GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Newsletter 25/03/19 - Sanità dopo il Gdpr, i chiarimenti del Garante - Banche, dati sanitari, carte fedeltà nel piano ispettivo del Garante Privacy

Newsletter
NOTIZIARIO
ANNO XXI
WWW.GARANTEPRIVACY.IT

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NEWSLETTER N. 451 del 25 marzo 2019

Sanità dopo il Gdpr, i chiarimenti del Garante

I medici possono trattare i dati dei pazienti per finalità di cura senza consenso

I medici potranno trattare i dati dei pazienti, per finalità di cura, senza dover richiedere il loro consenso, ma dovranno comunque fornire loro informazioni complete sull’uso dei dati. Il medico che opera come libero professionista non è tenuto a nominare il Responsabile della protezione dati. Tutti gli operatori del settore dovranno tenere un registro dei trattamenti dei dati.

Questi sono i principali chiarimenti forniti dal Garante della privacy a cittadini, medici, asl e soggetti privati, sulle novità introdotte, in ambito sanitario, dal Regolamento UE in materia di protezione dei dati (GDPR) e dalla normativa nazionale.

Il provvedimento generale, adottato dall’Autorità, intende favorire un’interpretazione uniforme della nuova disciplina, ancora in fase transitoria, e supportare gli operatori con informazioni utili alla sua corretta attuazione.

Il Garante ha chiarito, ad esempio, che il professionista sanitario (come il medico), soggetto al segreto professionale, non deve più richiedere il consenso per i trattamenti di dati necessari alla prestazione sanitaria.

E' invece richiesto il consenso, o una differente base giuridica, quando tali trattamenti non sono strettamente necessari per le finalità di cura, anche quando sono effettuati da professionisti della sanità. Ne sono un esempio i trattamenti di dati sulla salute connessi all'uso di "App" mediche (ad eccezione di quelle per la telemedicina), quelli effettuati per la fidelizzazione della clientela (come quelli praticati da alcune farmacie o parafarmacie), oppure per finalità promozionali, commerciali o elettorali.

L'Autorità ricorda che, sulla base dell'attuale normativa che regola il settore, permane la necessità di acquisire il consenso anche per il trattamento dei dati relativo al fascicolo sanitario elettronico, o per la consultazione dei referti online.

Nel documento del Garante sono forniti chiarimenti anche in merito all'informativa agli interessati, che deve essere concisa, trasparente, intelligibile e facilmente accessibile, scritta con linguaggio semplice e chiaro. Rispetto al modello pre-GDPR, essa deve contenere maggiori informazioni a tutela dell'interessato quali, ad esempio, quelle relative ai tempi di conservazione dei dati, che - se non sono specificati dalla normativa di settore - dovranno comunque essere individuati dal titolare (ad esempio il medico specialista o l'ospedale).

Il Garante dedica una sezione anche al Responsabile per la protezione dei dati (RPD, DPO nell'acronimo inglese). Sono tenuti alla nomina del RPD tutti gli organismi pubblici, nonché gli operatori privati che effettuano trattamenti di dati sanitari su larga scala, quali le case di cura. Non sono invece tenuti alla sua nomina i liberi professionisti o altri soggetti, come le farmacie, che non effettuano trattamenti su larga scala.

L'Autorità infine chiarisce che è obbligatorio per tutti gli operatori sanitari tenere un registro nel quale sono elencate le attività di trattamento effettuate sui dati dei pazienti. Tale documento rappresenta, in ogni caso, un elemento essenziale per il "governo dei trattamenti" e per l'efficace individuazione di quelli a maggior rischio, anche per dimostrare il rispetto del principio di responsabilizzazione (accountability) previsto da GDPR.

VEDI L'INFOGRAFICA

Banche, dati sanitari, carte fedeltà nel piano ispettivo del Garante Privacy

Con oltre 8 milioni di euro di sanzioni riscosse il bilancio 2018 segna un incremento del +116%

Istituti di credito, sanità, sistema statistico nazionale (Sistan), Spid, telemarketing, carte di fedeltà, grandi banche dati pubbliche. Sono questi i settori sui quali nei prossimi mesi punterà la sua lente il Garante per la protezione dei dati personali contenuti nel piano ispettivo per il primo semestre 2019 approvato nelle scorse settimane.

L'attività ispettiva, svolta anche in collaborazione con il Nucleo speciale privacy della Guardia di finanza, riguarderà innanzitutto i trattamenti di dati effettuati dalle banche, con particolare riferimento ai flussi legati all'anagrafe dei conti; i trattamenti di dati effettuati dalle Asl e poi trasferiti a terzi per il loro utilizzo a fini di ricerca; la gestione delle carte di fidelizzazione da parte delle aziende; il rilascio dell´identità digitale ai cittadini italiani (Spid); il Sistema Integrato di Microdati (Sim) dell´Istat.

I controlli si concentreranno anche sull´adozione delle misure di sicurezza da parte di pubbliche amministrazioni e di imprese che trattano dati sensibili, il rispetto delle norme sull´informativa e il consenso, la durata della conservazione dei dati da parte di soggetti pubblici e privati. L'attività ispettiva verrà svolta anche in riferimento a segnalazioni e reclami con particolare attenzione alle violazioni più gravi.

Intanto il bilancio 2018 dell´attività ispettiva dell´Autorità conferma l'incremento dell´attività sanzionatoria già registrato lo scorso anno.

Nel corso del 2018 sono state adottate 175 ordinanze-ingiunzione, a fronte delle 109 del 2017 ed è stato rilevato un notevole aumento delle somme riscosse pari a 8.161.806 euro, a fronte dei 3.776.694 euro registrati nel 2017 (con una variazione positiva del +116%).

Da registrare inoltre un incremento del 20% delle violazioni amministrative contestate: 707 nel 2018 rispetto alle 589 contestazioni del 2017.

Le contestazioni hanno riguardato la violazione di disposizioni del Codice per illeciti commessi prima della data di applicazione del Regolamento (UE) 2016/679.

Sono invece diminuite le segnalazioni all´autorità giudiziaria: 27 nel 2018 rispetto alle 41 del 2017.

Gli accertamenti, svolti nel 2018 anche con il contributo delle Unità Speciali della Guardia di finanza, Nucleo speciale privacy, hanno riguardato numerosi e delicati settori, sia nell´ambito pubblico che privato. Per quanto riguarda il settore privato le ispezioni si sono rivolte principalmente ai trattamenti effettuati: dagli istituti di credito, da società per attività di rating sul rischio e sulla solvibilità delle imprese, dalle aziende sanitarie locali e poi trasferiti a terzi per il loro utilizzo a fini di ricerca, da società che svolgono attività di telemarketing, da società che offrono servizi di "money transfer". Oggetto di particolare accertamento anche i trattamenti di dati svolti da società assicuratrici attraverso l'installazione di "scatole nere" a bordo degli autoveicoli e da società che offrono servizi medico-sanitari tramite app.

Per quanto riguarda il settore pubblico l´attività di verifica si è concentrata su enti pubblici, soprattutto Comuni e Regioni, che svolgono trattamenti di dati personali mediante app per smartphone e tablet, con particolare attenzione all'eventuale profilazione e geolocalizzazione degli utenti; sulle grandi banche dati; sul sistema della fiscalità, con speciale riguardo alle misure di sicurezza e al sistema degli audit; sul sistema informativo dell´Istat e sullo Spid.

No al "braccialetto" elettronico al polso degli operatori ecologici

Il Garante per la privacy chiede l'adozione di dispositivi rispettosi della dignità dei lavoratori

Bocciato il "braccialetto" elettronico al polso degli operatori ecologici. Il Garante per la privacy ha chiesto ad una società che si occupa della raccolta dei rifiuti per conto della municipalizzata di un comune toscano di utilizzare dispositivi elettronici alternativi che non ledano la dignità della persona.

La pronuncia è arrivata a conclusione di un procedimento aperto d'ufficio sull'onda dell'interesse mediatico suscitato dalla vicenda,

Nell'aprile dello scorso anno la società aveva consegnato a più di 70 dipendenti addetti alla pulizia delle strade dei dispositivi indossabili dotati anche di un gps, con i quali effettuare la lettura delle etichette elettroniche collocate sui cestini getta rifiuti e segnalare l'eventuale spostamento di quelli non ancorati al suolo. Obiettivo dichiarato della società era quello di rendicontare il lavoro svolto all'Azienza municipalizzata comunale.

Solo dopo l'avvio dell'istruttoria dell'Autorità la società aveva stipulato un accordo sindacale nel quale si stabiliva, tra l'altro, la lettura quotidiana dei tag per ogni turno di lavoro e si limitava l'attivazione del gps al massimo ad un turno di lavoro a settimana, previa comunicazione al lavoratore.

L'Autorità, pur giudicando tale configurazione non in contrasto con i principi di necessità e proporzionalità del Regolamento Ue rispetto alle finalità perseguite dalla società, ha tuttavia ritenuto necessario individuare ulteriori misure maggiormente rispettose della dignità dei lavoratori.

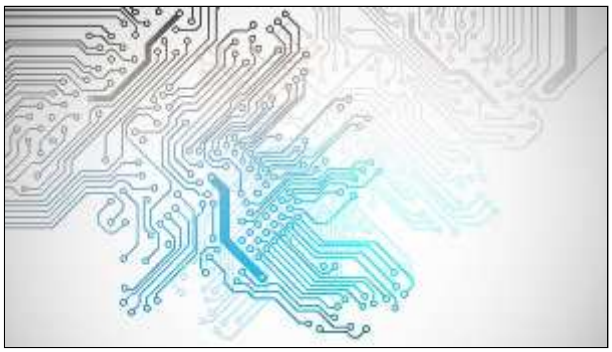
Il sistema consente infatti il trattamento di dati personali di lavoratori identificabili. Sebbene i "braccialetti" siano collegati alle zone di spazzamento e non ai singoli dipendenti, attraverso i registri dei turni di lavoro è possibile individuare il dipendente che ha effettuato le rilevazioni dei tag e, quando previsto, la relativa geolocalizzazione mediante il gps. Il Garante ha quindi prescritto alla società di individuare tempi di conservazione dei registri, cartacei e digitali, strettamente necessari a gestire le eventuali contestazioni da parte della società municipalizzata e descrivere nel dettaglio i casi specifici nei quali sarà possibile incrociare le informazioni. Analoghe cautele dovranno essere adottate nei confronti dei dati raccolti attraverso la lettura giornaliera dei tag, in grado di ricostruire nel dettaglio l'attività del lavoratore. La società dovrà, inoltre, adottare misure tecnologiche e organizzative per mantenere separate le basi di dati, in particolare quelli trattati attraverso i registri, quando ne sia comunque necessaria la conservazione a fini amministrativi.

Il Garante ha peraltro raccomandato, come indicato anche nell'accordo sindacale, l'adozione di un dispositivo che per le sue caratteristiche esteriori non sia lesivo della dignità e comunque non sia percepito come tale dal dipendente, considerato che dovrà essere utilizzato, anche se con diverse funzionalità, dai lavoratori per ogni turno di servizio.

L'Autorità ha ricordato, infine, alla società di effettuare una valutazione di impatto sulla protezione dei dati, come previsto dal Regolamento Ue, tenuto conto delle concrete caratteristiche del sistema tecnologico.

Privacy e intelligenza artificiale: vigilare sugli algoritmi

Il contributo del Garante italiano nel Comitato consultivo della Convenzione 108



Le applicazioni dell'intelligenza artificiale (AI) devono rispettare i diritti fondamentali, incluso quello alla protezione dei dati. Sviluppatori, produttori e fornitori di servizi AI devono valutare preventivamente i possibili rischi, adottando un approccio di tipo "precauzionale". Necessarie precise prescrizioni nelle procedure di appalto pubblico. Queste alcune delle indicazioni delle linee guida presentate - nel corso della Giornata della Protezione dei dati 2019 - dal Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108/1981), che dal 2016 è presieduto dalla rappresentante del Garante della privacy italiano.

Le linee-guida, (reperibili al link https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8, di cui è resa disponibile sul sito del Garante una traduzione a cura dell'Ufficio), si rivolgono a decisori pubblici, sviluppatori e fornitori di servizi basati sull'AI, come quelli utilizzati nell'ambito della domotica, delle smart cities, della sanità e della prevenzione del crimine. In particolare, sono evidenziati i principi da rispettare affinché l'impiego di tale tecnologia avvenga nel rispetto dei principi della nuova Convenzione 108 (nota come "Convenzione 108+"), adottata lo scorso 18 maggio 2018, e già firmata da 26 Paesi tra cui l'Italia.

Si sottolinea, innanzi tutto, che ogni progetto basato sull'intelligenza artificiale dovrebbe rispettare la dignità umana e le libertà fondamentali, nonché i principi base di liceità, correttezza, specificazione della finalità, proporzionalità del trattamento, protezione dei dati fin dalla progettazione (privacy by design) e protezione per impostazione predefinita (privacy by default), responsabilità e dimostrazione della conformità (accountability), trasparenza, sicurezza dei dati e gestione dei rischi.

Tra i punti cardine del documento si segnala la necessità di adottare un approccio fondato sulla preventiva valutazione dell'impatto che sistemi, software e dispositivi basati sull'intelligenza artificiale possono avere su diritti fondamentali, nonché sulla minimizzazione dei relativi rischi per le persone evitando, tra l'altro, potenziali pregiudizi (bias) ed altri effetti discriminatori, come quelli basati sulla differenza di genere o sulle minoranze etniche. Il Comitato consultivo rimarca, tra l'altro, l'opportunità di inserire nel processo di valutazione nuove "forme partecipatorie", basate sul coinvolgimento di individui e di gruppi potenzialmente colpiti dagli effetti dell'AI.

Varie le indicazioni anche per la pubblica amministrazione che dovrebbe, ad esempio, predisporre procedure di appalto pubblico dove si impongano a sviluppatori, produttori e fornitori di servizi di AI, specifici obblighi di trasparenza, la valutazione preliminare dell'impatto del trattamento dei dati sui diritti umani e sulle libertà fondamentali, e l'obbligo di "vigilanza sugli algoritmi", in particolare sugli effetti negativi e sulle conseguenze derivanti dalle applicazioni AI.

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

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

- Il Garante Privacy blocca il video su un uomo che compie atti autolesionistici in Commissariato - Comunicato del 22 marzo 2019

- Protocollo d'intesa tra Garante e Co.Re.Com. del Piemonte in materia di prevenzione e contrasto del fenomeno del cyberbullismo - 20 marzo 2019

- Garante Privacy su immagini deputata M5S - Comunicato del 13 marzo 2019

- Memoria del Presidente del Garante per la protezione dei dati personali nell'ambito dell'esame del disegno di legge C. 1637 Governo, approvato dal Senato, recante "Conversione in legge, con modificazioni, del decreto-legge 28 gennaio 2019, n. 4, recante disposizioni urgenti in materia di reddito di cittadinanza e di pensioni - 7 marzo 2019

- Privacy e sicurezza: l'iniziativa di Garante privacy e Intelligence a tutela dei cittadini. Firmato un nuovo Protocollo d'intenti tra Autorità Garante e Servizi segreti in linea con il nuovo Regolamento Ue - Comunicato congiunto del 6 marzo 2019

- Firmato dall'Italia il Protocollo emendativo della Convenzione 108 sulla protezione degli individui rispetto al trattamento automatizzato dei dati personali - Comunicato del 6 marzo 2019

- Indagine internazionale sul rispetto della privacy - Sweep 2018 - Comunicato del 5 marzo 2019

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*

Iscrizione alla Newsletter - Cancellazione dal servizio - Informazioni sul trattamento dei dati personali