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

NEWSLETTER N. 465 del 21 maggio 2020

• Processo amministrativo telematico: via libera del Garante privacy
• Conservazione documenti digitali: il Garante privacy chiede maggiori tutele
• Il ruolo degli Organismi di Vigilanza dopo il Gdpr
• Registro dei tumori della provincia di Trento: le indicazioni del Garante

---

Processo amministrativo telematico: via libera del Garante privacy

Parere favorevole (/garante/doc.jsp?ID=9347280) del Garante Privacy sullo schema di decreto del Presidente del Consiglio di Stato che fissa le regole tecniche per l'attuazione del processo amministrativo telematico, come modalità di trattazione della causa, alternativa a quella unicamente scritta, durante l'emergenza Covid19, nel periodo che va dal 30 maggio al 31 luglio 2020.

Il Garante auspica però che, cessata l'emergenza, Consiglio di Stato e Tar si dotino di una piattaforma gestita direttamente o comunque sotto il loro controllo.

Lo schema di decreto, mancando allo stato una disciplina tecnica specifica, stabilisce le modalità di collegamento, quelle di partecipazione dei difensori e dei magistrati, i tempi di discussione, le garanzie di sicurezza del sistema informativo, nonché lo svolgimento da remoto delle camere di consiglio dei magistrati. La celebrazione del processo in videoconferenza, prevista da un recente decreto legge in alternativa al contraddittorio cartolare, può essere chiesta dalle parti o disposta d'ufficio in qualsiasi udienza pubblica o camerale.

Il Garante ha ritenuto positivo, in particolare, il fatto che non sia consentita la registrazione delle udienze. Questo dovrebbe impedire infatti al provider, che offre il servizio di videoconferenza, di acquisire alcun dato personale al di fuori dei "metadati" necessari per il collegamento video da remoto (identificativi per l'autenticazione coincidenti con gli indirizzi email, indirizzi Ip delle postazioni, data e ora della connessione). Il ricorso alla videoconferenza, inoltre, sarebbe limitato alle sole udienze con presenza dei difensori essendo invece le camere di consiglio decisorie svolte di norma in "audioconferenza".

L'Autorità, pur prendendo atto delle soluzioni prospettate per fronteggiare l'attuale emergenza, auspica tuttavia che, una volta che questa sia cessata, si adotti una piattaforma interna, gestita dagli organi di Giustizia amministrativa o sotto il loro stretto controllo. La disponibilità di software open source del tutto comparabili per affidabilità e accuratezza ai migliori prodotti industriali, offre il vantaggio di prestarsi a "implementazioni" direttamente su datacenter e reti della Giustizia amministrativa, o comunque su infrastrutture gestite collettivamente da o con altre Pa. Tale soluzione eviterebbe in radice i rischi di flussi transfrontalieri interni o esterni all'Unione europea legati a soluzioni "cloud" di aziende extra-europee. Il parere richiama inoltre l'attenzione del Consiglio di Stato sull'esigenza di adottare ogni opportuna iniziativa volta alla formazione del personale sull'uso dei sistemi, anche per evitare inconvenienti, quali, ad esempio, l'ascolto delle udienze e delle camere di consiglio da parte di soggetti non autorizzati a partecipare.

L’Autorità, infine, ha rappresentato l’esigenza di interpretare la disciplina della pubblicazione on line delle “copie di studio” dei provvedimenti giurisdizionali alla luce della giurisprudenza della Cassazione e del Regolamento europeo, così includendo tra i casi di anonimizzazione obbligatoria anche quelli relativi ai dati sulla salute, genetici e biometrici.

Conservazione documenti digitali: il Garante privacy chiede maggiori tutele

Il parere dell’Autorità sulle linee guida AgID in caso di cessazione del servizio

L’AgID dovrà stabilire regole più precise per fare in modo che i soggetti che si occupano di conservazione dei documenti informatici rispettino a pieno la normativa sulla protezione dei dati personali, nel caso in cui la fornitura del servizio offerto a PA e a privati venga a cessare.

Questa la richiesta del Garante della privacy (/garante /doc.jsp?ID=9347287) in relazione alla bozza di “Linee guida per la stesura del piano di cessazione del servizio di conservazione”, predisposte dall’Agenzia per l’Italia digitale nell’ambito dell’attuazione del Codice per l’Amministrazione Digitale (Cad).

Lo schema sottoposto a parere individua regole tecniche e di indirizzo che aiutano il “conservatore” di documenti informatici (come quelli contabili e le dichiarazioni fiscali) a predisporre un piano per la corretta migrazione dei dati che eviti perdite di informazioni, sia in caso di cessazione del servizio che di ritiro dell’accreditamento da parte dell’AgID all’operatore che lo fornisce.

Nel predisporre tale piano, il conservatore deve tenere conto di molteplici variabili e fattori di rischio, tra cui il grado di interoperabilità nei processi di migrazione, l’affidabilità dell’impianto tecnologico, i livelli di aggiornamento e di sicurezza fisica e logica.

Nel parere finale, il Garante privacy ha chiesto all’AgID, di integrare lo schema in modo da assicurare specifiche tutele per i dati personali trattati in linea con il Regolamento europeo in materia, il cosiddetto GDPR.

Le Linee guida dovranno, in particolare, ricordare che la normativa impone al conservatore (che in questo caso riveste il ruolo di responsabile del trattamento) precisi obblighi in materia di restituzione dei dati al produttore (titolare del trattamento). A tale proposito, è importante che nel processo di cessazione venga coinvolto anche il responsabile per la protezione dei dati (cosiddetto Rpd/Dpo).

L’Autorità chiede poi che nelle Linee guida il conservatore sia invitato ad ampliare l’“analisi dei rischi”, tenendo conto di quelli connessi al trattamento dei dati personali valutando, tra l’altro, la presenza di dati personali di categorie particolari, come quelli relativi alla salute, alle condanne penali o a reati. Il conservatore dovrà inoltre adottare adeguate misure di sicurezza per il “trasferimento degli archivi di conservazione”, così da garantire riservatezza, integrità e disponibilità dei dati contenuti nei documenti.

Nel piano predisposto, il conservatore cessante dovrà infine indicare per quanto tempo sarà garantita l’accessibilità dei documenti, e definire modalità sicure per la “cancellazione degli archivi di conservazione”.

Queste indicazioni del Garante, insieme a quelle già proposte in un precedente parere (/garante/doc.jsp?ID=9283921) sulle “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici” consentiranno di aumentare la protezione dei dati personali contenuti nei documenti informatici, garantendo la sicurezza del trattamento, anche attraverso una più chiara attribuzione dei compiti e una corretta ripartizione delle responsabilità. Tali integrazioni permetteranno, se applicate, di condurre le pubbliche amministrazioni e le imprese verso una corretta innovazione dei processi, per una digitalizzazione a prova di privacy, riducendo i rischi per i diritti e le libertà degli interessati.

Il ruolo degli Organismi di Vigilanza dopo il Gdpr

I chiarimenti del Garante Privacy

Il Garante per la privacy ha precisato il ruolo e le responsabilità degli Organismi di Vigilanza (OdV) (/garante /doc.jsp?ID=9347842)riguardo ai trattamenti dei dati personali svolti nelle loro funzioni e ha escluso che essi possano essere qualificati come titolari autonomi o come responsabili del trattamento.

Gli OdV sono gli organi ai quali l’ente, ossia la persona giuridica, la società o l’associazione affida, nel rispetto della disciplina sulla

responsabilità amministrativa prevista dal decreto legislativo n. 231/2001, il compito di vigilare sull'osservanza dei modelli di organizzazione e di gestione adottati, allo scopo di prevenire i reati commessi nell'interesse o a vantaggio dell'ente, dai vertici dello stesso o da persone a questi sottoposti.

Nella risposta ad una richiesta di parere presentata da un'associazione rappresentativa dei componenti degli Organismi di Vigilanza, il Garante ha infatti chiarito che il Gdpr (Regolamento Ue 679/2016) si pone in linea di continuità con quanto già previsto dalla Direttiva europea sulla privacy del 1995 in relazione alla definizione del ruolo di titolare e responsabile del trattamento: il primo è il soggetto che "determina le finalità e i mezzi del trattamento di dati personali" e il secondo è colui che "tratta dati personali per conto del titolare del trattamento".

Gli OdV, sia pur dotati di autonomi poteri di iniziativa e controllo previsti dalla normativa 231 per l'espletamento delle loro funzioni, non possono essere considerati autonomi titolari del trattamento perché i loro compiti non sono determinati dagli Organismi stessi, ma dall'organo dirigente dell'ente che, nell'ambito del modello di gestione e organizzazione, ne definisce gli aspetti relativi al funzionamento, compresa l'attribuzione delle risorse, i mezzi e le misure di sicurezza.

Inoltre, l'OdV non può essere considerato neppure quale responsabile del trattamento, inteso come persona giuridicamente distinta dal titolare che agisce per conto di quest'ultimo secondo le istruzioni impartite. Il Gdpr, infatti, pur non modificandone l'essenza, prevede ora, in funzione della gestione dei dati svolta per conto del titolare, un serie di obblighi in capo al responsabile del trattamento, come pure la sua diretta responsabilità per l'eventuale inosservanza degli stessi. Al contrario, eventuali omessi controlli sull'osservanza dei modelli predisposti dall'ente non ricadono sull'OdV ma sull'ente stesso.

L'OdV nel suo complesso non è quindi distinto dall'ente ma è "parte dell'ente" che, quale titolare del trattamento, definisce il perimetro e le modalità di esercizio dei compiti assegnati all'organismo, nonché il ruolo che, in base alla disciplina in materia di protezione dei dati personali, deve essere previsto per i singoli membri che lo compongono. In particolare, l'ente designerà i singoli membri dell'OdV come soggetti autorizzati, i quali dovranno attenersi alle istruzioni del titolare.

Registro dei tumori della provincia di Trento: le indicazioni del Garante

Saranno necessari alcuni perfezionamenti per rendere lo schema di regolamento sull'esercizio del Registro Tumori della Provincia di Trento pienamente conforme al Regolamento europeo e al Codice privacy.

È quanto richiesto dal Garante per la protezione di dati personali nel parere reso alla Provincia (/garante/doc.jsp?ID=9344651).

Con il regolamento la Provincia di Trento si propone di individuare, oltre alle specifiche finalità perseguite dal Registro, che raccoglie informazioni sui malati di cancro residenti nel territorio, anche le operazioni eseguibili, i tipi di dati e i soggetti che li possono trattare. Lo schema disciplina anche la comunicazione e la diffusione delle informazioni in esso contenute ed è integrato da un apposito Disciplinare tecnico relativo alla sicurezza dei dati e dei sistemi.

Tra le disposizioni dello schema che necessitano ad avviso dell'Autorità di modifiche vi è quella che riguarda i tempi di conservazione dei dati, in conformità al principio di "limitazione della conservazione", prevista dal Regolamento Ue. Secondo il Garante la disposizione sulla conservazione dei backup per il ripristino dei dati per un periodo di 10 anni, in caso di guasti e malfunzionamenti del sistema, è insostenibile dal punto di vista economico e organizzativo e non in linea con le buone pratiche di settore. L'Autorità ha chiesto perciò di rimodulare il tempo di conservazione dei backup nell'ordine di grandezza di mesi e comunque non superiore all'anno.

Anche per quanto riguarda la sicurezza dei dati il Garante ha chiesto di perfezionare il testo e di inserire richiami normativi e contenuti conformi alla più recente normativa privacy europea e nazionale. Lo schema dovrà specificare, in particolare, che il titolare del trattamento dei dati contenuti nel Registro Tumori, individuato nell'Azienda provinciale per i servizi sanitari (APSS), è tenuto ad

adottare le misure tecniche e organizzative previste dal Regolamento europeo, anche a seguito di un'adeguata valutazione d'impatto sulla protezione dei dati, i cui dettagli andranno inseriti nel Disciplinare Tecnico.

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

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

- Covid-19, test sierologici sul posto di lavoro: i chiarimenti del Garante privacy (/garante/doc.jsp?ID=9343635) - Comunicato del 14 maggio 2020
- Audizione del Presidente del Garante per la protezione dei dati personali sull'affare assegnato atto n. 453 relativo al tema di Ricadute occupazionali dell'epidemia da Covid-19, azioni idonee a fronteggiare le situazioni di crisi e necessità di garantire la sicurezza sanitaria nei luoghi di lavor (/garante/doc.jsp?ID=9341993)o - 13 maggio 2020
- FAQ del Garante privacy su scuola, lavoro, sanità, ricerca ed enti locali. Chiarimenti e indicazioni per pubbliche amministrazioni e imprese private (/garante/doc.jsp?ID9337010) - Comunicato del 4 maggio 2020
- Registro elettronico: lettera del Presidente del Garante per la protezione dei dati personali, Antonello Soro, al Ministro dell’istruzione, Lucia Azzolina (/garante/doc.jsp?ID=9334326) - 4 maggio 2020
- Attenzione al ransomware. Il programma che prende "in ostaggio" il tuo dispositivo - La scheda informativa del Garante (/temi/cybersecurity/ransomware) -28 aprile 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/)*