ISSN 1127-8579

Pubblicato dal 21/10/2010

All'indirizzo http://www.diritto.it/docs/30374-newsletter-privacy-del-10-settembre-2010-informazioni-commerciali-giustizia-amministrativa-conservazione-dati-traffico

Autore: Autorità Garante per la protezione dei dati personali

Newsletter privacy del 10 settembre 2010: informazioni commerciali, giustizia amministrativa, conservazione dati traffico

NEWSLETTER 342-2010

Newsletter
NOTIZIARIO SETTIMANALE
ANNO XII
WWW.GARANTEPRIVACY.IT

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NUMERO 342

12 OTTOBRE 2010

Informazioni commerciali: al via i lavori del codice

Da fissare le regole per la raccolta dei dati economici e patrimoniali sulle aziende

Al via i lavori preparatori del codice deontologico per le imprese che offrono servizi di informazione commerciale. Con un provvedimento, di cui è stato relatore Francesco Pizzetti (pubblicato sulla Gazzetta Ufficiale n.238 dell'11 ottobre 2010), il Garante per la protezione dei dati personali ha invitato le associazioni di categoria interessate (operatori del settore, imprenditori, consumatori) a fornire il loro contributo in vista dell'adozione del codice che disciplinerà un ambito informativo di particolare rilievo per il sistema economico. I dati registrati dalle imprese che operano nel settore delle informazioni commerciali, infatti, possono riguardare aspetti organizzativi, finanziari o patrimoniali dell'attività svolta dagli operatori economici, ma possono anche fare riferimento a persone fisiche che svolgono ruoli di particolare responsabilità nelle società.
Il Codice di deontologia e buona condotta dovrà, in particolare, fissare le regole per la raccolta, l'elaborazione e la conservazione di tali informazioni, individuando anche idonei meccanismi per favorire la qualità e l'esattezza dei dati utilizzati.
Tutti i soggetti appartenenti alle categorie interessate e che ritengano di avere titolo a sottoscrivere il codice, sono dunque chiamati a comunicare la loro adesione o a confermarla se già espressa a seguito dell'invito formulato a suo tempo dall'Autorità.
Ai fini dell'ammissione ai lavori che porteranno all'adozione del Codice deontologico, il Garante, oltre a valutare la effettiva appartenenza alle categorie interessate alla sottoscrizione del codice, verificherà l'organizzazione e l'articolazione sul territorio dei soggetti che si ritengono rappresentativi, le attività da loro svolte in concreto anche con riferimento alla protezione dei dati personali, il numero dei soggetti effettivamente rappresentati in rapporto alla categoria.
Comunicazioni e documentazione potranno essere inoltrate, entro il 5 novembre 2010, al Garante per la protezione dei dati personali anche mediante e-mail: codiceinformazionicommerciali@garanteprivacy.it

Giustizia amministrativa più protetta

La giustizia amministrativa dovrà rafforzare le misure di sicurezza a protezione dei dati giudiziari. In particolare, dovrà garantire comunicazioni telematiche provenienti dall'esterno criptate e accessi alla rete interna sempre tracciati. Lo ha stabilito il Garante privacy al termine del recente ciclo di verifiche svolte in collaborazione con il Consiglio di Stato e il Tar del Lazio dalle quali, pur in un quadro confortante di rispetto delle regole, sono emerse alcune criticità. Gli organi della giustizia amministrativa avranno al massimo dodici mesi di tempo per adottare tutte le prescrizioni dettate dal Garante per proteggere con maggiore cura i fascicoli processuali e "blindare" gli accessi informatici che provengono dall'esterno - la cd. "scrivania del magistrato" - alla rete informatica interna. Particolare attenzione è stata infatti posta alla messa in sicurezza del Nuovo sistema informativo della giustizia amministrativa (Nsiga) che gestisce i documenti e i processi lavorativi dell'intero sistema, costituito dal Consiglio di Stato e dai 29 Tribunali amministrativi regionali. A completamento delle misure di sicurezza già adottate, la Giustizia amministrativa dovrà garantire che per le comunicazioni gestite da Nsiga fra le sedi del sistema giudiziario amministrativo e per gli accessi dei magistrati a Nsiga da postazioni esterne agli uffici, sia adottato un protocollo che cifri i dati in transito. E dovranno essere tracciate tutte le operazioni compiute sul Nsiga da magistrati e personale amministrativo, compresi gli accessi in sola lettura. Misura, questa, adottata finora solo per le operazioni di scrittura. La Giustizia amministrativa dovrà adottare, inoltre, delle policy che specifichino agli utenti di non utilizzare password banali per accedere al Nsiga (ad es. quelle contenenti il nome stesso dell'utente). L'accesso alla sala server e alla sala dove sono collocati i gruppi di continuità dovrà essere registrato (tramite log) e consentito solo con badge nominativi. Questi locali, inoltre, dovranno essere costantemente monitorati, eventualmente anche attraverso un impianto di videosorveglianza interno.

Conservazione dei dati di traffico e indagini di polizia: Ue in ordine sparso

Rapporto del Garanti Ue coordinato dall'Autorità italiana

Il Gruppo che riunisce le Autorità europee di protezione dati (Gruppo Articolo 29) ha di recente adottato il rapporto sullo stato di attuazione della direttiva 2006/24 (la cosiddetta "Direttiva Frattini") che riguarda la conservazione dei dati di traffico telefonico e telematico per finalità di polizia e giudiziarie (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf).

Dal rapporto emerge un quadro complessivamente disarmonico, sia sul recepimento della direttiva da parte degli Stati membri, sia sulle specifiche disposizioni nazionali, che in alcuni casi risultano contrarie ai principi della direttiva stessa o gravemente manchevoli con particolare riguardo alle misure di sicurezza adottate.

La direttiva 2006/24 introduce, come noto, disposizioni che derogano a quelle della direttiva sulla privacy nelle comunicazioni elettroniche (direttiva 2002/58) in materia di dati di traffico telefonico e telematico, consentendo di conservare tali dati oltre il periodo eventualmente necessario "ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione" quando ciò sia indispensabile per l'accertamento e la prevenzione di reati.

L'analisi del Gruppo Articolo 29, coordinata dall'Autorità italiana, ha preso le mosse da un questionario congiunto che è stato inviato dalle Autorità di protezione dati dei Paesi membri ai principali provider nazionali. I risultati mostrano che il periodo di conservazione nei diversi Paesi dell'Unione varia fra 6 mesi e 10 anni a seconda delle legislazioni nazionali; le categorie di dati conservati eccedono spesso quelle indicate nella direttiva, soprattutto per quanto riguarda i dati di traffico telematico che in taluni casi comprendono anche dati relativi ai contenuti delle comunicazioni (cosa espressamente vietata dalla direttiva stessa): ad esempio, alcuni provider conservano gli Url (indirizzi) delle pagine web visitate e le intestazioni (header) dei messaggi di posta elettronica. Le misure di sicurezza adottate, inoltre, non sempre sono idonee e, soprattutto per i provider di minori dimensioni, mostrano numerose lacune.

Alla luce delle risultanze dell'analisi, i Garanti hanno dunque elaborato una serie di raccomandazioni. Per quanto riguarda il periodo di conservazione, si chiede alla Commissione di fissare un periodo unico e preferibilmente più breve, anche considerando che in molti Paesi il termine massimo di conservazione risulta inferiore al limite previsto dalla direttiva (24 mesi), che appare quindi inutilmente ampio. Rispetto alle categorie di dati conservati, ai legislatori nazionali si ricorda di non imporre obblighi ulteriori rispetto a quanto previsto dalla direttiva. Riguardo alle misure di sicurezza, il Gruppo raccomanda ai provider di adottare alcuni ulteriori accorgimenti (sistemi di "strong authentication", registro dettagliato dei log di accesso, ecc.) e propone uno schema pan-europeo per la consegna dei dati da parte dei provider alle autorità di polizia e giudiziarie così da facilitare e armonizzare gli interscambi ed anche le analisi statistiche (quanti accessi, quali dati, richiesti da quali autorità, ecc.). Va ricordato, infine, che sullo stato di attuazione della direttiva 2006/24 è atteso anche il rapporto della Commissione europea.

L'attività del Garante. Per chi vuole saperne di più

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

Il Garante italiano aderisce al GPEN, un network internazionale per rafforzare la cooperazione in materia di privacy - Comunicato del 21.9.2010

Comunicazioni "captate" su reti wi-fi: il Garante ordina a Google Street View il blocco dei dati e trasmette gli atti alla magistratura - Comunicato del 21.9.2010

NEWSLETTER del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/696772751 - Fax: 06/696773755. *Newsletter* è consultabile sul sito Internet www.garanteprivacy.it