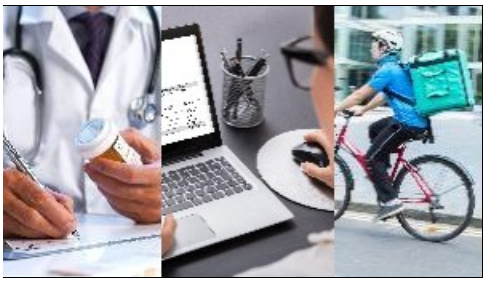
Newsletter
NOTIZIARIO
ANNO XXII
WWW.GARANTEPRIVACY.IT
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NEWSLETTER N. 462 del 18 febbraio 2020

Faro del Garante Privacy su sanità, fatturazione elettronica, food delivery

Approvato il piano ispettivo del primo semestre 2020. Nel 2019 sfiorati 16 milioni di euro di sanzioni



Approvato dal Garante Privacy il piano ispettivo per il primo semestre 2020. (/garante/doc.jsp?ID=9269607) L'attività di accertamento dell'Autorità, svolta anche in collaborazione con il Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza, riguarderà i trattamenti di dati svolti nell'ambito di settori particolarmente delicati, a partire da quello della sanità. Le verifiche riguarderanno, in particolare, gli enti pubblici che si occupano della cosiddetta "medicina di iniziativa" (un nuovo modello assistenziale per limitare gli effetti delle malattie croniche) e le società multinazionali del settore farmaceutico e sanitario.

Ulteriori accertamenti riguarderanno anche i trattamenti di dati effettuati dagli intermediari che operano nell'ambito della fatturazione elettronica, dalle società che gestiscono banche dati reputazionali e dalle società di food delivery. Le altre ispezioni programmate dal Garante saranno indirizzate a verificare il rispetto delle norme nel rilascio di certificati tramite l'Anagrafe nazionale della popolazione residente, nell'attività di marketing, nell'e-banking, nella gestione delle carte di fedeltà, nell'uso di software per la gestione delle segnalazioni di condotte illecite (il cosiddetto "whistleblowing"), nelle violazioni della sicurezza dei dati (data breach), sia nel settore pubblico che privato.

I controlli si concentreranno anche sull´adozione delle misure di sicurezza da parte di pubbliche amministrazioni e di imprese che trattano particolari categorie di dati personali, sul rispetto delle norme sulla informativa e il consenso, sui tempi di conservazione dei dati. L'attività ispettiva verrà svolta anche a seguito di segnalazioni e reclami, con particolare attenzione alle violazioni più gravi.

Un primo bilancio dell´attività ispettiva e sanzionatoria dell´ Autorità nel 2019 registra l'applicazione di sanzioni per 15.910.390 di euro. Sono state effettuate, inoltre, iscrizioni a ruolo per un importo complessivo di 12.243.267 euro, riguardanti trasgressori che non si sono avvalsi della facoltà di definizione agevolata prevista dal decreto legislativo n.101 del 2018.

Gli accertamenti svolti nel 2019, anche con il contributo del Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza, in linea con il piano ispettivo del 2018, hanno riguardato numerosi settori, sia nell´ ambito pubblico che privato. Per quanto riguarda il settore privato le ispezioni si sono rivolte principalmente ai trattamenti effettuati da società di intermediazione finanziaria, tour operator, circoli sportivi, istituti bancari (con particolare riferimento ai flussi di dati verso l'anagrafe dei conti correnti), società che svolgono attività di marketing e fidelizzazione (anche con riferimento alla profilazione dei clienti).

Per quanto riguarda il settore pubblico l´attività di verifica si è concentrata sul Sistema statistico nazionale (Sistan), sullo Spid, sui software per la gestione del "whistleblowing" e sulle banche dati di rilevanti dimensioni.

Whistleblowing non sicuro: Garante privacy sanziona un'università per 30.000 €

Diffusi i nomi di chi aveva segnalato illeciti

Il datore di lavoro, che adotta procedure tecnologiche per la segnalazione anonima di possibili comportamenti illeciti (whistleblowing), deve verificare che le misure tecnico-organizzative e i software utilizzati siano adeguati a tutelare la riservatezza di chi invia le denunce. Lo ha ribadito il Garante per la protezione dei dati personali (/garante/doc.jsp?ID=9269618)nel sanzionare un'università per aver reso accessibili on line i dati identificativi di due persone che avevano segnalato all'ateneo possibili illeciti.

L'università aveva dichiarato che, a causa di un aggiornamento della piattaforma software utilizzata, si era verificata la sovrascrittura accidentale dei permessi di accesso ad alcune pagine web interne dell'applicativo usato per il whistleblowing, rendendo così possibile a chiunque consultare i nomi e altri dati di coloro che avevano inviato segnalazioni riservate. Tali informazioni erano di conseguenza state indicizzate da alcuni motori di ricerca fino a che l'università, dopo essere venuta a conoscenza del problema, era intervenuta per farli deindicizzare e cancellare le relative copie cache.

Nel corso dell'istruttoria è stato rilevato che la violazione dei dati personali (data breach) era riconducibile all'assenza di adeguate misure tecniche per il controllo degli accessi, che avrebbero consentito di limitare la consultazione al solo personale autorizzato. In base al Regolamento spetta in primo luogo proprio al titolare del trattamento (in questo caso l'ateneo) - tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento - mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio. Tra queste rientra anche una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure adottate. Nel caso di specie invece l'università si è limitata a recepire le scelte progettuali del fornitore dell'applicativo che non prevedeva la cifratura dei dati personali (identità del segnalante, informazioni relative alla segnalazione, eventuale documentazione allegata), né l'adozione di un protocollo di trasmissione che garantisse una comunicazione sicura, sia in termini di riservatezza e integrità dei dati scambiati, sia di autenticità del sito web visualizzato da chi invia le segnalazioni. La gravità della violazione risulta acuita dal particolare regime di riservatezza stabilito dalle norme in materia di whistleblowing, proprio a maggior tutela degli interessati.

Il Garante, quindi, dopo aver accertato l'illecito trattamento dei dati e l'omesso adempimento degli obblighi di sicurezza imposti dal Gdpr - tenendo comunque conto che la violazione ha riguardato solo due persone e che l'Ente ha attivamente cooperato nel corso dell'istruttoria - ha inflitto all'ateneo una sanzione amministrativa di 30.000 euro.

Garante, no agli accessi indebiti ai dossier sanitari

Sanzione da 30mila € a un'azienda ospedaliera: alcuni dipendenti "sbirciavano" i dati dei colleghi

Non aver impedito che i dipendenti potessero "sbirciare" il dossier sanitario dei colleghi costerà ad un'azienda ospedaliera 30.000 euro. A tanto ammonta la sanzione comminata dal Garante (/garante /doc.jsp?ID=9269629) privacy per tre violazioni di dati personali comunicate all'Autorità dallo stesso ospedale a conclusione di normali controlli periodici. Gli accessi indebiti hanno riguardato dati sanitari di dipendenti in cura presso lo stesso nosocomio. In un caso l'accesso era stato effettuato con le credenziali di un medico che aveva lasciato incustodita la propria postazione; negli altri due casi uno specializzando e un tecnico radiologo erano entrati nel dossier sanitario dei loro colleghi.

In tutti e tre gli episodi risulta accertato, per stessa ammissione dell'azienda ospedaliera, che gli accessi erano stati effettuati non per erogare prestazioni mediche, ma per esclusive ragioni personali, descritte dall'azienda come "mera curiosità".

Gli accertamenti svolti dal Garante hanno evidenziato che le misure tecniche e organizzative adottate dall'ospedale, a tutela del dossier sanitario aziendale, non si erano dimostrate idonee ad assicurare una adeguata tutela dei dati personali dei pazienti e a proteggerli da trattamenti non autorizzati, determinando così un trattamento illecito di dati.

La violazione avrebbe potuto essere evitata se l'azienda avesse semplicemente osservato le Linee guida in materia di dossier sanitario, emanate dal Garante nel 2015, prevedendo che l'accesso al dossier sanitario fosse limitato al solo personale sanitario che interviene nel processo di cura del paziente ed avesse prestato particolare attenzione nell'individuare i profili di autorizzazione e nella formazione del personale abilitato. L'adozione preventiva di tali misure, anche alla luce dei principi di protezione dati fin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default), costituisce oggi, per effetto delle disposizioni contenute nel Regolamento Ue 679/2016, un preciso dovere per i titolari del trattamento.

Il Garante, nel prendere atto che in seguito alla vicenda l'azienda ha avviato spontaneamente la revisione delle procedure d'accesso ai dossier sanitari, ha ingiunto alla stessa di completare tale operazione entro 90 giorni e per gli illeciti commessi ha applicato una sanzione di 30.000 euro.

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

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

Big Data: pubblicata indagine Agcom, Agcm e Garante privacy (/garante/doc.jsp?ID=9264204) - Comunicato del 10 febbraio 2020

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)