COMUNICATO STAMPA

NUOVE REGOLE PER LA SICUREZZA DEI DATI IN RETE E NELLE TLC
In caso di distruzione o perdita dei dati personali società telefoniche e Internet provider avranno l'obbligo di avvisare gli utenti

Società telefoniche e Internet provider dovranno assicurare la massima protezione ai dati personali perché tra i loro nuovi obblighi ci sarà quello di avvisare gli utenti dei casi più gravi di violazioni ai loro data base che dovessero comportare perdita, distruzione o diffusione indebita di dati.

In attuazione della direttiva europea in materia di sicurezza e privacy nel settore delle comunicazioni elettroniche, di recente recepita dall'Italia, il Garante per la privacy ha fissato un primo quadro di regole in base alle quali le società di tlc e i fornitori di servizi di accesso a Internet saranno tenuti a comunicare, oltre che alla stessa Autorità, anche agli utenti le "violazioni di dati personali" ("*data breaches*") che i loro data base dovessero subire a seguito di attacchi informatici, o di eventi avversi, quali incendi o altre calamità.

Le Linee guida adottate dal Garante stabiliscono chi deve adempiere all'obbligo di comunicare, in quali casi scatta l'obbligo di avvisare gli utenti, le misure di sicurezza tecniche e organizzative da mettere in atto per avvisare l'Autorità e gli utenti di un avvenuto "data breach", i tempi e i contenuti della comunicazione.

Al fine di armonizzare le procedure e le modalità di notifica, l'Autorità ha comunque deciso di avviare una consultazione pubblica (con pubblicazione sulla G.U.), per acquisire da parte delle società telefoniche e degli Isp elementi utili a valutare l'adeguatezza delle misure individuate.

Ecco in sintesi i punti principali delle Linee guida del Garante.

Chi deve comunicare le violazioni

L'obbligo di comunicare le violazione di dati personali spetta esclusivamente ai fornitori di servizi telefonici e di accesso a Internet. L'adempimento non riguarda quindi le reti aziendali, gli Internet point (che si limitano a mettere a disposizione dei clienti i terminali per la navigazione), i motori di ricerca, i siti Internet che diffondono contenuti.

La comunicazione al Garante

La comunicazione della violazione dovrà avvenire in maniera tempestiva: entro 24 ore dalla scoperta dell'evento, aziende tlc e Internet provider dovranno fornire le informazioni per consentire una prima valutazione dell'entità della violazione (tipologia dei dati coinvolti, descrizione dei sistemi di elaborazione, indicazione del luogo dove è avvenuta la violazione). Aziende telefoniche o internet provider avranno 3 giorni di tempo per una descrizione più dettagliata. Per agevolare l'adempimento il Garante ha predisposto un modello di comunicazione disponibile on line sul suo sito (www.garanteprivacy.it)

All'esito delle verifiche, i provider dovranno comunicare al Garante le modalità con le quali hanno posto rimedio alla violazione e le misure adottate per prevenirne di nuove.

La comunicazione agli utenti

Nei casi più gravi, oltre al Garante, le società telefoniche e gli Isp avranno l'obbligo di informare anche ciascun utente delle violazioni di dati personali subite. I criteri per la comunicazione dovranno basarsi sul grado di pregiudizio che la perdita o la distruzione dei dati può comportare (furto di identità, danno fisico, danno alla reputazione), sulla "attualità" dei dati (dati

più recenti possono rivelarsi più interessanti per i malintenzionati), sulla qualità dei dati (finanziari, sanitari, giudiziari etc.), sulla quantità dei dati coinvolti.

La comunicazione agli utenti deve avvenire al massimo entro 3 giorni dalla violazione e non è dovuta se si dimostra di aver utilizzato misure di sicurezza e sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati.

I controlli del Garante

Per consentire l'attività di accertamento del Garante, i provider dovranno tenere un inventario costantemente aggiornato delle violazioni subite che dia conto delle circostanze in cui queste si sono verificate, le conseguenze che hanno avuto e i provvedimenti adottati a seguito del loro verificarsi.

Le sanzioni

Non comunicare al Garante la violazione dei dati personali o provvedere in ritardo espone a una sanzione amministrativa che va da 25mila a 150mila euro. Stesso discorso per la omessa o mancata comunicazione agli interessati, siano essi soggetti pubblici, privati o persone fisiche: qui la sanzione prevista va da 150 euro a 1000 euro per ogni società o persona interessata. La mancata tenuta dell'inventario aggiornato è punita con la sanzione da 20mila a 120mila euro.

Roma, 1 agosto 2012