Newsletter
NOTIZIARIO
ANNO XXII
WWW.GARANTEPRIVACY.IT
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NEWSLETTER N. 463 del 6 marzo 2020

Prescritte ad un gestore misure urgenti per la sicurezza del servizio pec

Il provvedimento a tutela degli utenti reso noto solo oggi per impedire lo sfruttamento delle vulnerabilità rilevate nel corso di un'ispezione

Il Garante per la protezione dei dati personali con un provvedimento d'urgenza (/garante/doc.jsp?ID=9283040) ha prescritto ad Aruba Pec S.p.a. l'implementazione di misure per la messa in sicurezza del proprio servizio di posta elettronica certificata, che gestisce oltre sei milioni di caselle utilizzate da soggetti pubblici (come amministrazioni centrali e locali dello Stato), società private e singoli professionisti.

A seguito delle vulnerabilità rilevate durante un accertamento ispettivo in merito alla gestione del servizio pec, condotto nella seconda metà del 2019, l'Autorità ha adottato un provvedimento urgente per evitare che diverse categorie di interessati coinvolti (intestatari delle caselle pec, mittenti e destinatari dei messaggi, soggetti i cui dati sono presenti all'interno dei messaggi o degli allegati) fossero esposti a gravi rischi per i diritti e le libertà derivanti da possibili utilizzi impropri di dati personali o da furti d'identità.

La pubblicazione del provvedimento è stata però posticipata per dare modo alla società di implementare le misure prescritte e impedire che le vulnerabilità rilevate potessero essere sfruttate da eventuali malintenzionati. La società ha dichiarato di aver adempiuto, nei termini previsti, alle prescrizioni impartite.

Dagli accertamenti è emerso che circa 560.000 utenti utilizzavano ancora, per l'accesso alla propria casella pec, la password iniziale, scelta per loro da uno degli 8.900 partner della società (come ordini professionali, Pa e soggetti privati) senza che fosse imposto, come avrebbe dovuto, l'obbligo di modifica al primo accesso. Le procedure informatiche adottate contenevano, poi, ulteriori gravi vulnerabilità. Ad esempio, le password tecniche di gestione di alcuni servizi informatici erano riportate in chiaro nei log di tracciamento delle operazioni, aumentando così considerevolmente la possibilità di accessi illeciti, sia da parte di soggetti interni non autorizzati che in caso di attacco informatico.

Un'altra criticità riguardava la possibilità di consultare ed esportare, da rete internet, i log dei messaggi scambiati da oltre 6 milioni di caselle pec. Tale operazione era per altro effettuabile da un'utenza, con elevati privilegi di amministrazione (superadmin), utilizzata da più persone, in violazione dei più elementari principi di sicurezza del trattamento (che richiedono invece l'attribuzione a ogni operatore di credenziali individuali) e senza un'adeguata valutazione dei rischi connessi alla possibilità di accedere a queste

informazioni, anche al di fuori della rete aziendale.
Il Garante ha quindi imposto ad Aruba Pec S.p.a. la modifica obbligatoria delle password di accesso alle caselle di posta certificata rilasciate in modo non sicuro, la ridefinizione delle modalità di tracciamento, prevedendo che i log prodotti non contengano informazioni non indispensabili per le finalità di controllo e sicurezza, nonché un intervento sulle modalità di consultazione ed esportazione dei log dei messaggi inviati o ricevuti da tutte le caselle pec.
Con successivo provvedimento il Garante valuterà ulteriori aspetti del trattamento dei dati svolto da Aruba Pec S.p.a., nonché il complesso delle violazioni rilevate.

Sanità: più tutele privacy nei bandi di gara

Importante novità per le gare pubbliche nel settore sanitario. Alcuni bandi riguardanti l'acquisto di apparecchiature e dispositivi medici saranno infatti modificati per renderli maggiormente conformi alla disciplina sulla privacy e assicurare maggiori tutele per i dati dei pazienti. È questo il risultato della collaborazione avviata tra il Garante per la protezione dei dati personali e la Consip, dopo che lo stesso Garante era intervenuto nei confronti di un'azienda sanitaria che aveva comunicato illecitamente dati sulla salute dei pazienti ad una società fornitrice di apparecchiature diagnostiche.
Nei nuovi bandi di gara riguardanti l'acquisto delle apparecchiature e dei dispositivi medici da parte delle strutture sanitarie, Consip inserirà idonee misure a tutela dei dati trattati, come ad esempio l'impossibilità per il fornitore, che esegue un'attività di manutenzione a distanza dell'apparecchio, di accedere direttamente ai dati anagrafici dei pazienti presenti nelle immagini diagnostiche.
Nelle future gare d'appalto sarà inserita, inoltre, come clausola standard di contratto, la nomina dell'aggiudicatario quale responsabile del trattamento.
Consip avvierà anche un confronto con le società interessate ai bandi di gara per definire e comprendere quali funzionalità possano essere programmate sulle apparecchiature nel rispetto dei principi di privacy by design e by default, fissati dal Regolamento europeo, soprattutto con riferimento al servizio di assistenza e manutenzione a distanza delle apparecchiature.
Sulla base delle indicazioni fornite dall'Autorità, la Consip ha infine provveduto a modificare i bandi in corso anche per quanto riguarda le modalità di acquisizione delle immagini diagnostiche anonimizzate, da parte delle società partecipanti alle gare, per dimostrare la sussistenza dei requisiti tecnico-funzionali richiesti nei capitolati.

Scuola, graduatorie docenti: no alla pubblicazione di dati sulla salute o non necessari

Sanzionate due scuole della regione Campania

Il Garante per la privacy ha comminato sanzioni di 4000 euro ciascuna a due Licei della regione Campania per aver diffuso illecitamente informazioni non necessarie e dati sulla salute nelle graduatorie dei docenti pubblicate sui siti web degli istituti. [doc. web. nn. 9283029 (/garante/doc.jsp?ID=9283029)e 9283014 (/garante/doc.jsp?ID=9283014)]
L'Autorità, intervenuta a seguito dei reclami di due cittadini, ha riscontrato violazioni nella pubblicazione di dati personali riguardanti circa 1500 docenti in un caso e più di 2000 nell'altro.
Oltre ai dati identificativi, erano stati pubblicati in chiaro sul web, per alcuni anni, dati personali dei docenti non necessari rispetto alle finalità perseguite con la pubblicazione delle graduatorie: codici fiscali, indirizzi di residenza, recapiti telefonici, indirizzi e-mail, numero di figli, codici di preferenza.
Le graduatorie, rimosse dalle scuole a seguito dell'intervento del Garante, contenevano anche dati sulla salute di 25 docenti di un liceo e di 20 dell'altro: accanto al nominativo di alcuni insegnanti compariva infatti una sigla che indicava, in base alla disciplina di

settore in materia di istruzione, l'appartenenza alle categorie di "invalidi e mutilati civili".

L'Autorità, dopo aver dichiarato illecita la pubblicazione di tali dati personali, perché avvenuta in assenza di un presupposto normativo e in violazione dei principi di "liceità, correttezza e trasparenza", di "minimizzazione dei dati", nonché del divieto di diffusione di dati relativi alla salute, ha quindi sanzionato gli istituti.

Privacy: luci e ombre sulla gestione dei data breach. I risultati dello Sweep 2019

Sulla gestione dei data breach c'è una conoscenza approfondita, ma limitata a pochi organismi. È quanto emerge da un'indagine internazionale svolta dalle Autorità per la protezione dei dati personali di 16 Paesi, tra cui l'Italia, e coordinata dall'Autorità neozelandese (Office of the Privacy Commissioner).

Considerata la mole di informazioni raccolte e conservate dai soggetti pubblici e privati, è inevitabile che in determinate circostanze si verifichino accessi, comunicazioni o acquisizioni di dati personali in forma non autorizzata. Per questi motivi, sottolinea l'indagine, l'approccio a queste violazioni di dati - in termini sia di segnalazione/notifica sia di adozione di misure atte a prevenire il ripetersi della violazione - riveste importanza fondamentale per le Autorità di protezione dati e per le persone i cui dati sono stati violati.

Lo Sweep ("indagine a tappeto"), che viene annualmente portato avanti dal Gpen (Global Privacy Enforcement Network), ha preso quest'anno in esame le modalità di gestione e reazione in caso di violazioni dei dati nei diversi paesi. Sono stati somministrati questionari a 1145 soggetti, tra pubblici e privati, ma solo il 21% (258) ha fornito risposte puntuali.

Tra i motivi ipotizzati dai coordinatori dello Sweep riguardo al limitato numero di soggetti che ha deciso di rispondere alle domande dell'inchiesta, c'è anche il timore che, nei Paesi dove la segnalazione dei data breach è obbligatoria, i Garanti nazionali possano avviare attività di accertamento e sanzione sulla base delle risposte fornite.

Alla luce dei risultati emersi, le singole Autorità dovranno ora valutare quali interventi si rendano necessari per migliorare il controllo degli utenti sui dati personali che li riguardano.

I risultati dello Sweep

Fra i dati positivi emerge che l'84% dei soggetti intervistati nei diversi Paesi hanno designato un'equipe o un gruppo incaricati della gestione delle violazioni di dati nonché della ricezione delle relative segnalazioni.

Nel 75% dei casi le procedure prevedono fasi essenziali quali attività di contenimento, di valutazione e di analisi dei rischi associati.

Nel 18% dei casi le risposte fornite in merito a tali procedure sono insufficienti, e ciò segnala la necessità di maggiore chiarezza rispetto alle politiche da seguire in modo da assicurare l'adozione di tutte le misure fondamentali per rispondere a una violazione dei dati.

Il 65% degli organismi dispone di procedure buone o eccellenti in caso di violazione dei dati al fine di prevenire quelle future. Per il rimanente 35% le procedure previste risultano insufficienti o non vengono specificate.

Gli organismi che hanno risposto di non avere politiche interne in caso di violazioni di dati hanno specificato di fare riferimento agli orientamenti forniti dalla competente Autorità di protezione dati, ove necessario. In un caso, l'organismo ha descritto il sistema di valutazione delle violazioni, spiegando di avere implementato un meccanismo di rating a tre colori (rosso, arancio, verde - RAG); il rating tiene conto del numero di dati violati, della sensibilità delle informazioni, del disagio causato, del contenimento o non-contenimento della violazione, della possibilità di recuperare i dati e dell'eventuale applicazione di dispositivi di cifratura.

In 12 dei 16 Paesi che hanno partecipato allo Sweep sono previsti obblighi di notifica delle violazioni di dati. La quasi totalità degli organismi interpellati conosce il quadro giuridico di riferimento, compresi i criteri e le tempistiche per tale notifica. Solo cinque organismi hanno evidenziato una scarsa conoscenza del quadro giuridico.

La maggioranza di essi giudica utili le indicazioni fornite dalle rispettive Autorità di protezione dei dati in materia di notifica delle

violazioni di dati. La scarsità di risorse ha tuttavia impedito ai soggetti di minori dimensioni di mettere a punto tecniche e procedure sofisticate per la gestione delle violazioni.
Molte strutture fanno registrare dati negativi quanto al monitoraggio della performance interna con riguardo agli standard in materia di protezione dei dati: oltre il 30% non dispone di programmi per l'autovalutazione né per la conduzione di audit interni.
Il 45% circa degli organismi che hanno risposto allo sweep hanno dichiarato di tenere registri aggiornati di tutte le violazioni (anche di quelle potenziali).

Il Gpen

La Rete globale per l'attuazione della privacy (Global Privacy Enforcement Network (https://www.privacyenforcement.net/), Gpen) è nata nel 2010 in seguito a raccomandazioni dell'Ocse. La rete, che ha natura informale e comprende oltre 60 Autorità di 39 paesi, mira a promuovere la cooperazione internazionale fra le Autorità per la privacy in un contesto sempre più globale, ove consumatori e imprese necessitano di un flusso costante di informazioni personali a prescindere dalle frontiere nazionali.

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

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

- Assistenti digitali (smart assistant): i consigli del Garante per un uso a prova di privacy - Vademecum del 4.03.2020 (/temi/assistenti-digitali)
- Lotteria degli scontrini: ok del Garante privacy - Comunicato del 3 marzo 2020 (/garante/doc.jsp?ID=9282894)
- Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati - Comunicato del 2 marzo 2020 (/garante/doc.jsp?ID=9282117)
- Soro replica a Visco su presunti ostacoli privacy ad efficienza P.A. - Comunicato del 25 febbraio 2020 (/garante/doc.jsp?ID=9276991)

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 Venezia, n. 11 - 00187 Roma.
Tel: 06.69677.2751 - Fax: 06.69677.3785
Newsletter è consultabile sul sito Internet *www.garanteprivacy.it (http://www.garanteprivacy.it/)*

Iscrizione alla Newsletter - Cancellazione dal servizio - Informazioni sul trattamento dei dati personali
(https://www.garanteprivacy.it/home/stampa-comunicazione/newsletter)