ISSN 1127-8579

Pubblicato dal 18/02/2010

All'indirizzo http://www.diritto.it/docs/29007-newsletter-privacy-del-11-febbraio2010-n-334-carte-di-credito-banche-sanit-elettronica

Autore: Autorità Garante per la protezione dei dati personali

Newsletter privacy del 11 febbraio2010 n. 334: carte di credito, banche, sanità elettronica

Newsletter
NOTIZIARIO SETTIMANALE
ANNO XI
WWW.GARANTEPRIVACY.IT

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NUMERO 334

11 FEBBRAIO 2010

Carte di credito, banche, sanità elettronica sotto la lente del Garante

Varato il piano ispettivo per il primo semestre 2010. Nello scorso anno applicate sanzioni per circa 1.600.000 euro

Banche, carte di credito, fascicolo sanitario elettronico, vendita di banche dati per finalità di marketing, sistema informativo del fisco, enti previdenziali. E' su questi delicati settori e sulle modalità con le quali vengono trattati i dati personali di milioni di cittadini italiani che si concentrerà l'attività di accertamento del Garante per la privacy nei primi sei mesi dell'anno. Il piano ispettivo appena varato prevede specifici controlli, sia nel settore pubblico che in quello privato, anche riguardo all'adozione delle misure di sicurezza, alla durata di conservazione dei dati, all'informativa da fornire ai cittadini, al consenso da richiedere nei casi previsti dalla legge. Oltre 250 gli accertamenti ispettivi programmati che verranno effettuati anche in collaborazione con le Unità Speciali della Guardia di Finanza - Nucleo Privacy. A questi accertamenti si affiancheranno quelli che si renderanno necessari in ordine a segnalazioni e reclami presentati.
Un primo bilancio sull'attività ispettiva relativa al 2009 svolta, come di consueto, in collaborazione con il Nucleo Privacy della Guardia di Finanza, mostra il significativo lavoro di controllo svolto dall'Autorità: sono state circa 500 le ispezioni effettuate e 368 i procedimenti sanzionatori avviati. Sono state riscosse somme per circa 1 milione e 600 mila euro, di cui oltre 62.000 relativi alla mancata adozione di misure di sicurezza da parte di aziende e pubbliche amministrazioni.
Sul fronte sanzioni va ricordato che nel 2009 sono state applicate le nuove sanzioni introdotte dal decreto "mille proroghe" del dicembre 2008. L'Autorità ha contestato per la prima volta - a una società che commercializza dati per finalità di marketing - la sanzione, che va da 50.000 a 300.000 euro, prevista nei casi in cui si riscontrino più violazioni commesse in relazione a banche dati di particolare rilevanza o dimensione.
43, infine, sono state nel 2009 le segnalazioni all'autorità giudiziaria che hanno riguardato, tra l'altro, casi di mancata di adozione delle misure di sicurezza, trattamento illecito dei dati, falsità nelle dichiarazioni e nelle notificazioni, il mancato adempimento ai provvedimenti del Garante.

Certificati medici: scambio di dati tra Inps e Inpdad

L'Inps potrà ricevere dall'Inpdap le informazioni sulle amministrazioni a cui inviare i certificati medici dei dipendenti pubblici. Il Garante ha infatti dato il via libera allo scambio di dati tra i due enti che avevano comunicato all'Autorità la necessità di realizzare tale flusso informativo.
In base alla "riforma Brunetta" del pubblico impiego in tutti i casi di assenza per malattia la certificazione medica deve essere inviata per via telematica, direttamente dal medico che la rilascia, all'Inps e da questo immediatamente inoltrata all'ente dove il dipendente lavora. Per poter eseguire questi invii l'Inps deve acquisire presso l'Inpdap gli estremi identificativi delle amministrazioni dove prestano servizio gli impiegati. Perché una tale comunicazione di dati tra enti sia possibile, è però necessario che essa sia prevista da una norma di legge o di regolamento oppure sia indispensabile per assicurare lo svolgimento delle funzioni istituzionali dei soggetti pubblici interessati. Mancando la previsione normativa, l'Inps ha dunque rappresentato al Garante la necessità di accedere ai dati dell'Inpdap per poter svolgere i propri compiti istituzionali in materia di controlli sulle assenze.
L'Autorità ha riconosciuto, pur in assenza di un'espressa norma di legge e di regolamento, le esigenze dell'Inps e ha stabilito che l'ente, per le proprie funzioni istituzionali, possa acquisire dall'Inpdap i dati delle amministrazioni dove prestano servizio i dipendenti pubblici. Ha comunque prescritto ai due enti di assicurare

l'accesso selettivo alle sole informazioni essenziali e di individuare strumenti e misure organizzative per garantire la protezione dei dati, in particolare con il tracciamento delle operazioni compiute dal personale incaricato. Inps e Inpdap dovranno poi stipulare una convenzione atta a circoscrivere le finalità per le quali viene consentito questo esclusivo trattamento dei dati, definendo rigorose procedure per l'autenticazione e le autorizzazioni degli utenti deputati alla consultazione dei dati. L'Inps non dovrà in ogni caso creare banche dati autonome con le informazioni ricevute dall'Inpdap. In conformità alle norme in materia, infine, ha ricordato l'Autorità, i certificati medici trasmessi dall'Inps alle amministrazioni non dovranno contenere l'indicazione della diagnosi.

Archivi Schengen: rafforzare le misure a protezione dei dati

Il Garante privacy ha chiesto al Ministero dell'interno un rafforzamento delle misure impiegate a tutela dei dati trattati in applicazione dell'Accordo di Schengen, che prevede uno scambio di informazioni tra le banche dati delle forze di polizia dei Paesi aderenti al fine di garantire meglio la sicurezza delle frontiere.
La sicurezza e l'integrità dell'archivio nazionale del Sistema Schengen, data la particolare importanza e delicatezza delle informazioni contenute (segnalazioni su soggetti non appartenenti all'area Schengen, persone scomparse, estradizioni, notifiche di provvedimenti dell'Autorità Giudiziaria), dovranno essere maggiormente garantite dalla Divisione N-S.i.s. del Dipartimento di pubblica sicurezza che gestisce il database nazionale. Gli accessi effettuati al sistema dovranno essere tracciabili e basati su procedure certificate, su cui dovrà vigilare un'unità di auditing potenziata e responsabile della sicurezza dei dati. Analoga accortezza dovrà essere adottata per garantire i flussi informativi della Divisione S.i.r.e.n.e. che raccoglie dal C.e.d. del Dipartimento e dagli uffici di polizia interessati, le informazioni aggiuntive ritenute utili a dare seguito alle segnalazioni e le trasmette agli uffici dell'omologa Divisione del Paese in cui il soggetto è stato rintracciato. Tali dati dovranno essere inviati mediante posta elettronica certificata e, laddove si utilizzi il fax, dovranno essere protetti con particolari tecniche di cifratura e l'uso di gruppi chiusi di numerazione. La sala server delle Divisioni N-S.i.s. e S.i.r.e.n.e. dovrà essere protetta mediante l'adozione di una procedura speciale di *strong authentication*, ottenuta dalla combinazione di più credenziali di accesso (badge nominale e dispositivo basato su una caratteristica biometrica), dovrà inoltre essere garantita la disponibilità e la continuità di esercizio della banca dati adottando piani di prevenzione che impediscano la sospensione dei servizi. Il Ministero dell'interno dovrà dare riscontro all'Autorità dell'avvenuta adozione delle misure prescritte.

Va ricordato, infine, che l'Autorità italiana collabora con quelle degli altri Paesi Schengen al fine di ottimizzare il funzionamento armonizzato del Sistema informativo Schengen.

Ue-Usa: la Commissione lancia una consultazione sulla protezione dei dati

La Commissione europea ha lanciato nei giorni scorsi una consultazione pubblica sul futuro accordo tra Ue e Usa sulla protezione dei dati personali e lo scambio di informazioni a fini di collaborazione giudiziaria e di polizia. Nel nuovo quadro del Programma di Stoccolma sulla giustizia, libertà e sicurezza approvato nell'ultimo Consiglio europeo di dicembre, la Commissione intende raccogliere indicazioni utili alla definizione dei contenuti che saranno oggetto del futuro negoziato con gli Stati uniti su un nuovo accordo in materia di privacy e sicurezza. La consultazione sarà aperta sino al 12 marzo prossimo, e il documento relativo è disponibile all'indirizzo
http://ec.europa.eu/yourvoice/consultations/index_en.htm
E' stata inoltre programmata una serie di incontri con i soggetti istituzionali più direttamente coinvolti. Al primo di tali incontri, tenutosi lo scorso 2 febbraio a Bruxelles, ha partecipato il presidente dell'Autorità italiana Francesco Pizzetti, anche in qualità di presidente del Gruppo di lavoro europeo in materia di cooperazione giudiziaria e di polizia (WPPJ).

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

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

Violenza sessuale a Salerno. Il Garante ai media: no ai nomi dei violentatori se rendono identificabile la vittima - Comunicato del 27.1.2010