Italia Oggi Sette

Lavoro

Prontuario privacy per il lavoro

Dal fascicolo del personale alla rilevazione delle presenze: le misure per la tutela dei dati in base ai provvedimenti del Garante


ItaliaOggi Sette

Prontuario privacy per il lavoro

Dal fascicolo del personale alla rilevazione delle presenze: le misure per la tutela dei dati in base ai provvedimenti del Garante

Il lavoro è stabile sul podio degli argomenti trattati nei provvedimenti del Garante della privacy. Sul totale (11802) dei provvedimenti pubblicati sul sito istituzionale www.garanteprivacy.it l'argomento lavoro conta 749 documenti. È preceduto di poche lunghezze dal marketing (786 documenti) e da pubblica amministrazione, che primeggia con 1219 documenti.

Le categorie interne all'argomento lavoro, che sono toccate dai provvedimenti, sono tantissime. Il maggior numero dei provvedimenti riguarda in generale il lavoro dipendente (trattato in 172 documenti). Il lavoro pubblico (trattato in 162 documenti) e il lavoro privato (in 137 documenti). Tra gli altri temi si segnalano: il fascicolo del personale (in 57 documenti), le sanzioni disciplinari (in 48 documenti) e le valutazioni dei lavoratori (in 40 documenti), il licenziamento (in 33 documenti). La previdenza (in 32 documenti), la rilevazione degli orari di lavoro (in 27 documenti), il monitoraggio degli accessi ai dispositivi aziendali (in 15 documenti) e la sicurezza lavoro (in 15 documenti).

Restringendo il campo di ricerca alle sole ordinanze-ingiunzioni (provvedimenti che applicano sanzioni), il lavoro è l'argomento che si colloca al quarto posto con 171 provvedimenti.

Il dato quantitativo testimonia due cose: la difficoltà di applicare la privacy nell'ambito dei rapporti di lavoro; la conflittualità che deriva da questa difficoltà.

Le difficoltà e conflittualità nell'ambito della applicazione della privacy nei rapporti di lavoro emergono anche dalla quantità di pagine dedicate a questo settore nelle relazioni annuali del Garante della privacy, che affrontano temi caldi quali i trattamenti di dati mediante dispositivi tecnologici, videosorveglianza e biometria, l'esercizio dei diritti dei lavoratori, il rapporto della disciplina della privacy con le leggi a tutela dei lavoratori (prima tra tutte la legge 300/1970, ancora attuale dopo oltre 54 anni) e così via.

D'altra parte, i problemi hanno anche una certa ripetitività. Si prenda l'esempio emblematico della posta elettronica, per certi versi già superata da diversi canali di comunicazione. Anzi, proprio per questo, si potrebbe dire che tutti i problemi dovrebbero essere risolti. E, invece, così non è. E così il garante, quasi come un ritornello, spiega e rispiega che la legittima necessità di assicurare la conservazione di documentazione necessaria per l'ordinario svolgimento e la continuità dell'attività aziendale, anche in relazione ai rapporti intrattenuti con soggetti privati e pubblici, nonché in base a specifiche disposizioni dell'ordinamento, è assicurata, in primo luogo, non dalla posta elettronica, ma dalla predisposizione di sistemi di gestione documentale con i quali attraverso l'adozione di appropriate

misure organizzative e tecnologiche individuare i documenti che nel corso dello svolgimento dell'attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile. I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche. Se si comprassero e si usassero a tappeto questi sistemi di gestione documentale, diminuirebbero i problemi dell'accesso alle e-mail del dipendente licenziato o pensionato, alla conservazione delle stesse per esigenze dell'impresa e così via. Se, però, non lo si fa, a parte chi dolosamente o colposamente non intende mettersi in regola, è perché, soprattutto per le realtà economiche medie e piccole, l'adeguamento e la conformità alle regole della prote

zione dei dati hanno un costo. Eppure, giorno per giorno, gli operatori economici devono confrontarsi con la necessità di adeguarsi ag

li strumenti della tecnologia. E adeguarsi non è solo un problema di spesa, ma anche un problema di conoscenza selezionata: non sempre sono disponibili strumenti che, pescando nel mare magnum delle informazioni disponibili, selezionino quel che interessa a chi

si occupa di privacy e lavoro. Per raccogliere questa esigenza, ItaliaOggi 7 ha raccolto e schedato le esperienze più recenti e più significative del Garante italiano della privacy. Attenzione però: non si tratta sempre di esperienze che giungono a

risultati conformi ed univoci. La schedatura dei precedenti ha, pertanto, l'obiettivo di mettere in evidenza, nell'ambito di un cantiere sempre aperto, alcune regole di dettaglio, anche desunte a contr ario rispetto a quelle punite. Per ogni pronuncia catalogata si riporta in due parole la parte essenziale del provvedimento dell'autorità che lo ha adottato, seguita dalla storia e cioè una breve descrizione dei fatti effettivamente capitati, per finire con la citazione

di cosa ha deciso il Garante. Il numero nella colonna di sinistra della seguente tabella corrisponde al numero del paragrafo in cui è riportata ciascuna vicenda. Se non espressamente segnalato, i provvedimenti citati sono del Garante per la protezione dei dati personali italiano e

le disposizioni sono tratte dal regolamento Ue n. 2016/679 (Gdpr). CONSERVAZIONE DEI DATI 1.I DATI DEL LAVORATORE PER FINALITÀ AMMINISTRATIVE E CONTABILI SI CONSERVANO 10 ANNI (Ingiunzione n. 305 del 15 settembre 2022) In due parole Si conservano per 10 anni dalla conclusione del rapporto di lavoro i dati raccolti per finalità di gestione amministra

tiva, contabile, operativa e organizzativa del rapporto di lavoro. La storia L'ex dipendente di una banca ha chiesto al suo ex datore di lavoro la cancellazione dei dati detenuti dalla stessa. La banca ha riferito di conservare per 10 anni dalla conclusione del rapporto di lavoro, con la finalità di gestione amministrativa, contabile, operativa e organizzativa del rapporto di lavoro, i seguenti dati: dati anagrafici e identificativi, dati di contatto (indirizzo, numero di telefono, e-mail), immagini fotografiche presenti su copia di documento d'identità del dipendente, informazioni relative a competenze professionali e

al percorso di carriera (studi, auto-rilevazione delle competenze, corsi di formazione), informazioni relative ai rapporti di lavoro intercorsi con la banca (matricola, tipologia di rapporto, causale di assunzione, causale di cessazione, stato lavorativo, livello retributivo, tipo di contratto, incarichi e ruoli organizzativi ricoperti, sedi di lavoro). La banca ha aggiunto di conservare per 10 anni dalla generazione del documento inerente al pagamento, eccetto i dati trasposti nel libro unico del lavoro, conservati per i tempi di legge applicabili, con la finalità di gestione degli adempimenti connessi al pagamento degli stipendi i seguenti dati: dati anagrafici

e identificativi, dati di contatto e dati relativi alle presenze. La banca ha, infine, dichiarato di applicare una regola di conservazione dei dati rilevanti in linea col termine ordinario civilistico di prescrizione dei diritti, nonché coi termini per accertamenti di natura pubblicistica (per esempio fiscali, penali, ecc.) con prolungamento del termine in caso di contenzioso e/o procedimento amministrativo/giudiziario per esercitare il propr

io diritto di difesa e/o conformarsi alle richieste dell'autorità. In rel

azione alle descritte finalità la banca non ha dato corso alla richiesta di cancellazione. Il Garante ha deciso che a)con riferimento alla mancata cancellazione dei dati attinenti a precedenti rapporti di lavoro intercorrenti tra il dipendente e la banca/datrice di lavoro e a rapporti bancari nei termini e per le finalità indicati, si condivide quan

to rappresentato dalla società circa la liceità dell'ulteriore conservazione degli stessi. DIRITTO DI ACCESSO DEL LAVORATORE 2. I LAVORATORI HANNO DIRITTO ALLA COPIA DI TUTTI I DATI (Ingiunzione n. 403 del 14 settembre 2023) In due parole Il datore di lavoro deve fornire i

dati riferibili ai lavoratori, tra cui le singole localizzazioni degli stessi tramite gps. La storia Alcuni lavoratori (letturisti di contatori di utenze domestiche presso il domicilio degli utenti) hanno rivolto un'istanza di accesso ai dati relativi ai trattamenti effettuati dal datore di lavoro al fine di calcolare i tempi della prestazione lavorativa e i rimborsi chilometrici, in particolare relativamente ai t

rattamenti effettuati attraverso un terminalino fornito dal datore di lavoro (smartphone). Quest'ultimo non ha comunicato gli specifici dati trattati, tra l'altro, attraverso la geolocalizzazione sul terminale fornito nell'ambito della prestazione lavorativa né tutte le informazioni richieste dai lavoratori in proposito al trattamento dei predetti dati; si è limitato, infatti, ad in

dicare le modalità e le finalità del trattamento dei dati relativi alla geolocalizzazione. Il Garante ha deciso che a)il datore di lavoro ha commesso una violazione del Gdpr; b)il datore di lavoro, nei limiti dei dati conservati, deve fornire ai lavoratori dati relativi alle specifiche rilevazioni/coordinate geografiche effettuate con il gps dello s

martphone attivato dai lavoratori in prossimità del contatore per la lettura del medesimo. 3. ALLE RICHIESTE DI ACCESSO NON SI RISPONDE ORALMENTE PER TELEFONO (Ingiunzione n. 475 del 12 ottobre 2023) In due parole

Il datore di lavoro non può rispondere oralmente alle richiest

e di accesso se il lavoratore non ha chiesto espressamente tale modalità di comunicazione. La storia Un lavoratore chiede, a mezzo posta elettronica, al suo datore di lavoro gli attestati di formazione effe

ttuati durante il rapporto di lavoro. Il datore risponde negativamente con una telefonata. Il Garante ha deciso che a) viola il Gdpr il diniego dell'esercizio di un diritto fornito tramite una forma (oralmente) non espressamente richiesta dall'interessato; b) solo se richiesto dall'interessato, le informazioni possono essere fo

rnite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato stesso. 4. NON BASTA UN COLLOQUIO PER RISPONDERE ALLE ISTANZE DI ACCESSO DEI LAVORATORI (Ingiunzione n. 303 del 15 settembre 2022) In due parole Alle richieste di accesso

del lavoratore bisogna rispondere per iscritto e non solo a mezzo di colloqui individuali. La storia Un lavoratore ha chiesto l'accesso ai propri dati detenuti nel fascicolo personale, nelle note di qualifica, nelle annotazioni e/o valutazioni sulla attività svolta, negli atti relativi al percorso professionale e all'attività svolta in esecuzione del rapporto di lavoro e l'elenco, dalla data di assunzione sino alla data di presentazione della domanda, della mansione giornaliera assegnata sulla linea di lavoro, con specificazione della linea di lavoro. Il datore di lavoro non ha inviato una risposta scritta, ma ha dichiarato che per prassi aziendale il lavoratore era solito avere colloqui con l'ufficio Risorse Umane e tutte le richieste di incontro sono sempre state celermente gestite con apposite riunioni. A riguardo della richiesta non evasa, a causa di eventi di natura organizzativa legati alla sospensione delle attività dello stabilimento per ricorso alla cassa integ

razione collegata anche all'emergenza Covid, il colloquio in presenza non si è realizzato. Il Garante ha deciso che a)solo se richiesto dall'interessato le informazioni possono essere fornite oralmente; b)in assenza di richiesta dell'inter

essato, la risposta orale, anche se osservata per prassi, non è legittima e viola il Gdpr. 5. AI DIPENDENTI NON SI CONSEGNA BREVI MANU LA COPIA DEI DATI RELATIVI ALLA RILEVAZIONE DELLE PRESENZE (Ingiunzione n. 66 del 9 marzo 2023) In due parole I dati richiesti dai lavoratori non devono essere consegnati d

irettamente brevi manu, salvo richiesta espressa di tale modalità da parte dei lavoratori. La storia Alcuni dipendenti di una società hanno chiesto di accedere ai dati riferiti relativi alla rilevazione della loro presenza sul posto di lavoro effettuata tramite badge. In assenza di risposta hanno presentato un reclamo al Garante. Il datore di lavo

ro ha sostenuto di avere consegnato le informazioni brevi manu diretta

mente ai dipendenti. Questa circostanza non è stata dimostrata nel corso del procedimento. Il Garante ha deciso che a)la società ha omesso di fornire riscontro alle istanze di accesso ai dati relativi alle presenze rilevate con il badge; b)viola il Gdpr il mancato riscontro alla richiesta di accedere ai dati

personali riferiti alla rilevazione della presenza in servizio (inizio e fine dell'attività lavorativa), effettuata mediante dispositivo badge; c)il riscontro mediante consegna brevi manu dei dati, anche se effettivamente avvenuto, non è conforme a quanto stabilito con l'articolo 12 del Gdpr (la risposta orale è ammessa solo se espressamente richiesta dall'interessato); d)il riscontro mediante consegna brevi manu dei dati viola anche l'articolo 15, par. 3, del Gdpr, ai sensi del quale se

l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune. 6. AMMISSIBILI LE RIPETUTE ISTANZE DI ACCESSO DEI LAVORATORI (Ingiunzi

one n. 303 del 15 settembre 2022) In due parole Sono ammissibili le richieste di accesso del lavoratore anche se hanno ad oggetto informazioni di cui lo stesso sia già in possesso. La storia Un lavoratore ha chiesto l'accesso ai propri dati detenuti nel fascicolo personale, nelle note di qualifica, nelle annotazioni e/o valutazioni sulla attività svolta, negli atti relativi al percorso professionale e all'attività svolta in esecuzione del rapporto di lavoro e l'elenco, dalla data di assunzione sino alla data di presentazione della domanda, della mansione giornaliera assegnata sulla linea di lavoro, con specificazione della linea di lavoro. Il datore di lavoro ha eccepito che

le informazioni di cui il dipendente ha chiesto l'accesso consistevano prevalentemente in dati già nella sua disponibilità, in quanto attingibili attraverso piattaforme aziendali. Il Garante ha deciso che a)l'istanza di accesso può riguardare dati personali già in possesso dell'interessato per consentirgli di verificare, anche a intervalli ragionevoli di tempo se sia in corso un determinato trattamento e valutarne la liceità e la correttezza; b)la circostanza che in precedenti occasioni siano già state fornite al dipendente le in

formazioni relative ai trattamenti effettuati non può giustificare la mancata risposta a una richiesta di esercizio dei diritti peraltro presentata formalmente al datore di lavoro. 7. IL LAVORATORE PUÒ PRESENTARE RICHIESTE DI ACCESSO ANCHE USANDO CANALI DIVERSI DA QUELLI INDICATI NELLE PROCEDURE AZIENDALI (Ingiunzione n. 529 del 16 novembre 2023) In due parole Il lavoratore può chiedere l'accesso con

una comunicazione elettronica inviata alla PEC del datore di lavoro anziché al diverso indirizzo elettronico appositamente destinato a queste esigenze dal datore di lavoro stesso. La storia Numerosi dipendenti, con una mail inviata dal loro avvocato di fiducia all'indirizzo di posta elettronica certificata aziendale, hanno chiesto al datore di lavoro di aver accesso ai propri fascicoli personali, alle buste paga e a una serie di informazioni relative al trattamento dei dati per il calcolo delle buste paga stesse, senza, però, ottenere alcuna risposta; hanno, quindi, presentato un rec

lamo al Garante. Il datore di lavoro ha contestato la regolarità della richiesta pervenuta a un indirizzo e-mail diverso da quello indicato dall'azienda per questi tipi di istanze. Il Garante ha deciso che a)le istanze di accesso sono state regolarmente presentate; b)le istanze di esercizio dei diritti sono state presentate all'indirizzo di posta certificata del datore di lavoro e non a un indirizzo qualunque;

c)il Gdpr non impone agli interessati alcun requisito riguardo al formato della richiesta di accesso ai dati personali. 8. LA RICHIESTA DI ACCESSO DEL LAVORATORE NON DEVE NECESSARIAMENTE ELENCARE TUTTI I SINGOLI DOCUMENTI RICHIESTI (Ingiunzione n.

n. 290 del 6 luglio 2023) In due parole Il datore di lavoro non può respingere un'istanza di accesso del lavoratore perché non contiene l'elenco specifico dei documenti richiesti. La storia Un lavoratore ha chiesto al suo datore di lavoro l'accesso a tutti i dati utilizzati dallo stesso per

effettuare una contestazione disciplinare ai suoi danni. Il datore di lavoro ha respinto la richiesta ritenendola generica e pretendendo l'elenco specifico dei documenti richiesti. Il Garante ha deciso che a)non è conforme all'articolo 15 del Gdpr subordinare il riscontro all'istanza di accesso alla indicazione dettagliata da parte dell'interessato dei documenti cui si chiede di accedere; b)il diritto di accesso privacy ricomprende anche le categorie di dati personali nonché, qualora i dati non siano raccolti presso l'intere

ssato, tutte le informazioni disponibili sulla loro origine: c)il datore di lavoro deve accogliere le richieste di accesso e fornire tutti i dati raccolti sul conto del lavoratore. 9. INDICARE AL LAVORATORE LA PIATTAFORMA DOVE TROVARE I DATI (Ingiunzione n. 529 del 16 novembre 2023) In due parole Se il lavoratore chiede dati, che

può apprendere collegandosi in autonomia alla piattaforma aziendale, il datore di lavoro non può omettere la risposta, ma deve ricordargli le modalità di accesso alla piattaforma. La storia Numerosi dipendenti hanno chiesto al datore di lavoro di aver

accesso ai propri fascicoli personali, alle buste paga e a

una serie di informazioni relative al trattamento dei dati per il calcolo delle buste paga stesse, senza ottenere alcuna risposta e, quindi, hanno presentato un reclamo al Ga

rante. Il datore di lavoro si è difeso eccependo che i dipendenti avrebbero potuto conoscere i propri dati retributivi accedendo in autonomia alla piattaforma informatica dedicata. Il Garante ha deciso che a)il datore di lavoro deve sempre rispondere alle istanze dei dipendenti, precisando il motivo del diniego nonché la possibilità di presentare reclamo al Garante o ricorso all'autorità giudiziaria; b)Il d

atore di lavoro, se i dati richiesti sono già nella disponibilità dei lavoratori, deve indicare loro la piattaforma informatica attraverso cui accedere alle informazioni richieste. 10. AL LAVORATORE SPIEGARE SEMPRE IL NO ALL'ACCESSO PER RAGIONI DIFENSIVE (Ingiunzione

n. 529 del 16 novembre 2023) In due parole Se il datore di lavoro, per non compromettere la difesa in giudizio, non intende consegnare dati al dipendente con cui è in lite, deve spiegarlo esplicitamente nel diniego di accesso ai dati rivolto dal lavoratore. La storia Numerosi dipendenti hanno chiesto al datore

di lavoro di aver accesso ai propri fascicoli personali, alle buste paga e a

una serie di informazioni relative al trattamento dei dati per il calcolo delle buste paga stesse, senza ottenere alcuna risposta e, quindi, hanno presentato un reclamo al Garante. Alla richiesta di spiegazioni del Garante, il datore di lavoro ha risposto

di non aver dato riscontro alle istanze per non compromettere il proprio diritto di difesa in giudizio. Tra la società e i lavoratori, infatti, erano in corso diversi procedimenti giudiziari riguardanti l'accantonamento e le modalità di calcolo della liquidazione. Il Garante ha deciso che a)il datore di lavoro, qualora sussistano fondate ragioni per non consentire l'esercizio del diritto, deve comunque tempestivamente informare l'interessato dei motivi del diniego oltre che della possibilità di presentare reclamo al Garante o ricorso all'autorità giudiziaria; b)il datore di lavoro può non rispondere solo qualora la stessa possa compromettere la finalità della limitazione. Circostanza, quest'ultima, difficile da dimostrare; c)il datore di lavoro non può sostenere, a fondamento della sua mancata risposta, la possibilità che comunicazione del diniego sia prodotta come mezzo di prova da parte dei lavoratori nel corso dei giudizi pendenti, al fine di ingenerare nel giudice la convinzione che il datore di lavoro, abusando della propria posizione di forza, intenda compromettere il diritto di produzione degli atti, con il concreto rischio di accoglimento della la richiesta di acquisizione dei dati in giudizio; d)non fornire la comunicazione di diniego nella prospettiva che gli interessati pos

sano utilizzare il riscontro per esercitare il diritto di difesa nelle forme previste dall'ordinamento non può essere idonea condizione per fare valere l'ipotesi della ricorrenza di una sorta di esenzione dalla comunicazione del diniego dell'esercizio dei diritti. 11. IL LAVORATORE HA DIRITTO ALLA COPIA DELLA RELAZIONE INVEST

IGATIVA (Ingiunzione n. 290 del 6 luglio 2023) In due parole Il lavoratore ha diritto ad avere accesso ai propri dati personali, compresi quelli contenuti nella relazione dell'agenzia investigativa incaricata dall'azienda di raccogliere informazioni sul suo conto. La storia Un dipendente non riusciv

a ad ottenere un completo riscontro alle richieste di accesso ai propri dati personali, avanzate dopo il ricevimento di una contestazione disciplinare, nella quale erano contenuti puntuali riferimenti ad attività extra lavorative, cui era seguito il licenziamento. A distanza di quasi un anno dalla prima richiesta e in occasione de

l processo iniziato a seguito della di impugnazione del licenziamento, il dipendente è venuto a conoscenza dell'esistenza e del contenuto della relazione investigativa, dalla quale erano stati tratti riferimenti specifici inseriti nella contestazione disciplinare. Il Garante ha deciso che a)l'azienda, nei riscontri forniti al lavoratore, non avendo fatto cenno alla relazione investigativa, ha violato il principio di correttezza; b)il lavoratore ha diritto ad avere accesso ai propri dati personali, compresi quelli contenuti nella relazione dell'agenzia investigativa incaricata dall'azienda di raccogliere informazioni sul suo conto; c)l'azienda ha l'obbligo di fornire al lavoratore tutti i dati raccolti con la relazione investigativa, anche quelli che non trasferiti nella contestazione disciplinare (fotografie, una rilevazione

Gps, descrizioni di luoghi, persone e situazioni). Informazioni che, in ipotesi, avrebbero anche potuto essere utili per l'esercizio del diritto di difesa 12. LECITO CHIEDERE AL DIPENDENTE LA CARTA D'IDENTITÀ PRIMA DI CANCELLARE I SUOI DATI (Ingiunzione n. 305 del 15 settembre 2022) In due parole È lecito verificare l'identità del dipendente, che chiede la cancellazione dei suoi dati, prima di procedere alla cancellazione, che deve avvenire entro un mese, prorogabile di due mesi per giustificate ragioni La storia L'ex dipendente di una banca ha chiesto al suo ex datore di lavoro la cancellazione dei dati detenuti dalla stessa. La banca ha risposto solo dopo alcuni mesi, cancellando alcuni dati e, in particolare, i dati dell'interessato dalle tabelle del database sottostante la sezione Lavora con noi del sito internet della banca e relativi identificativo user e password dell'account. Durante il procedimento di reclamo avanti al Garante, promosso dall'interessato, è emerso che la banca, per evadere la richiesta di cancellazione, abbia chiesto la scannerizzazione di carta di

identità e codice fiscale allegati alla richiesta di cancellazione e che, nonostante il giorno successivo l'interessato abbia inviato la documentazione richiesta (documento d'identità e codice fiscale), la stessa non ha poi fornito effettivo riscontro all'istanza. Il Garante ha deciso che a)è lecito verificare l'identità verificare l'identità dell'interessato richiedente l'esercizio del diritto alla cancellazione; b)viola il Gdpr, il datore di lavoro che, una volta soddisfatta la lecita esigenza di verificare l'identità del dipendente, non dia seguito nei temp

i previsti dal Gdpr all'istanza (un mese, prorogabile di due mesi per giustificate ragioni); c)quando si risponde a una richiesta di accesso non bisogna dimenticare di indicare la possibilità di proporre reclamo all'autorità di controllo o ricorso giurisdizionale. POSTA ELETTRONICA 13. L'INTERESSE A NON PERDERE CLIENTI NON GIUSTIFICA DI PER SÉ L'ACCESSO AI CONTENUTI DELLA POSTA ELETTRONICA DEL COLLABORATIORE (Ingiunzione n. 8 d

ell'11 gennaio 2023) In due parole Il legittimo interesse a trattare dati personali contenuti nelle e-mail del dipendente/collaboratore, per non perdere potenziali clienti, deve essere bilanciato con il diritto dei collaboratori alla protezione dei dati personali. La storia Una cooperativa e una srl si accordano per partecipare a una fiera, nella quale promuovere i prodotti della srl. Una dipendente della cooperativa viene incaricata di tenere lo stand alla fiera e le viene assegnato un indirizzo e-mail personalizzato con l'estensione della srl. La dipendente era in procinto di essere assunta dalla srl. L'iniziativa non ha avuto seguito e la signora in questione ha chiesto alla srl la disattivazione dell'account con il suo nome. La srl ha preso tempo e ha letto i contenuti dei messaggi ricevuti dalla signora e ciò al fine di ricontattare i soggetti, con i quali la signora aveva scambiato messaggi usando la e-mail della srl: questo per coltivare la possibilità che i soggetti dive

ntassero clienti della srl e non della cooperativa, con la quale la srl è entrata in contenzioso (appunto per sviamento della clientela). Ne è sorto un reclamo al Garante a riguardo della legittimità della lettura da parte della srl delle e-mail scritte e ricevute dalla signora all'indirizzo personalizzato

con dominio della srl. Il Garante ha deciso che: a)l'esigenza di mantenere i rapporti con i potenziali clienti non è elemento tale da configurare un idoneo criterio di legittimazione del trattamento consistente nella lettura dei contenuti delle comunicazioni di posta elettronica; b)l'interesse alla prosecuzione dell'attività economica aziendale può essere realizzato mediante attivazione di un sistema di risposta automatico con il quale vengono forniti

indirizzi alternativi ai quali contattare l'impresa; c)non è necessario che l'impresa prenda visione delle comunicazioni in entrata sull'account individualizzato assegnato al collaboratore; d)la finalità legittima di non perdere contatti utili per la propria attività commerciale si deve perseguire con trattamenti meno invasivi. 14

. INFORMATIVA PREVENTIVA NECESSARIA PER I CONTROLLI SU ACCOUNT E-MAIL E TELEFONINI (Ingiunzione n. 127 del 13 aprile 2023) In due parole Il datore di lavoro deve specificare in dettaglio e preventivamente i tipi di controlli che si riserva di effettuare sui dispositivi in uso ai lavoratori per la tutela del patrimonio aziendale. La storia Un dipendente si è lamentato della sostituzione delle credenziali di accesso all'account di posta elettronica di tipo individualizzato, assegnatogli nell'ambito di una pluralità di rapporti di colla

borazione coordinata e continuativa stipulati con un'impresa, e della disattivazione del telefono aziendale disposti, prima della concordata cessazione del rapporto di lavoro, con conseguente impossibilità, per lo stesso,

di accedere ai propri dati personali, anche di tipo privato e di natura particolare, contenuti nell'account. L'interessato ha rilevato di non avere avuto informazione preventiva di questo tipo di controlli e ha chiesto l'immediato sblocco della email aziendale e la fornitura di nuove credenziali di accesso per potervi accedere. L'impresa si è difesa sostenendo che il blocco è maturato a seguito del riscontro da parte dell'amministratore del sistema di una serie di inusuali accessi alla VPN aziendale, nell'ora che aveva preceduto l'invio al collaboratore della comunicazione PEC per l

a cessazione del rapporto, con uno scarico massivo, inusuale ed ingiustificato, di oltre 600 file dai server della società da un solo account

, risultato essere quello assegnato all'interessato. L'impresa ha, quindi, opposto l'esigenza di tutelare il proprio interesse, legittimo e prevalente, alla tutela del patrimonio aziendale. L'ex dipendente ha ribattuto che lo scarico dei dati è occorso in costanza di rapporto contrattuale e dunque è stato tutt'altro che abusivo. Nel corso del procedimento sono stati valutati i documenti sui controlli aziendali, dai quali non è emerso alcun rifer

imento alla possibilità di effettuare controlli preordinati alla verifica dell'osservanza delle regole sull'uso delle caselle di e-mail e in particolare controlli nella forma di raccolta di dati riferiti ad attività anomale, individuazione della singola postazione, esame dei dati contenuti nei dispositivi aziendali riconsegnati. Il Garante ha deciso che a)l'impresa ha omesso di informare l'interessato circa

la possibilità di effettuare indagini sui contenuti memorizzati sui dispositivi aziendali (notebook e smartphone), nonché di analizzare le attività svolte attraverso i dispositivi medesimi, individuando, pur all'esito di una ricognizione improntata a gradualità, il singolo utilizzatore di un'utenza cui sono ricollegate attività ritenute anomale; b)l'impresa ha violat

o il Gdpr avendo omesso di informare l'interessato circa la specifica modalità di trattamento in concreto effettuata mediante i controlli svolti sull'uso dei dispostivi informatici e l'analisi dei dati contenuti all'interno dei propri dispositivi oggetto di riconsegna (successivamente sottoposti ad attività di indagine forense). 15. TRASPARENZA SULLA POSSIBILITÀ DI LE

TTURA DELLE E-MAIL NON INDIVIDUALIZZATE (Ingiunzione n. 93 del 23 marzo 2023) In due parole Il datore di lavoro deve informare preventivamente dipendenti e collaboratori della possibilità concessa ai dirigenti dell'azienda di accedere alle e-mail aziendali non individualizzate (recanti ad esempio la denominazione di un ufficio). La storia Una società ha assegnato a un consulente esterno un account di posta elettronica individualizzato (con nome e cognome). Il consulente ha presentato un reclamo al Garante lamentandosi del fatto che la corrisponde

nza scambiata mediante il predetto account sarebbe stata quotidianamente controllata da una dirigente della soc

ietà, in assenza di alcuna informativa fornita ai dipendenti/colla

boratori della società in ordine alla visibilità da parte della direzione degli scambi di e-mail, avvenuti utilizzando anche account aziendali condivisi. In numerosi casi, la dirigente ha scritto espressioni di biasimo sull'operato del consulente esterno e di altri collaboratori, anche con l'uso di espressioni poco commendevoli. Il Garante ha deciso che a)viola il Gdpr il datore di lavoro che non informa gli assegnatari di account e-mail aziendali circa le modalità d'uso dell'account di posta elettronica individualizzato e alla gestione degli account non individualizzati, compresa la possibilità della visibilità degli indirizzi non individualizzat

i da parte di soggetti apicali; b)il datore di lavoro deve indicare ai propri dipendenti e collaboratori, in ogni caso, chiaramente e in modo adeguato, quali siano l

e modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli che devono comunque essere conformi ai principi di liceità, proporzionalità e gradualità. c)nell'ambito di un rapporto di lavoro di qualsiasi natura l'obbligo di informare il lavoratore è espressione del principio generale di correttezza dei trattamenti. 16. IL COORDINAMENTO DIREZIONALE NON IMPLICA LIBERT

À ASSOLUTA DI INTERVENTO IN TUTTE LE E-MAIL AZIENDALI (Ingiunzione n. 93 del 23 marzo 2023) In due parole La funzione di coordinamento assegnata alla direzione aziendale non comporta la possibilità di leggere e intervenire senza limiti nella corrispondenza elettronica interna, scrivendo contenuti di rimprovero a carico di dipendenti o consulenti, leggibili da tutti i partecipanti alle conversazioni. La storia

Italia Oggi Sette

Lavoro

Una società ha assegnato a un consulente esterno un account di posta elettronica individualizzato. Il consulente ha presentato

un reclamo al Garante, lamentandosi del fatto che una dirigente, abilit

ata alla conoscenza della corrispondenza scambiata con account non individualizzati, avendo accesso, quindi, alla corrispondenza intercorsa con l'account da lui utilizzato, abbia scritto espressioni di biasimo sull'operato del consulente esterno medesimo e di altri collaboratori, anche con l'uso di espressioni poco commendevoli. In dettaglio, attraverso la ricostruzione a r

itroso della catena dei messaggi inviati, la dirigente ha fornito indicazioni, chiesto chiar

imenti ed espresso commenti e valutazioni (spesso di biasimo) sull'operato di dipendenti e collaboratori, lasciando e/o mettendo in copia tutti gli interlocutori della comunicazione originaria (in alcuni casi inserendone altri), in modo tale che tutti i partecipanti alla conversazione ne apprendessero il contenuto. La società ha rivolto una nota di richiamo alla dirigente per il comportamento non consono. Il Garante ha deciso che a)indipendentemente dalla natura del rapporto, il datore di lavoro è tenuto a rispettare il principio di correttezza, proporzionalità e minimizzazione; b)non rispettano tali principi gli interventi sistematici sull'operato di singoli dipendenti e collaboratori, reso noto anche ad altri colleghi/collaboratori, utilizzando in alcuni casi espressioni lesive della dignità anche professionale dei destinatari e realizzando in tal modo

una interferenza nella sfera privata e professionale di collaboratori e dipendenti; c)il coordinamento dell'attività e, a maggior ragione, l'assunzione di decisioni che rientrino nella sfera di competenza della direzione aziendale e la relativa comunicazione ai destinatari può avvenire con modalità individu alizzate e che comunque non comportino la lesione della riservatezza di collaboratori e dipendenti. 17. NON SI DISATTIVA L'ACCOUNT DI POSTA ELETTRONICA AZIENDALE DEL LAVORATORE DURANTE IL PERIODO DI MALATTIA (Ingiunzione n. 145 del 9 luglio 2020) In due parole Non è corretto disattivare l'account di posta elettronica aziendale individualizzato durante il periodo di malattia del lavoratore, anche se lungo. La storia Un datore di lavoro, nel quadro di un rapporto difficile con un suo dipendente, ha disposto la disattivazione della casella di posta elettronica aziendale per il periodo di malattia dello stesso, dopo 22 giorni non consecutivi di assenza, senza svolgere alcun ulteriore trattamento dei dati del dipendente e ciò, a detta dell'azienda, come conseguenza della norma

le e sistematica applicazione delle politiche di sicurezza, pienamente conformi al disciplinare tecnico. Il Garante ha accertato che nei documenti aziendali non vi era alcun riferimento a tale procedura, né la società ha prodotto altri documenti contenenti elementi informativi resi noti ai dipendenti relativi ad una disciplina riguardante l'accesso alla posta elettronica aziendale in costanza di malattia. Il Garante ha

deciso che a)non è conforme al Gdpr la disattivazione dell'account di posta elettronica aziendale operata dal datore di lavoro durante il periodo di malattia del lavoratore interessato; b)Il Garante ha prescritto

al titolare di dare corso all'istanza di accesso ai dati contenuti nell'account di posta elettronica a suo tem

po presentata dall'interessato ed ha irrogato una sanzione amministrativa pecuniaria. 18. NON SI CAMBIA LA PASSWORD DELLA POSTA ELETTRONICA AZIENDALE DEL LAVORATORE DURANTE IL PERIODO DI MALATTIA (Ingiunzione n. 91 del 19 maggio 2020) In due parole Senza informativa preventiva, il

datore di lavoro non può cambiare la password della posta elettronica aziendale del lavoratore durante il periodo di malattia. La storia Un lavoratore ha contestato la modifica, avvenuta i

n pendenza della sua assenza per malattia, senza informativa preventiva, da parte del datore di lavoro dell

a password di accesso all'account di posta elettronica di tipo individualizzato assegnato al lavoratore medesimo. Il datore di lavoro ha eccepito che, per policy aziendale, era inibito l'utilizzo della mai l aziendale per scopi e fini personali al di fuori dei locali aziendali e degli orari di lavoro. Il datore di lavoro ha comunicato al dipendente la password di accesso nel momento del ritorno in azienda. Il Garante ha deciso che a)viola la privacy, per carenza di informativa, il datore di lavoro che procede al cambio di password di accesso all'account di posta el

ettronica individuale in uso al lavoratore. 19. DA DISATTIVARE L'E-MAIL AZIENDALE DEL COLLABORATORE (ANCHE NON DIPENDENTE) CESSATO (Ingiunzione n. 263 del 22 giugno 2023) In due parole Non si possono mantenere attivi gli account di posta elettronica di tipo individualizzato, assegnati ai due collaboratori, per un periodo di tempo pari a 120 giorni successivo alla cessazione del rapporto di collaborazione. La storia A seguito dell'interruzione del rapporto di lavoro con due collaboratori, un'agenzia di assicurazione ha predisposto il blocco delle loro caselle di posta elettronica aziendale, la quale non poteva, perciò, più essere visionata né utilizzata da alcuno dei dipendenti della società, salvo solo il re

sponsabile informatico della stessa ed il responsabile della riassegnazione dei clienti gestiti dai collaboratori cessati. La disattivazione definitiva degli account veniva successivamente disposta entro il termine di 120 giorni dall'interruzione del rapporto di collaborazione, in base a una consolidata prassi azi

endale. Tale periodo di tempo è stato ritenuto necessario per consentire all'agenzia di riassegnare e ridistribuire il portafoglio polizze e clienti dei lavoratori cessati ad altri collaboratori. La riassegnazione dei clienti, ha spiegato l'agenza, non è un'attività automatica ed immediata, giacché l'agente generale deve effettuare diverse stime e valutazioni, sia del portafoglio suddetto, che del carico, delle capacità e disponibilità degli altri collaboratori, per determinare le modalità di smistamento. Il Garante ha deciso che a)l'attività di reindirizzamento automatico dei messaggi in transito sugli account dei collaboratori cessati verso un altro account aziendale, protratta per un periodo di tempo pari a 120 giorni, ha comportato la conoscibilità del contenuto dei messaggi da parte di terzi non autorizzati e si è protratta per un periodo temporale eccessivo e non commisurato alle effettive esigenze organizzative; b)il datore di

lavoro, dopo la cessazione del rapporto di lavoro o di collaborazione, deve provvedere alla rimozione dell'account di posta elettronica aziendale di tipo individualizzato, previa disattivazione della stessa e contestuale adozione di sistemi automatici volti a informarne i

terzi e a fornire a questi ultimi indirizzi alternativi, evitando in tal modo di prendere visione delle comunicazioni in entrata sull'account individualizzato assegnato all'interessato; c)tali obblighi risultano pienamente applicabili anche con riferimento a relazioni professionali

e di collaborazione che, pur non essendo caratterizzati da una relazione di dipendenza, attribuiscono comunque al titolare del trattamento un ampio potere organizzativo, sia interno che esterno, come risulta nel caso di specie. 20. LE E-MAIL N

ON SI CONSERVANO PER SEMPRE (Ingiunzione n. 263 del 22 giugno 2023) In due parole Le esigenze di conservazione dei documenti aziendali non possono essere perseguite con la conservazione senza limiti delle e-mail transitate sugli account di dipendenti e collaboratori. La storia Un'impresa conserva, senza limiti di tempo definiti, il contenuto della corrispondenza transitata sugli account di posta elettronica individualizzata attribuiti ai dipendenti e ciò per finalità di continuità dell'attività aziendale. Il Garante ha deciso che a)è illegittima la conservazione, senza limiti di tempo, del contenuto della corrispondenza che transita sugli account di posta elettronica, assegnati ai propri collaboratori, successivamente alla cessazione del rapporto di collaborazione; b)la legittima necessità di assicurare la conservazione di documentazione necessaria per l´ordinario svolgimento e la continuità dell´attività aziendale, anche in relazione ai rapporti intrattenuti con soggetti privati e pubblici, nonché in base a specifiche disposizioni dell´ordinamento, è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale con i quali attraverso l´adozione di appropriate misure organizzative e tecnologiche individuare i documenti che nel corso dello svolgimento dell´attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile. I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche; c)lo scopo di predisporre strumenti per l'ordinaria ed efficiente gestione dei flussi documentali aziendali, pertanto, può ben essere perseguito con strumenti meno invasivi per il diritto alla riservatezza degli interessati, rispetto alla sopra descritta attività di accesso al contenuto delle comunicazioni pervenute sugli account assegnati ai collab

oratori, che risulta pertanto non necessaria né proporzionata rispetto allo scopo; d)la conservazione senza limiti di tempo del contenuto della corrispondenza transitata sugli account di posta elettronica individualizzata dei dipendenti e collaboratori, nonché la loro reperibilità per mere finalità di continuità dell'attività aziendale risulta illecita, in quanto posta in

essere in assenza di un presupposto di liceità e contraria ai principi di minimizzazione e di limitazione della conservazione dei dati. 21. POSTA ELETTRONICA: IL COLLABORATORE ESTERNO HA GLI STESSI DIRITTI

DEL DIPENDENTE (Ingiunzione n. 127 del 7 aprile 2022) In due parole Gli obblighi informativi e di corretta e trasparente gestione della casella di posta aziendale a carico delle imprese devono essere rispettati anche a favore di soggetti che, come gli agenti, non sono qualificati lavoratori subordinati. La storia A una collaboratrice esterna di una società è stata assegnata una casella di e-mail individualizzata. A un certo punto, la società senza alcun preavviso né comunicazione successiva, aveva inibito alla collaboratrice l'accesso al suo

account, utilizzato per le relazioni commerciali, account che risultava però ancora attivo. La collaboratrice, infatti, continuava a ricevere sul suo computer e sul telefono gli avvisi e le richieste di immettere la nuova password di accesso, che era stata cambiata da remoto a sua insaputa. L'interessata ha segnalato l'accaduto alla società, chiedendo il tempestivo ripristino della casella di p

osta, che conteneva comunicazioni di lavoro e personali, ma non avendo ricevuto risposta si è rivolta al Garante. Nel corso del procedimento la società non ha provato di avere rilasciato all'interessata alcuna informativa in merito al trattamento dei dati, in particolare con riferimento all'account di posta elettronica aziendale, in costanza di rapporto ed al termine di questo, comprese la gestione dello stesso dopo la cessazione del rapporto e la conservazione dei dati presenti n

ella casella elettronica. Il Garante ha deciso che: a)il diritto di essere informato a riguardo della gestione delle caselle di posta elettronica è previsto a favore di qualsiasi persona fisica in quanto interessata' e, quindi, non è riservato esclusivamente al lavoratore subordinato

, ma è appannaggio anche del collaboratore esterno; b)nell'ambito di un rapporto di lavoro di qualsiasi tipo, informare compiutamente il prestatore dell'attività lavorativa sul trattamento dei suoi dati è

espressione dei principi generali di liceità e correttezza dei trattamenti. 22. NON SI COMUNICA CON UNA E-MAIL AGLI UTENTI LA GRAVIDANZA DELLA DIPENDENTE (Ingiunzione n. 152 del 28 aprile 2022) In due parole È illegittima, perché eccessiva e senza base giuridica, la comunicazione agli utenti dell

a causa dell'assenza di una dipendente in stato di gravidanza. La storia Un asilo privato, in periodo di diffusione della pandemia Covid, ha mandato una e-mail ai genitori per avvisarli del fatto che una maestra sarebbe stata assente a causa del suo stato gravidanza. La scuola ha dichiarato di aver agito in buona fede, in un periodo complicato dal diffondersi della pandemia, per rassicurare i genitori sulle ragioni dell'assenza ed anche con l'intento di proteggere la reputazione dell'educatrice, che aveva dovuto lasciare bruscamente e senza saluti la classe. Il Garante ha deciso che a)è illecita la comunicazione effettuata da una società che gestisce un asilo nido alle famiglie dei bambini iscritti concernente lo stato di gravidanza della loro educatrice e la necessità, per la stessa, di assentarsi dal lavoro, in considerazione della qualificazione del ruolo di insegnante come posizione ad alto rischio; b)risulta violato il diritto dell'interessata di det

erminare le proprie scelte riguardanti le modalità e i tempi con i quali rendere noto uno stato, avente

natura eminentemente privata, a soggetti terzi, estranei al rapporto di lavoro, nell'ambito del quale l'informazione era stata doverosamente resa, peraltro in una fase ancora del tutto iniziale della gravidanza; c)il trattamento dei dati è avv

enuto in violazione dei principi di liceità e minimizzazione dei dati, trattandosi di informazioni fornite a terzi non necessarie rispetto alle finalità perseguite e in assenza di un idoneo criterio di legittimazione. CONTROLLI 23. SANZIONI DOPPIE PER VIDEOSORVEGLIANZA SENZA ACCORDO SINDACALE (Ingiunzione n. 58 del 2 marzo 2023) In due parole In caso di videosorveglianza installata in violazione dell'a

rticolo 4 della legge 300/1970 non c'è bis in idem se il Garante applica le sanzioni del Gdpr dopo quelle irrogate dall'Ispettorato nazionale del lavoro (INL). La storia Un'impresa, che gestisce esercizi commerciali, ha installato e utilizzato impianti di videosorveglianza in assenza dell'accordo sindacale o dell'autorizzazione dell'Ispettorato del lavoro. La violazione dell'articolo 4 dello Statuto dei lavoratori è stata sanzionata dall'Ispettorato. Il Garante deve decidere se e come applicare la sanzione prevista dall'articolo 114 del codice della privacy. Il Garante ha deciso che: a)l'articolo 4 della legge n. 300 del 1970 prevede la competenza dell'INL al rilascio della autorizzazione amministrativa necessaria ai fini dell'installazione di impianti audiovisivi e altri strumenti dai quali derivi anche la possibilità di controllo a distanza dei lavoratori per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale con riferimento a profili prettamente lavoristici; b)l'articolo 114 del Codice della privacy incardina la competenza del Garante relativamente alla verifica del rispetto della disciplina di protezione dei dati personali anche ai fini della disciplina sui controlli a distanza, attribuendo poteri sia sanzionatori sia correttivi, prevedendo, tra l'altro, una propria cornice edittale completamente differente da quella prevista per il lato lavoristico; c)se il Garante ravvisa la violazione dell'articolo 114 del Codice, deve accertare la stessa, disponendo le misure correttive e sanzionatorie necessarie, sia nel c

aso in cui l'Ispettorato abbia provveduto, per i profili di propria competenza, a sanzionare il soggetto che ha tenuto una condotta in violazione dell'articolo 4 della legge 300 del 1970, sia nel caso in cui lo stesso non abbia proceduto in tal senso; d)gli ambiti di operatività delle due discipline, seppure collegati, sono quindi autonomi; e)nell'ambito delle valutazioni relative alla commisur

azione della sanzione applicabile al caso concreto il Garante può comunque tenere conto delle sanzioni amministrative applicate dall'Ispettorato e pagate dall'impresa. 24. L'ACCORDO SINDACALE NON SCRIMINA IL CONTROLLO A TAPPETO DELLA NAVIGAZIONE SUL WEB DEL DIPENDENTE (Ingiunzione n. 190 del 13 maggio 2021) In due parole Indipendentemente da specifici ac

cordi sindacali, le eventuali attività di monitoraggio della navigazione internet dei lavoratori devono comunque essere sempre svolte nel rispetto dello Statuto dei lavoratori e della normativa sulla privacy. La storia Un lavoratore dipendente, nel corso di un procedimento disciplinare, aveva scoperto di essere stato costantemente controllato. Il datore di lavoro, che inizialmente gli aveva contestato la consultazione

di Facebook e Youtube durante l'orario di lavoro, aveva poi archiviato il procedimento per l'inattendibilità dei dati di navigazione raccolti. Il datore di lavoro aveva stipulato un accordo con le organizzazioni sindacali, come richiesto dalla disciplina di settore. Nel corso del reclamo presentato dal lavoratore, il Garante ha accertato che il datore di lavoro impiegava, da circa dieci anni, un sistema di controllo e filtraggio della navigazione internet dei dipendenti, con la conservazione dei dati per un mese e la creazione

di apposita reportistica, per finalità di sicurezza della rete. Il sistema in questione, peraltro, senza aver adeguatamente informato i dipendenti, consentiva inoltre operazioni di trattamento non necessarie e sproporzionate rispetto alla finalità di protezione e sicurezza della rete interna, effettuando una raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web visitati dai singoli dipendenti. Il sistema raccoglieva anche informazioni estranee all'attività professionale e comunque riconducibili alla vita privata dell'interessato. Il Garante ha deciso che a)l'esigenza di ridurre il rischio di usi impropri della navigazione in Internet non può portare al completo annullamento di ogni aspettativa di riservatezza dell'interessato sul luogo di lavoro, anche nei casi in cui il dipendente utilizzi i servizi di rete messi a disposizione del datore di lavoro; b)a prescindere dal contenuto dell'accordo sindacale, il trattamento di dati deve rispettare anche i principi di protezione dei dati previsti dal Gdpr. 25. CONTROLLO PRESENZE MEDISANTE DATI BIOMETRICI SENZA AUTORIZZAZIONE DELL'ISPETTORATO, MA NON BASTA (Ingiunzione n. 404 del

14 settembre 2023) In due parole Anche se il sistema di controllo biometrico degli accessi non richiede l'autorizzazione dell'Ispettorato, ciò non è sufficiente a renderlo legittimo rispetto al Gdpr La storia Un datore di lavoro ha adottato un sistema di rilevazione delle presenze basato sulla lettura delle impronte digitali

e ha chiesto all'Ispettorato del lavoro territorialmente competente richiede l'autorizzazione di cui all'art. 4 della legge 300/1970. L'Ispettorato ha confermato che l'installazione del sistema di rilevazione delle presenze, basato sul riconoscimento biometrico, non richiede la pre

detta autorizzazione. Il Garante ha deciso che a)la non necessità di autorizzazione ex articolo 4 dello Statuto dei lavoratori no

n rende lecito rispetto al Gdpr il trattamento dei dati biometrici, privi di base giuridica per assenza di normativa di copertura normativa; b)il Garante ha applicato la sanzione per trattamento privo di base giuridica. VICENDE DEL RAPPORTO DI LAVORO 26. NON SI PUÒ USARE LA BIOMETRIA PER IL CONTROLLO DELLE PRESENZE DEI LAVORATORI (Ingiunzione n. 404 del 14 settembre 2023) In due parole Il sistema di rilevazione biometrica dell'accesso dei lavoratori è illegittimo perché non previsto da una norma. La storia Un datore di lavoro ha adottato un sistema di rilevazione delle presenze basato sulla lettura delle impronte digitali. Il Garante ha deciso che a)affinché un trattamento avente

a oggetto dati biometrici possa essere lecitamente realizzato non basta che sia necessario per la gestione

del rapporto di lavoro, essendo anche necessario che lo stesso trovi il proprio fondamento in una disposizione normativa che abbia le caratteristiche richieste dalla disciplina di protezione dei dati, b)allo stato non s

ussiste un'idonea base giuridica che possa soddisfare i requisiti richiesti dal Gdpr e dal Codice per legittimare i titolari del trattamento a porre in essere il trattamento dei dati biometrici per finalità di rilevazione delle presenze dei dipendenti ai sensi dell'articolo 9, par. 2, lett. b) del Gdpr. 27. LA CONVOCAZIONE DELL'ISPETTORATO DEL LAVORO NON GIUSTIFICA LA COMUNICAZIONE DI DATI GIUDIZIARI SUL LAVORATORE (Ingiunzione n. 167 del 27 aprile 2023) In due pa

role Quando l'Ispettorato del lavoro convoca per un tentativo di conciliazione, il dat

ore di lavoro non può rispondere comunicando dati giudiziari del lavoratore. La storia Rispondendo all'Ispettorato Territoriale del Lavoro, nell'ambito di tentativo di conciliazione, un datore di lavoro ha comunicato all'ufficio che: per quanto di utilità, va inoltre evidenziato che la Procura della Repubblica, in relazione a procedimento penale pendente a carico del lavoratore, con decreto di esibizione ha delegato la Polizia giudiziaria locale all'acquisizione di documentazione inerente agli affidamenti contrattuali in capo al medesimo. Il lavoratore ha presentato un reclamo per indebita comunicazione di dati giudiziari. Il Garante ha deciso che: a)l'informazione sulla pendenza di indagini penali è un dato giudiziario anche se non vi siano riferimenti espressi agli specifici reati commessi o ai procedimenti giudiziari in corso; b)il datore di lavoro può comunicare all'Ispettorato Territoriale del Lavoro i dati personali relativi a reati solo nel caso in cui una norma di legge lo autorizzi; c)non può applicarsi in questi casi, l'articolo 2-octies, comma 3, lett. e), del Codice della privacy, ai sensi del quale il trattamento di dati personali relativi a condanne penali e a reati è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Al momento della replica alla comunicazione dell'Ispettorato Territoriale del Lavoro, con la quale lo stesso limiti a convocare il datore di lavoro per il tentativo di concili azione monocratica con riferimento alle rivendicazioni del lavoratore (mancata corresponsione degli emolumenti dovuti quale lavoratore subordinato), a tale momento non sussistono ancora effettive esigenze difensive: il tentativo di conciliazione potrebbe concludersi con un accordo tra le parti, senza che si concretizzi la necessità per il datore di lavoro di e

sercitare alcuna difesa, dando conto, in tale sede, della condizione d'indagato dell'interessato; d)quando si forniscono informazioni, scrivendo l'espressione per quanto di utilità si dimostra che non c'è comprovata esigenza di comunicare dati di soggetti interessati. 28. INUTILIZZABILI NEL PROCEDIMENTO DISCIPLINARE I DATI RACCOLTI IN VIOLAZIONE DELLA PRIVACY (Ingiunzione n. 577 del 16 novembre 2023) In due p

arole Un datore di lavoro non può utilizzare nel procedimento disciplinare contro un proprio dipendente dati personali acquisiti in violazione del Gdpr, in quanto l'illegittima acquisizione rende i dati inutilizzabili. La storia Un datore di lavoro ha utilizzato nel procedimento disciplinare contro un proprio dipendente

registrazioni audio-video acquisite in violazione del Gdpr: nel caso specifico un comune ha raccolto la registrazione di un colloquio di un suo dipendente presso gli uffici di un altro ente, adducendo non fondate ragioni di giustizia. Il comune ha usato la registrazione per contestare illeciti disciplinari al dipendente, che ha presentato reclamo al Garante della privacy. Il Garante ha deciso che a)il titolare del trattamento può successivamente utilizzare i soli dati personali lecitamente raccolti e, quindi, nei limiti in cui l'originaria raccolta si

a stata lecitamente effettuata; b)è illecito usare in un procedimento disciplinare contro un dipendente dati acquisiti irregolarmente; c)l'illiceità della raccolta dei dati investe anche il successivo trattamento di dati personali; d)se i dati sono raccolti in assenza di una base giuridica, non po

ssono essere utilizzati per una finalità ulteriore, come per avviare un procedimento disciplinare nei confronti del dipendente; e)i successivi trattamenti - ancorché effettuati nell'ambito dell'esercizio di compiti e poteri attribuiti al datore di lavoro sono viziati dall'illecita acquisizione e, quindi, avvengono in modo non conforme alla disciplina in materia di protezione dei dati personali. 29. IL FORNITORE DI SERVIZI DI GEOLOCALIZZAZIONE PER CONTO DEL DATORE DI LAVORO È UN RESPONSABILE DEL TRATTAMENTO (Ingiunzione n. 428 del 15 dicembre 2022) In due parole Il fornitore di servizi di geolocalizzazione per conto del datore di lavoro deve essere designato

responsabile del trattamento. La storia Un lavoratore ha lamentato il rinvenimento, nel vano motore del proprio veicolo adibito al trasporto beni, di un dispositivo di geolocalizzazione. L'attività di geolocalizzazione era effettuata da un distinto soggetto, che metteva a disposizione del datore di lavoro sia i dispositivi sia l'accesso ad un applicativo web. Quest'ultimo consentiva la localizzazione mediante sistema Gps, il controllo su mappa della distanza percorsa da ciascun veicolo, il calcolo dei chilometri, del tempo di viaggio e della velocità media di guida. Il sistema installato sul veicolo aziendale era associato alla targa del veicolo e non (direttamente) al nome dell'autista. Il Garante ha deciso che a)è configurabile un trattamento di dati personali anche qualora il dispositivo completo di funzionalità di geolocalizzazione (tram

ite sistema Gps) installato sul veicolo aziendale sia associato alla targa del veicolo e non (direttamente) al nome dell'autista, poiché è possibile identificare il guidatore del mezzo anche attraverso l'associazione con altre informazioni (ad esempio i documenti relativi ai turni di servizio); b)il rapporto con il fornitore del servizio deve essere regolato ai sensi dell'articolo 28 del Gdpr (responsabile del trattamento); c)in mancanza di designazione del fornitore del servizio di localizzazione quale responsabile del trattamento si viola il Gdpr, posto che il titolare ha, in tal modo, effettuato una comunicazione a terzi, in assenza di un idoneo presupposto di liceità del trattamento. 30. IL MEDICO COMPETENTE

È TITOLARE AUTONOMO (Ingiunzione n. 522 del 31 agosto 2023) In due parole Il medico competente deve informare il

lavoratore se esamina i dati sanitari per una consulenza a un'impresa La storia Un'impresa, per una

verifica sommaria della compatibilità delle condizioni fisiche di una persona disabile rispetto alla prevista mansione impiegatizia, ha chiesto al medico competente un parere preventivo. Il medico competente ha esaminato la documentazione medica presentata spontaneamente dal candidato all'impresa e ha ritenuto, sulla base delle patologie indicate nei documenti e senza visita medica, di dover esprimere un preventivo parere di controindicazione rispetto alla mansione impiegatizia. L'interessato ha presentato reclamo al Garante, il quale ha aperto un procedimento contro il medico competente. Il Garante ha deciso che a)il medico competente è titolare del trattamento relativamente ai trattamenti volti a valutare l'idoneità alla mansione del lavoratore; b)il medico competente ha effettuato alcune operazioni di trattamento riferite all'interessato che risultano non conformi alla disciplina in materia di protezione dei dati personali, in particolare per avere omesso l'informativa; c)si aggiunge che a riguardo della qualifica del medico competente il Garante ha preso posizione con

i seguenti provvedimenti del Garante: provvedimento 27 aprile 2016, n. 194; Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro, con particolare riguardo alla tenuta delle cartelle sanitarie e di ris chio da parte del medico competente e alla diversa attività di tenuta e aggiornamento dei fascicoli personali dei dipendenti da parte del datore di lavoro; nota 19 marzo 2019 di risposta al quesito specifico posto dalla Società Italiana di Medicina del Lavoro; Documento Il ruolo del medico competente in materia di s

icurezza sul luogo di lavoro, anche con riferimento al contesto emergenziale. 31. LA CONCILIAZIONE DELLA CAUSA DI LAVORO NON FERMA IL RECLAMO DEL GARANTE (Ingiunzione n. 66 del 9 marzo 2023) In due parole Se il lavoratore e il datore di lavoro chiudono, con una transazione, la controversia di lavoro, questo accordo non rende improcedibile il re

clamo pendente avanti al Garante. La storia Alcuni lavoratori e il proprio datore di lavoro raggiungono un accordo e chiudono una causa pendente avanti al tribunale. Nel parallelo procedimento di reclamo avanti al Garante, il datore di lavoro ritiene che la transazione intervenuta comporti il venir meno dell'interesse alla prosecuzione del reclamo. Il Garante ha deciso che a)la conciliazione giudiziale ha ad oggetto profili prettamente lavoristici e non relativi alla protezione dei dati e, quindi, non è idonea a determinare l'archiviazione del procedimento del Garante nei confronti della società; b)il potere di accertamento attribuito al Garante non è subordinato all'iniziativa di parte.

