Newsletter
NOTIZIARIO
ANNO XXI
WWW.GARANTEPRIVACY.IT

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NEWSLETTER N. 453 del 30 maggio 2019

Data breach: Garante, le comunicazioni agli utenti non devono essere generiche

Le informazioni devono consentire alle persone di comprendere i rischi e proteggere i loro dati

(/garante/document?ID=9099233)

Le comunicazioni agli utenti dei data breach non devono essere generiche e devono fornire precise indicazioni su come proteggersi da usi illeciti dei propri dati, primo fra tutti il furto di identità. È quanto affermato dal Garante per la privacy nel provvedimento (/garante/doc.jsp?ID=9116509)adottato nei confronti di uno tra i principali fornitori nazionali di servizi di posta elettronica.

La società dovrà effettuare una nuova comunicazione sul data breach subito nei mesi scorsi, che aveva provocato l'accesso fraudolento alle caselle di posta elettronica di circa un milione e mezzo di propri utenti. La nuova comunicazione dovrà contenere una descrizione della natura della violazione e delle sue possibili conseguenze e dovrà fornire agli utenti precise indicazioni sugli accorgimenti da adottare per evitare ulteriori rischi. Nel caso specifico, ad esempio, dovrà essere spiegato agli utenti di non utilizzare più le credenziali compromesse e di modificare la password utilizzata per l'accesso a qualsiasi altro servizio online se uguale o simile a quella violata.

La decisione è stata presa dall'Autorità nell'ambito di un procedimento avviato a seguito della notifica di data breach trasmessa al Garante dall'azienda. Nella notificazione dell'incidente di sicurezza, la società ha dichiarato che il 20 febbraio scorso le analisi tecniche avevano evidenziato un accesso fraudolento tramite un hotspot della rete Wifi, dal quale era derivata la violazione di circa un milione e mezzo di credenziali di utenti che avevano avuto accesso tramite webmail.

Per contenere le possibili conseguenze del data breach la società aveva "forzato" gli utenti a reimpostare la password e predisposto una pagina apposita sul proprio sito per informare della violazione, in attesa di inviare una mail a tutti agli interessati colpiti dall'incidente. Mail effettivamente inviata, ma che, dagli atti acquisiti dal Garante nel corso di un'ispezione, è risultata carente e non in linea con quanto previsto dalla normativa sulla tutela dei dati personali. La società, infatti, aveva inviato due diverse comunicazioni a seconda che l'utente avesse provveduto o meno a effettuare il cambio della password entro le 48 ore successive all'avviso dell'avvenuto data breach.

In entrambi i casi la violazione era descritta come "attività anomala sui sistemi" e a chi aveva cambiato la password non veniva suggerita alcuna ulteriore azione correttiva, affermando che il cambio di password aveva reso inutilizzabili le credenziali precedenti;

a chi, invece, non aveva provveduto alla modifica si suggeriva solamente di cambiare la password per “eliminare il rischio di accesso indesiderato alla casella mail”. Informazioni ritenute dall’Autorità insufficienti, a fronte dei possibili e gravi rischi ai quali sono stati esposti gli utenti.

Telemarketing: dal Garante sì condizionato alla riforma

La tutela delle persone deve essere effettiva

Si condizionato del Garante privacy al regolamento del Ministero dello sviluppo economico che disciplina le nuove regole per il funzionamento del Registro pubblico delle opposizioni (Rpo) (/garante /doc.jsp?ID=9109315). Al Registro possono iscriversi gli utenti che non intendono ricevere offerte promozionali, né sul telefono fisso né sul cellulare, né tramite la posta cartacea.

Il regolamento, che estende la possibilità di iscrivere al Rpo anche i numeri di telefonia mobile e i numeri riservati, o non presenti negli elenchi telefonici pubblici, tiene già conto di alcune delle indicazioni fornite dall’Ufficio del Garante.

L’Autorità, tuttavia, per rendere il regolamento pienamente conforme alla normativa sulla protezione dei dati personali e realmente effettive le garanzie per gli utenti, ha fornito al Mise ulteriori indicazioni.

In primo luogo, il Garante ritiene che sia necessario precisare ulteriormente che l’iscrizione al Registro comporta automaticamente l’opposizione a tutti i trattamenti a fini promozionali, da chiunque effettuati, con la revoca anche dei consensi manifestati in precedenza. Su questo specifico punto il testo va quindi emendato eliminando ogni riferimento alle categorie merceologiche degli operatori che potrebbero generare dubbi interpretativi e alimentare il contenzioso.

L’Autorità chiede, inoltre, di valutare l’opportunità che nel Rpo possano confluire tutti gli indirizzi postali indicati dai contraenti, anche quelli non presenti negli elenchi telefonici. Per quanto riguarda poi la possibilità di revoca “selettiva” dell’opposizione al trattamento nei confronti di uno o più operatori di categorie merceologiche l’Autorità ritiene che questa procedura possa rivelarsi una “ipotesi residuale”. E ’prevedibile, infatti, che la revoca verrà, nella maggior parte dei casi, esercitata più facilmente manifestando il consenso, di volta in volta, alla singola società.

Anche per tale ragione, la gestione delle categorie merceologiche potrebbe risultare di difficile applicazione. Se si considera poi, che gli operatori (ad esempio, le piattaforme di e-commerce) svolgono attività riconducibili anche a più categorie merceologiche, la soluzione prospettata - per poter essere utilmente applicata a tutela dei diritti e degli interessi - dovrebbe, in teoria, consentire ai contraenti di revocare l’opposizione non solo riguardo all’attività dell’operatore, ma anche per singole campagne promozionali. Il Garante, infine, per rendere più esplicito l’obbligo della norma ed evitare comportamenti non corretti, suggerisce al Mise di prevedere in caso di illeciti, una responsabilità della società “non derogabile contrattualmente in concorso o in solido” con i call center che hanno effettuato la chiamata promozionale.

Garante privacy sanziona società: 2 milioni di euro per telemarketing indesiderato

Il Garante privacy ha comminato una sanzione di oltre 2 milioni di euro (/garante/doc.jsp?ID=9116053) ad una società che aveva svolto, tramite un call center albanese, attività di telemarketing e teleselling per conto di una azienda del settore energetico, in violazione della normativa sulla protezione dei dati personali in vigore prima del Regolamento europeo.

La Guardia di finanza, Nucleo speciale privacy, a seguito di un’ispezione, aveva accertato che la società, oltre a non aver reso alcuna informativa alle persone contattate, non aveva richiesto come previsto il consenso al trattamento dei dati personali per finalità di marketing. Consenso che la società, peraltro, avrebbe dovuto annotare per iscritto. Tali adempimenti spettavano infatti alla società che operava

in qualità di autonomo titolare del trattamento, non essendo mai stata designata responsabile.
La società, sulla base di presunti accordi con l'agente di vendita del gestore di energia, aveva incaricato il call center albanese di contattare telefonicamente potenziali clienti utilizzando numerazioni telefoniche raccolte dal call center stesso, senza che la lista dei contatti fosse stata fornita o validata dalle tre aziende coinvolte nella campagna promozionale (la società multata, l'agente di vendita del gestore e il gestore stesso). Dopo il primo contatto da parte del call center, le persone che avevano manifestato la volontà di sottoscrivere un contratto venivano richiamate dalla società.
La sanzione, definita cumulando ogni violazione contestata per singolo interessato, tiene conto anche della gravità della condotta della società che ha evidenziato un marcato disinteresse per la normativa in materia di protezione dei dati e una netta sottovalutazione delle gravi implicazioni che possono derivare dall'utilizzo di forme di acquisizione della clientela improntate all'informalità e alla unilaterale semplificazione degli adempimenti prescritti.

Garante: sì alle nuove regole per il Ced del Viminale

Chieste però maggiori garanzie per le persone

Il Garante per la privacy ha espresso parere favorevole (/garante /doc.jsp?ID=9116046)sulla bozza di decreto, predisposta dal Ministero dell'Interno, per la gestione del Centro elaborazione dati interforze (Ced) del Dipartimento della pubblica sicurezza. Sono state però richieste alcune modifiche per rendere la banca dati pienamente compatibile con la direttiva europea relativa al trattamento dei dati personali per finalità di polizia, nonché con la normativa italiana in materia.
Nel suo parere, il Garante ha segnalato che particolare attenzione deve essere posta alla tutela dei diritti delle persone i cui dati sono registrati nel Ced, integrando le modalità previste per l'esercizio di tali diritti - ad esempio quello di rettifica dei dati o di cancellazione di quelli illegittimamente conservati - e le informazioni da rendere agli interessati stessi, come il tempo di conservazione dei dati e i soggetti anche extra-europei a cui possono essere comunicati. Ha quindi sottolineato che eventuali limitazioni possono essere previste soltanto in presenza di specifiche esigenze puntualmente individuate. Ad esempio, per non compromettere indagini o procedimenti giudiziari, per l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o quella nazionale, per proteggere i diritti e le libertà altrui.
L'Autorità ha inoltre ricordato che il ruolo di Responsabile per la protezione dei dati (Rpd, spesso conosciuto con il termine inglese Dpo) dovrà essere ricoperto da un soggetto che svolge le sue funzioni in maniera indipendente.
Alcune novità importanti di cui tiene conto lo schema di decreto del ministero sono riferite a quelle introdotte dal cosiddetto "decreto sicurezza" che, tra l'altro, consente l'accesso al Ced anche al personale dei Corpi e servizi di polizia municipale, per verificare eventuali provvedimenti nei confronti delle persone controllate.
A tal proposito, il Garante ha chiesto di indicare nel testo chi ha il potere di autorizzare gli operatori - in particolare quelli delle capitanerie di porto e della polizia municipale - alla consultazione dei dati. Ha infine rimarcato che il personale incaricato dovrà essere individuato per iscritto e ricevere opportune istruzioni in merito alle modalità di trattamento dei dati del Ced.

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

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

- T4DATA: il 7 giugno ad Ancona un incontro formativo per gli RPD - Comunicato del 28 maggio 2019 (/garante /doc.jsp?ID=9116160)
- Protezione dati: firmato protocollo tra Procura di Vasto e Garante privacy - Comunicato del 22 maggio 2019 (/garante

/doc.jsp?ID=9115315)

- Anonymous: Garante privacy avvia istruttoria, "pec insicure" - Dichiarazione di Antonello Soro del 9 maggio 2019 (/garante/doc.jsp?ID=9109858)

- Il Garante privacy presenta la Relazione annuale. Il 7 maggio alla Camera dei Deputati - Comunicato del 3 maggio 2019 (/garante/doc.jsp?ID=9104297)

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 Venezia, n. 11 - 00187 Roma.
Tel: 06.69677.2751 - Fax: 06.69677.3785
Newsletter è consultabile sul sito Internet *www.garanteprivacy.it (http://www.garanteprivacy.it/)*