unione Europea 2004/512/CE del 8 giugno 2004 e disciplinato dal Regolamento (CE) n. 767/2008 del Parlamento e del Consiglio e dalla decisione del Consiglio 2008/633/HA del 23 giugno 2008.

L'attività di vigilanza svolta dall'Autorità è specificamente prevista dall'art. 41 del Regolamento (CE) n. 767/2008, il quale prevede che, almeno ogni quattro anni, le autorità di protezione dati europee effettuino una verifica di conformità dei rispettivi sistemi nazionali per rilevare eventuali difformità e indicare azioni di miglioramento.

L'ATTIVITÁ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÚ

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

- Il testo del Regolamento Ue 2016/679 arricchito con riferimenti ai Considerando e aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9039802) – online il 7 settembre 2018

- Nuovo attacco hacker a piattaforma Rousseau: il Garante per la privacy avvia verifiche (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9039786) - Comunicato del 6 settembre 2018

- Pubblicato in Gazzetta Ufficiale il decreto per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9039744)– online il 5 settembre 2018

- Google-Mastercard: Garante verifica e valutazione su privacy (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9038858)- Comunicato del 31 agosto 2018

NEWSLETTER
del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).
Direttore responsabile: Baldo Meo.
Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n. 121 - 00186 Roma.
Tel: 06.69677.2752 - Fax: 06.69677.3755
Newsletter è consultabile sul sito Internet *www.garanteprivacy.it (http://www.garanteprivacy.it/)*