

Privacy e comunicazioni elettroniche: più tutele per gli utenti che subiscono perdita, distruzione o diffusione indebita dei propri dati

Autore: Redazione

In: Prassi amministrativa

Biancamaria Consales

Nuovi obblighi nel settore delle comunicazioni elettroniche, in caso di violazione di sicurezza. Le società elettroniche devono obbligatoriamente avvisare il Garante privacy e gli utenti quando i dati trattati per fornire i servizi subiscono gravi violazioni a seguito di attacchi informatici o di eventi avversi, come incendi o altre calamità, che possano comportare perdita, distruzione o diffusione indebita di dati.

Il Garante per la privacy ha, infatti, adottato, all'esito di una consultazione pubblica, un provvedimento generale che fissa, in attuazione della direttiva europea sulla privacy nel settore delle comunicazioni elettroniche, gli adempimenti per i casi in cui si dovessero verificare i cosiddetti "data breach".

In particolare, il provvedimento stabilisce che l'obbligo di comunicare le violazioni di dati personali, contenuti in data base elettronici o cartacei, spetta esclusivamente ai fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, ai siti internet che diffondono contenuti, ai motori di ricerca, agli internet point, alle reti aziendali). Pertanto, entro 24 ore dalla scoperta dell'evento, le società elettroniche devono fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione (con riferimento alla tipologia dei dati coinvolti, alla descrizione dei sistemi di elaborazione, all'indicazione del luogo dove è avvenuta la violazione). Per agevolare questo adempimento, il Garante ha predisposto un modello di comunicazione disponibile sul suo sito (www.garanteprivacy.it).

Nei casi più gravi di violazione, però, oltre che al Garante, le società telefoniche dovranno informare entro tre giorni anche ciascun utente coinvolto, facendo riferimento ad alcuni parametri fondamentali:

- a) il grado di pregiudizio che la perdita o la distruzione dei dati può comportare (furto di identità, danno fisico, danno alla reputazione);
- b) l'attualità dei dati (dati più recenti possono rivelarsi più interessanti per i malintenzionati);
- c) infine, la qualità (finanziari, sanitari, giudiziari etc.) e la quantità dei dati coinvolti.

Eccezione a tale regola, per cui la comunicazione agli utenti non è dovuta, è costituita dalla dimostrazione di aver utilizzato misure di sicurezza e sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati; in ogni caso, tuttavia, il Garante può comunque imporla nei casi più gravi.

Le società telefoniche, pertanto, per consentire l'attività di accertamento del Garante, dovranno tenere un inventario costantemente aggiornato in merito alle 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.

Per quanto riguarda, infine, l'aspetto sanzionatorio, la mancata o ritardata comunicazione al Garante espone le società telefoniche e gli Internet provider a una sanzione amministrativa che va da 25mila a 150mila euro. Sanzioni previste anche per l'omessa o mancata comunicazione agli utenti che vanno da 150 euro a 1000 euro per ogni società, ente o persona interessata. Invece, la mancata tenuta dell'inventario aggiornato è punita con la sanzione da 20mila a 120mila euro.

<https://www.diritto.it/privacy-e-comunicazioni-elettroniche-piu-tutele-per-gli-utenti-che-subiscono-perdita-distruzione-o-diffusione-indebita-dei-propri-dati/>