



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

SERVIZIO RELAZIONI CON I MEZZI DI INFORMAZIONE

COMUNICATO STAMPA

PRIVACY: SCATTA L'OBBLIGO PER SOCIETA' TELEFONICHE E INTERNET PROVIDER DI SEGNALARE AGLI UTENTI LE VIOLAZIONI SUBITE DAI PROPRI DATA BASE

Scatta l'obbligo per società telefoniche e Internet provider di 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".

Il provvedimento, pubblicato oggi nella Gazzetta Ufficiale, stabilisce che l'obbligo di comunicare le violazioni di dati personali, contenuti in particolare 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). Entro 24 ore dalla scoperta dell'evento, società di tlc e Isp devono fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione (ad esempio, tipologia dei dati coinvolti, descrizione dei sistemi di elaborazione, 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 l'Authority, le società telefoniche e gli Isp dovranno informare entro tre giorni anche ciascun utente coinvolto, facendo riferimento a alcuni parametri fondamentali: il grado di pregiudizio che la perdita o la distruzione dei dati può comportare (furto di identità, danno fisico, danno alla reputazione); l' "attualità" dei dati (dati più recenti possono rivelarsi più interessanti per i malintenzionati); la qualità (finanziari, sanitari, giudiziari etc.) e la quantità dei dati coinvolti.

La comunicazione agli utenti non è dovuta se si dimostra di aver utilizzato misure di sicurezza e sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati, ma il Garante può comunque imporla nei casi più gravi. Per consentire l'attività di accertamento del Garante, le società telefoniche e 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.

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 la omessa o mancata comunicazione agli utenti che vanno da 150 euro a 1000 euro per ogni società, ente o persona interessata. La mancata tenuta dell'inventario aggiornato è punita con la sanzione da 20mila a 120mila euro.

Roma, 26 aprile 2013