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

NEWSLETTER N. 460 del 20 dicembre 2019

Lavoro: è illecito mantenere attivo l'account di posta dell'ex dipendente

Dopo la cessazione del rapporto di lavoro la società aveva avuto anche accesso alle email

Commette un illecito la società che mantiene attivo l'account di posta aziendale di un dipendente dopo l'interruzione del rapporto di lavoro e accede alle mail contenute nella sua casella di posta elettronica. La protezione della vita privata si estende anche all'ambito lavorativo.

Questi i principi ribaditi dal Garante per la privacy nel definire il reclamo di un dipendente che lamentava la violazione della disciplina sulla protezione dei dati da parte della società presso la quale aveva lavorato.

L'ex dipendente contestava, in particolare, alla società la mancata disattivazione della email aziendale e l'accesso ai messaggi ricevuti sul suo account. L'interessato era venuto a conoscenza di questi fatti per caso, nel corso di un giudizio davanti al giudice del lavoro promosso nei suoi confronti dalla sua ex azienda, avendo quest'ultima depositato agli atti una email giunta sulla sua casella di posta un anno dopo la cessazione dal servizio.

Dagli accertamenti svolti dall'Autorità è emerso che l'account di posta era rimasto attivo per oltre un anno e mezzo dopo la conclusone del rapporto di lavoro prima della sua eliminazione, avvenuta solo dopo la diffida presentata dal lavoratore. In questo periodo la società aveva avuto accesso alle comunicazioni che vi erano pervenute, alcune anche estranee all'attività lavorativa del dipendente.

Il Garante ha ritenuto illecite le modalità adottate dalla società perché non conformi ai principi sulla protezione dei dati, che impongono al datore di lavoro la tutela della riservatezza anche dell'ex lavoratore. Subito dopo la cessazione del rapporto di lavoro, un'azienda deve infatti rimuovere gli account di posta elettronica riconducibili a un dipendente, adottare sistemi automatici con indirizzi alternativi a chi contatta la casella di posta e introdurre accorgimenti tecnici per impedire la visualizzazione dei messaggi in arrivo.

L'adozione di tali misure tecnologiche - ha spiegato il Garante - consente di contemperare l'interesse del datore di lavoro di accedere alle informazioni necessarie alla gestione della propria attività con la legittima aspettativa di riservatezza sulla corrispondenza da parte di dipendenti/collaboratori oltre che di terzi. Lo scambio di email con altri dipendenti o con persone esterne all'azienda consente infatti di conoscere informazioni personali relative al lavoratore, anche solamente dalla visualizzazione dei dati esterni delle comunicazioni (data, ora oggetto, nominativi di mittenti e destinatari).

Oltre a dichiarare l'illecito trattamento, il Garante ha quindi ammonito la società a conformare i trattamenti effettuati sugli account di posta elettronica aziendale dopo la cessazione del rapporto di lavoro alle disposizioni e ai principi sulla protezione dei dati ed ha disposto l'iscrizione del provvedimento nel registro interno delle violazioni istituito presso l'Autorità. Tale iscrizione costituisce un precedente per la valutazione di eventuali future violazioni.

Pa: il Garante Privacy chiede più tutele per chi segnala gli illeciti

Parere favorevole alle linee guida Anac sul cosiddetto "whistleblowing", ma con alcune integrazioni

Adottare ulteriori misure per proteggere l'identità di chi segnala riservatamente

condotte illecite e quella dei presunti autori, delineare più precisamente i fatti che possono essere segnalati con il “whistleblowing” nella Pa, definire meglio il ruolo dei soggetti coinvolti.

Queste sono alcune delle condizioni e osservazioni indicate dal Garante per la privacy nel parere sulla bozza di “Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell’art. 54-bis del d.lgs. 165/2001, (c.d. whistleblowing)”, predisposta dall’Anac.

Le Linee guida - rivolte ai datori di lavoro in ambito pubblico, ma contenenti anche indicazioni per l’inoltro di segnalazioni da parte di dipendenti di imprese fornitrici di beni o servizi per la Pa - specificano le misure tecniche di base che le pubbliche amministrazioni, titolari del trattamento dei dati, dovranno adottare ed eventualmente ampliare, tenendo conto degli specifici rischi del trattamento e nel rispetto dei principi di privacy-by-design e privacy-by-default.

Il testo delle linee guida era stato inizialmente posto dall’Autorità anticorruzione in consultazione pubblica e poi integrato sulla base di una positiva collaborazione con il Garante per la privacy, così da rafforzare la tutela della speciale riservatezza dell’identità del segnalante e delle informazioni che facilitano l’individuazione di fenomeni corruttivi nella Pa.Tale collaborazione aveva portato anche a delineare meglio, ad esempio, il ruolo dei fornitori di applicativi e servizi informatici utilizzati per l’acquisizione e la gestione delle segnalazioni, nonché a proporre accorgimenti specifici per evitare la tracciabilità del segnalante.

Il parere favorevole del Garante privacy è però condizionato - anche alla luce degli esiti di attività ispettive avviate nel corso del 2019 proprio nei confronti dei principali soggetti (società informatiche, pubbliche amministrazioni) che trattano dati nell’ambito del whistleblowing - all’introduzione di specifiche modifiche che possano evitare di compromettere la corretta gestione delle segnalazioni.

Al fine di incrementare l’utilizzo e la fiducia in questo strumento, il Garante ha chiesto, ad esempio, che nelle Linee guida vengano circoscritte e definite meglio le condotte segnalabili con il “whistleblowing”, così da evitare che gli uffici che gestiscono le segnalazioni rischino di trattare illecitamente i dati delle persone citate, magari perché riferibili a casi non previsti dalla normativa anticorruzione. Dovranno poi essere specificati meglio - seppure con alcune limitazioni a tutela dell’identità del segnalante - i diritti garantiti dalla normativa privacy anche all’autore del presunto illecito.

Dovrà inoltre essere limitata al “responsabile della prevenzione della corruzione e della trasparenza” la possibilità di associare la segnalazione all’identità del segnalante. Nel parere è indicato, tra l’altro, che occorre specificare meglio il ruolo svolto nel trattamento dei dati dai soggetti (sia interni all’amministrazione, sia esterni come l’Autorità giudiziaria e la Corte dei Conti) che possono conoscere le informazioni contenute nelle segnalazioni riservate.

Il Garante ha infine chiesto all’Anac di rafforzare nelle Linee guida le misure tecniche e organizzative necessarie per tutelare l’identità del segnalante, utilizzando, ad esempio, protocolli sicuri per la trasmissione dei dati, abilitando accessi selettivi ai dati contenuti nelle segnalazioni, ed evitando che la piattaforma invii al segnalante notifiche sullo stato della pratica, in quanto tali messaggi potrebbero consentire di svelarne l’identità.

Gdpr: conclusi i seminari del progetto Smedata

Oltre 1.400 tra imprenditori e professionisti hanno partecipato agli incontri organizzati dal Garante in collaborazione con l’Università di Roma Tre

Si è concluso il ciclo di incontri formativi previsti dal progetto Smedata. Obiettivo dell’iniziativa quello di supportare le piccole e medie imprese (Pmi) e i professionisti impegnati negli adempimenti normativi in materia di protezione dei dati personali e di offrire chiarimenti ai soggetti che operano nella consulenza giuridica sul Regolamento.

Grazie alla collaborazionecon il Dipartimento di Giurisprudenza dell’Università degli Studi RomaTre - partner del Garante per lo sviluppo in Italia di Smedata - tra settembre e novembre sono stati organizzati 12 corsi di formazione tenuti da dirigenti e funzionari dell’Autorità, professori universitari ed esperti giuridici, per un totale di oltre 70 ore di lezione.

Gli eventi formativi hanno fatto tappa in 6 città (Milano, Genova, Firenze, Roma, Salerno, e Cosenza) e hanno coinvolto complessivamente oltre 1.400 partecipanti, tra imprenditori delle Pmi e professionisti.

Il percorso di Smedata continuerà nei prossimi mesi con ulteriori iniziative: un programma di formazione dei formatori, convegni internazionali e lo sviluppo di uno strumento di auto-valutazione per le Pmi. Tutte le informazioni sono disponibili sul sito del Garante, alla pagina https://www.garanteprivacy.it/regolamentoue/formazione/smedata.

Smedata, co-finanziato da fondi della Commissione europea e nato da una partnership tra le Autorità per la protezione dei dati Italiana e Bulgara, integra l'offerta di formazione già realizzata dal Garante con il progetto T4Data dedicato ai Responsabili della Protezione Dati (Rpd) dei soggetti pubblici.

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

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

- Privacy: controllo più efficace sui grandi sistemi informativi Ue - Comunicato del 9 dicembre 2019

- GDPR: bilancio positivo per il progetto formativo internazionale T4Data - Comunicato del 2 dicembre 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*