



MODULO 4

UNITÀ DIDATTICA 2

PAGINA 209

Nuove regole per la sicurezza dei dati in rete

A seguito dell'attuazione della direttiva europea in materia di sicurezza e privacy nel settore delle comunicazioni elettroniche avvenuta con il D.Lgs. 69/2012, è stato introdotto l'obbligo per società telefoniche e Internet Service Provider di avvisare gli utenti in caso di distruzione o perdita dei dati personali.

Società telefoniche e Internet Provider devono quindi assicurare la massima protezione ai dati personali; infatti sono obbligati ad avvisare gli utenti dei casi più gravi di violazioni ai data base che dovessero comportare perdita, distruzione o diffusione indebita di dati.



Il Garante per la privacy ha fissato un primo quadro di regole in base alle quali le società di telecomunicazione e i fornitori di servizi di accesso a Internet sono 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.

L'obbligo di comunicare la 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 della violazione deve avvenire in maniera tempestiva. Entro 24 ore dalla scoperta dell'evento, aziende di telecomunicazione 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).



prevista va da €1000,00 per ogni società o persona interessata, mentre la mancata tenuta dell'inventario aggiornato è punita con la sanzione da €20.000 a €120.000,00.

(Adattato da www.tmt-legal.com)

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.

Ovviamente sono previste delle sanzioni. Non comunicare al Garante la violazione dei dati personali o provvedere in ritardo espone a una sanzione amministrativa che va da €25.000,00 a €20.000,00. Stesso discorso per la omessa o mancata comunicazione agli interessati, siano essi soggetti pubblici, privati o persone fisiche: qui la sanzione