Luglio 2024

LA TUTELA DEI DATI PERSONALI IN AZIENDA

Si esaminano le novità sul tema introdotte di recente da varie normative in materia

Informativa n.	26/2024
Riferimenti normativi	Decreto Legislativo n. 24/2023 (“Decreto Whistleblowing”)
	Legge n. 90/2024 (“Legge Cybersecurity”)
	Provvedimento Garante Privacy del 7.12.2023 (“Linee Guida Conservazione delle Password”)
	Provvedimento Garante Privacy del 6.6.2024 (“Documento di indirizzo per il trattamento dei metadati”)

UNISTUDIO LEGAL & TAX
VIA DURINI 26
20122 MILANO
T. +39.02.83418800
VIA DOMINUTTI 20
37135 VERONA
T. +39.045.8013399
VIA DEI TRE OROLOGI 14
00197 ROMA
T. +39.06.73100755
info@unistudio.it
www.unistudio.it
C.F. e P.IVA 02901730230

Recentemente sono entrate in vigore numerose norme che hanno arricchito il panorama della tutela dei dati personali in azienda, quali il Decreto Whistleblowing e la Legge sulla Cybersicurezza, nonché le indicazioni del Garante Privacy quali le Linee Guida sulla conservazione delle password e il Documento di Indirizzo sulla conservazione dei metadati delle e-mail dei dipendenti.

Si analizzano di seguito alcuni aspetti e obblighi introdotti dalle varie disposizioni sopra citate.

Whistleblowing
La normativa in vigore richiede alle aziende con almeno 50 dipendenti:

a) l'adozione di un canale di segnalazione interno per consentire la segnalazione di violazioni del dritto dell'UE e delle normative nazionali;
b) di garantire l'accesso al canale di segnalazione non solo ai dipendenti ma anche ai soggetti esterni, quali clienti, fornitori, ex dipendenti e collaboratori;
c) l'adozione di misure tecniche specifiche per garantire la protezione dei segnalanti e la riservatezza delle segnalazioni.

Cybersicurezza
La normativa in vigore richiede:

a) l'attivazione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio, inclusa la protezione dei dati personali e delle informazioni aziendali sensibili;
b) la formazione specifica del personale mediante programmi periodici e aggiornati in base alle nuove minacce tecnologiche;
c) lo svolgimento di valutazione del rischio, documentate e riesaminate periodicamente per identificare e mitigare la vulnerabilità delle infrastrutture IT;
d) l'adozione di politiche e procedure che assicurino il rispetto delle disposizioni legislative e la capacità di dimostrarne la conformità in caso di audit e ispezioni.

Conservazione password
Per le imprese che, in qualità di titolari o responsabili del trattamento, conservano sui propri sistemi le password di propri utenti) la normativa in vigore richiede:

a) l'adozione delle misure tecniche raccomandate nelle linee guida in materia di funzioni crittografiche per la conservazione delle password o misure che garantiscono un analogo livello di sicurezza;
b) la cancellazione tempestiva delle password in caso di cessazione o dismissione dei sistemi informatici o servizi online le cui credenziali di autenticazione consentivano l'accesso o in caso di disattivazione o revoca delle credenziali di autenticazione.

Conservazione metadati delle e-mail dei dipendenti
E' necessario provvedere alla:

a) verifica delle impostazioni di base dei programmi e servizi di gestione della posta elettronica in uso ai dipendenti per impedire la raccolta automatica e senza limiti di tempo dei metadati;
b) conservazione dei metadati per un periodo massimo di 21 giorni;
c) attivazione delle procedure di garanzia previste dallo Statuto dei Lavoratori in caso di necessità a trattare i metadati per un periodo superiore ai 21 giorni;
d) predisposizione di un'informativa specifica agli interessati circa il trattamento dei metadati.

Il mancato rispetto delle disposizioni suddette espone le aziende al rischio di sanzioni alquanto severe che, in caso di violazione delle norme in materia di protezione dei dati personali, possono arrivare fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato annuo. Per l'inosservanza degli obblighi previsti dal Decreto Whistleblowing, e, in particolare, la mancata attivazione del canale di segnalazione interna, sono previste anche sanzioni amministrative pecuniarie fino ad un massimo di 50.000,00 euro applicabili direttamente dall'ANAC.

Unistudio è a disposizione per offrire **un check up privacy gratuito**, ossia un esame approfondito dello stato della tutela dei dati personali in azienda e una valutazione sugli eventuali adempimenti anche alla luce dei nuovi

provvedimenti, che Vi permette di ricevere un report completo con indicazione delle eventuali criticità e le attività da svolgere per la conformità al Regolamento Europeo 679/2016 ("GDPR") e alla normativa privacy.
Qualora interessati, potete scrivere una mail a privacy@unistudio.it "