GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NEWSLETTER N. 432 del 15 settembre 2017

Regolamento privacy, come scegliere il responsabile della protezione dei dati

Le prime indicazioni del Garante: necessarie competenze specifiche non attestati formali

Le pubbliche amministrazioni, così come i soggetti privati, dovranno scegliere il Responsabile della protezione dei dati personali (RPD) con particolare attenzione, verificando la presenza di competenze ed esperienze specifiche. Non sono richieste attestazioni formali sul possesso delle conoscenze o l'iscrizione ad appositi albi professionali. Queste sono alcune delle indicazioni fornite dal Garante della privacy alle prime richieste di chiarimento in merito alla nomina di questa nuova importante figura - introdotta dal Regolamento UE 2016/679 - che tutti gli enti pubblici e anche molteplici soggetti privati dovranno designare non più tardi del prossimo maggio 2018.

Nella nota inviata a un'azienda ospedaliera l'Ufficio del Garante ricorda che i Responsabili della protezione dei dati personali - spesso indicati con l'acronimo inglese DPO (Data Protection Officer) – dovranno avere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Nella selezione sarà poi opportuno privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari documentando le esperienze fatte, la partecipazione a master e corsi di studio/professionali (in particolare se risulta documentato il livello raggiunto). Gli esperti individuati dalle aziende ospedaliere, ad esempio, in considerazione della delicatezza dei trattamenti di dati effettuati (come quelli sulla salute o quelli genetici) dovranno preferibilmente vantare una specifica esperienza al riguardo e assicurare un impegno pressoché esclusivo nella gestione di tali compiti.

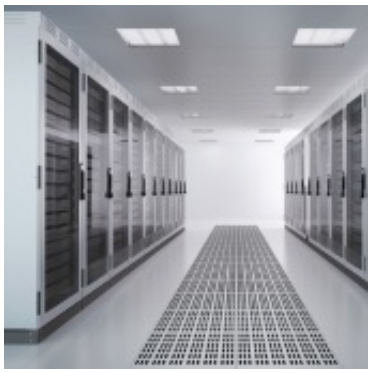
L'Autorità ha inoltre chiarito che la normativa attuale non prevede l'obbligo

per i candidati di possedere attestati formali delle competenze professionali. Tali attestati, rilasciati anche all'esito di verifiche al termine di un ciclo di formazione, possono rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenza della disciplina ma, tuttavia, non equivalgono a una "abilitazione" allo svolgimento del ruolo del RPD. La normativa attuale, tra l'altro, non prevede l'istituzione di un albo dei "Responsabili della protezione dei dati" che possa attestare i requisiti e le caratteristiche di conoscenza, abilità e competenza di chi vi è iscritto. Enti pubblici e società private dovranno quindi comunque procedere alla selezione del RPD, valutando autonomamente il possesso dei requisiti necessari per svolgere i compiti da assegnati.

Il Garante si riserva di fornire ulteriori orientamenti, che saranno pubblicati sul sito istituzionale, anche all'esito dei quesiti e delle richieste di approfondimento sul Regolamento privacy, raccolti nell'ambito di specifici incontri che l'Autorità ha in corso con imprese e Pubblica Amministrazione.

Ced del Viminale, definite le procedure privacy

Chiesto il divieto assoluto di scaricare dati in forma massiva e ribaditi tempi ridotti di conservazione



Parere favorevole del Garante privacy sullo schema di decreto del Presidente della Repubblica che disciplina le procedure di raccolta, accesso, comunicazione, cancellazione e integrazione delle informazioni e dei dati registrati nel Centro elaborazione dati del Viminale [doc. web n. 6826534]. Per innalzare ulteriormente il livello di protezione, il Garante ha però chiesto al Ministero dell'interno di esplicitare il divieto assoluto per gli operatori autorizzati all'accesso di poter scaricare i dati contenuti nel sistema in forma massiva con qualunque mezzo, ad esempio tramite chiavette usb. L'Autorità, inoltre, ha ribadito la necessità di stabilire tempi di conservazione dei dati più brevi e commisurati alle finalità della raccolta, rispetto a quelli attuali, ritenuti immotivatamente lunghi. Analogo rilievo era già stato sollevato in un precedente parere adottato su uno schema di decreto generale riguardante i trattamenti effettuati a "fini di polizia". Considerata poi la complessità e l'importanza del Ced, il Garante ha suggerito di dettagliare con un atto di natura regolamentare anche le specifiche misure di sicurezza.

Si è così concluso l'iter di regolamentazione dei dati personali trattati a "fini di polizia", dando completa attuazione al Titolo II della Parte II del Codice privacy.

Il Ced è un grande archivio informatico alimentato e aggiornato dalle forze di polizia con dati e informazioni (denunce, segnalazioni) acquisiti nel corso delle attività di tutela dell'ordine e della sicurezza pubblica. Nel Ced confluiscono anche sentenze dell'autorità giudiziaria, dati acquisiti dalle capitanerie di porto e rilevati dalla polizia municipale (ad es., quelli su veicoli e documenti rubati). I dati registrati nel Ced possono essere scambiati con le forze di polizia degli Stati membri dell'Unione europea o di Stati terzi o con organismi internazionali nell'ambito delle attività di cooperazione.

Nel decreto è ora definita in modo dettagliato l'organizzazione del Ced, sono specificate le regole per la conservazione e l'uso dei dati, i criteri per la loro comunicazione, gli obblighi di sicurezza e i collegamenti con le altre banche dati, ed è espressamente prevista la figura del Responsabile per la protezione dei dati cui vengono affidati importanti compiti di informazione, sorveglianza, consulenza e cooperazione con l'Autorità. Il Responsabile,

infatti, deve essere consultato per individuare, tra l'altro, le categorie di dati da trattare, i casi in cui può essere autorizzato un allungamento dei termini massimi di conservazione e le modalità di cancellazione o anonimizzazione delle informazioni contenute nel database.

A Hong Kong la 39^ Conferenza mondiale delle Autorità privacy

Costruire ponti tra Occidente e Oriente per proteggere i dati personali

Costruire ponti tra Occidente e Oriente per proteggere i dati personali. È questo il tema al centro della 39^ Conferenza internazionale delle Autorità di protezione dati che si terrà a Hong Kong dal 25 al 29 settembre e vedrà riuniti rappresentanti provenienti da tutti i continenti. Nel corso dei lavori, ai quali parteciperà anche una rappresentanza del Garante italiano, saranno affrontati temi cruciali del mondo iperconnesso legati all'intelligenza artificiale, alla cybersecurity, ai trasferimenti transfrontalieri di dati, alle differenze privacy tra Est e Ovest e alla necessità di individuare "denominatori comuni" tra i due continenti.

In particolare, il Segretario dell'Autorità italiana interverrà nell'ambito della presentazione di un progetto dell'Unesco volto a definire indicatori comuni per un accesso a Internet democratico e internazionalmente condiviso.

Le Autorità affronteranno anche i delicati temi derivanti dall'uso dei big data da parte dei governi: dai benefici della condivisione delle informazioni alla gestione dei rischi; dall'analisi dei dati per la ricerca sociale e sanitaria allo sviluppo di modelli predittivi e di profilazione potenzialmente rischiosi per la privacy e la libertà individuale. Anche le amministrazioni pubbliche, infatti, cercano di utilizzare a loro vantaggio l'enorme mole di dati in loro possesso: per guidare le scelte economiche, diffondere conoscenze, aumentare la trasparenza, contrastare l'evasione fiscale, migliorare i servizi pubblici, ridurre i costi. Le Autorità di protezione dati riunite a Hong Kong esamineranno quindi l'impatto che questo processo di data mining comporta sulla riservatezza di milioni di persone e cercheranno di individuare le misure più efficaci a protezione dei dati personali.

Al termine della Conferenza è prevista l'adozione di alcune risoluzioni, tra le altre, quelle sui veicoli automatizzati e connessi, il rafforzamento della cooperazione internazionale, la protezione della riservatezza del consumatore.

Avvocati e crediti formativi: ok al riconoscimento via webcam

Il sistema non prevede l'uso di dati biometrici per la verifica dell'identità dei partecipanti ai corsi online

Via libera del Garante privacy ad un sistema informatico che consente di verificare l'effettiva corrispondenza tra l'identità degli avvocati iscritti a corsi di formazione professionali, erogati in streaming, a quella delle persone effettivamente connesse [doc. web n. 6826368]. Il sistema, sottoposto a verifica preliminare dell'Autorità, è finalizzato a evitare che alcuni partecipanti pongano in essere comportamenti sleali per farsi attribuire crediti formativi simulando la partecipazione ai corsi a distanza.

Secondo quanto dichiarato dalla società il controllo dell'identità avverrà acquisendo, a intervalli casuali durante lo svolgimento del corso, la fotografia dei partecipanti collegati in diretta streaming, mediante la webcam del pc di ciascun professionista. Al termine dell'evento le immagini

acquisite verranno inserite nelle schede personali insieme al diagramma di connessione.

Successivamente un operatore confronterà le fotografie con quelle dei documenti di identità raccolti in fase di iscrizione, mediante un'operazione che non comporta alcun trattamento biometrico, non essendo prevista la verifica automatizzata di immagini digitali. Il Garante ha richiamato a tale proposito la definizione di riconoscimento facciale elaborata dal Gruppo Art. 29 secondo cui "il riconoscimento facciale è il trattamento automatizzato di immagini digitali contenenti i volti degli individui allo scopo di identificarli, verificarne l'identità o categorizzarli".

L'Autorità ha ritenuto lecito il trattamento dei dati personali che dovrà essere oggetto di una specifica e articolata informativa che consenta agli interessati l'esercizio dei diritti, espliciti le finalità e le modalità del trattamento, descriva le caratteristiche tecniche del sistema ed evidenzi i tempi di conservazione dei dati personali.

Il Garante ha prescritto inoltre alla società di raccogliere dagli interessati uno specifico consenso informato al trattamento delle immagini e di configurare il sistema in modo da trattare i dati nel rispetto dei principi di proporzionalità, necessità e correttezza. La società dovrà consentire l'accesso ai dati personali acquisiti solo a soggetti adeguatamente formati, designati "responsabili" e "incaricati" del trattamento, e dovrà adottare idonee misure di sicurezza a tutela della privacy degli interessati.

L'ATTIVITÁ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÚ

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

- Privacy e vaccini: le scuole potranno inviare gli elenchi degli iscritti alle Asl - Comunicato del 1° settembre 2017
- Tim: Garante privacy, ragionevole Governo pensi a sicurezza rete Telecom - Dichiarazione di Antonello Soro del 29 agosto 2017
- Nuove tutele per i minori vittime di cyberbullismo sui social network e sul web - Scheda informativa del 24 agosto 2017
- Vaccini: Garante privacy, comunicazione diretta a famiglie scelta ragionevole - Dichiarazione dell'Ufficio del Garante privacy del 21 agosto 2017
- M5S: Garante privacy, istruttoria su attacco hacker – Dichiarazione dell'Ufficio del Garante privacy del 10 agosto 2017

NEWSLETTER
del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).
Direttore responsabile: Baldo Meo.
Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n. 121 - 00186 Roma.
Tel: 06.69677.2752 - Fax: 06.69677.3755
Newsletter è consultabile sul sito Internet *www.garanteprivacy.it*