ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO

Direzione generale
Direzione centrale per l'organizzazione digitale

Circolare n. 37

Roma, 20 ottobre 2020

Al Direttore generale vicario
Ai Responsabili di tutte le Strutture centrali e territoriali

e p.c. a: Organi istituzionali
Magistrato della Corte dei conti delegato all'esercizio del controllo
Organismo indipendente di valutazione della performance
Comitati consultivi provinciali

Oggetto

Istruzioni operative per le Strutture centrali e territoriali in materia di *privacy*.

Quadro normativo

- **Decreto legislativo 30 giugno 2003, n. 196:** "Codice in materia di protezione dei dati personali".
- **Provvedimento del Garante del 1° marzo 2007:** "Lavoro: le linee guida del Garante per posta elettronica e internet.
- **Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (GDPR)** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
- **Determinazione del Presidente Inail 22 marzo 2018, n. 149:** "Regolamento unico per la disciplina del diritto di accesso ai documenti amministrativi ai sensi degli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e del diritto di accesso a documenti, dati e informazioni ai sensi degli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33.
- **Determinazione del Presidente Inail 22 maggio 2018, n. 234:** "Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» - RGPD. Designazione del

Responsabile della protezione dei dati personali (RPD) - art. 37 Regolamento UE 2016/679".

- **Decreto legislativo 10 agosto 2018, n. 101:** "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati".

- **Determinazione del Presidente Inail 8 ottobre 2019, n. 297:** "Regolamento unico per la disciplina del diritto di accesso ai documenti amministrativi ai sensi degli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e del diritto di accesso a documenti, dati e informazioni ai sensi degli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33. Modifiche".

- **Determinazione del Presidente Inail munito dei poteri del Consiglio di amministrazione 12 marzo 2020, n. 53:** "Nuovo modello organizzativo della privacy e della protezione dei dati personali ai sensi del Regolamento UE 2016/679 (GDPR)"

- **Circolare Inail 12 maggio 2020, n. 19**: "Designazione degli autorizzati al trattamento dei dati personali, relative istruzioni operative e contestuale pubblicazione della nuova versione dell'informativa per l'utilizzo di posta elettronica e internet da parte dei dipendenti".

Premessa

Il modello organizzativo della *privacy* e della protezione dei dati, modificato in base al Regolamento Ue 2016/679 (*General Data Protection Regulation* - GDPR), di cui alla determinazione del Presidente Inail munito dei poteri del Consiglio di amministrazione del 12 marzo 2020, n. 53, conferisce, nell'ambito dell'organizzazione dell'Istituto, specifiche responsabilità a vari livelli, finalizzate alla conformità al GDPR relativamente ai trattamenti di cui l'Istituto è titolare.

Il codice della *privacy* italiano, introdotto con il decreto legislativo 30 giugno 2003, n. 196, contemplava la figura del responsabile interno e dell'incaricato del trattamento dei dati. A questo riguardo:

- relativamente alla figura del responsabile, il GDPR (art. 28) nel disciplinare tale figura si riferisce esclusivamente al "responsabile esterno", come ulteriormente avallato anche dal Gruppo di lavoro (art. 29)[1]. L'Istituto, in ottemperanza alla normativa, con la determinazione presidenziale del 12 marzo 2020, n. 53 recante il nuovo modello organizzativo della *privacy* e della protezione dei dati personali ai sensi del GDPR:
  - abroga la figura formale di responsabile interno;
  - distribuisce le responsabilità interne in modo specifico e concreto. Tali responsabilità discendono dai compiti all'interno dell'organizzazione, tenendo presente che ogni compito ha una relazione con la protezione dei dati personali.
- relativamente alla figura dell'incaricato, il GDPR non la contempla esplicitamente, né richiede la relativa nomina formale in forma scritta come invece previsto dal decreto legislativo 30 giugno 2003, n. 196. Il GDPR infatti, al fine di favorire una

[1] v. parere 1/2010 dello stesso Gruppo di lavoro.

distribuzione delle responsabilità che sia più sostanziale che formale, lascia al titolare la possibilità di individuare e designare le persone cosiddette autorizzate al trattamento dei dati personali. Pertanto l'Istituto, con la circolare Inail 12 maggio 2020, n. 19, ha individuato le modalità di designazione degli autorizzati al trattamento dei dati personali e indicato le relative istruzioni operative.

La presente circolare declina gli adempimenti necessari alle Strutture centrali e territoriali per operare in conformità alla normativa in materia di privacy comprese le azioni relative all'ambito di "gestione delle violazioni di dati personali (*data breach*)".

Rispetto dei principi GDPR

Le Strutture centrali e territoriali, secondo i propri ambiti di competenza, governano, con riferimento alle politiche, istruzioni e linee guida emesse, gli aspetti legati alla protezione dei dati nelle attività del territorio, negli ambulatori e nei rapporti con l'utenza, compresi quelli legati alla videosorveglianza e alla sicurezza fisica. La Direzione centrale per l'organizzazione digitale, in accordo con il Responsabile della protezione dati personali (RPD) evolve e aggiorna tali linee guida, politiche e istruzioni operative, pubblicandole nella sezione *Privacy* del *repository* ufficiale di Inail.

Nel trattare i dati personali, indipendentemente dalla loro natura ordinaria o particolare (categorie di dati personali che comprendono dati relativi alla salute) o di dati personali relativi a condanne penali e reati, le Strutture centrali e territoriali devono puntualmente attenersi ai principi e agli obblighi del GDPR, nonché al modello organizzativo *privacy* dell'Istituto di cui alla determinazione del Presidente Inail munito dei poteri del Consiglio di amministrazione del 12 marzo 2020, n. 53. Nel caso di utilizzo di collaboratori esterni (es. stagisti, fornitori, consulenti), le Strutture centrali e territoriali notificano le istruzioni in materia di trattamento di dati personali estendendo anche a tali figure le istruzioni contenute nella circolare Inail 12 maggio 2020, n. 19.

I responsabili delle Strutture si impegnano a garantire, nel proprio ambito di responsabilità, il pieno rispetto dei principi del GDPR e vigilano sui comportamenti dei dipendenti e dei collaboratori esterni, che devono trattare i dati in modo consapevole e corretto.

Gestione del registro delle attività di trattamento (art. 30 del GDPR)

Il registro delle attività di trattamento è uno degli adempimenti previsti dal Regolamento Ue 2016/679, che deve anche essere messo a disposizione dell'autorità di controllo qualora richiesto. Il registro, corretto e aggiornato nel tempo, costituisce una significativa evidenza della responsabilizzazione del titolare e del responsabile, ed è uno strumento fondamentale non soltanto per disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'organizzazione, ma è anche la fonte primaria di riferimento per lo svolgimento delle attività di analisi e valutazione degli impatti sulla *privacy* e dei rischi di sicurezza delle informazioni trattate.

Il registro delle attività di trattamento dell'Istituto indica, per ogni specifico trattamento, la Struttura Inail che ha la titolarità istituzionale dei servizi correlati.

Tali Strutture in relazione ai predetti trattamenti:

- assicurano la liceità e il rispetto dei principi del GDPR;
- collaborano con il Responsabile della protezione dei dati (RPD) nella definizione del registro dei trattamenti e comunicano nuovi trattamenti o eventuali variazioni

inerenti i trattamenti di loro competenza, in modo da garantire il costante aggiornamento del registro;

- pongono particolare attenzione a informazioni quali il periodo di conservazione dei dati, la presenza di dati di minori, il trasferimento dei dati verso paesi terzi e alle relative prescrizioni previste dal GDPR.

Valutazione d'impatto (artt. 35 e 36 del GDPR)

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate, il GDPR impone al titolare di effettuare una valutazione di impatto sulla protezione dei dati (DPIA). Qualora il rischio residuale per i diritti e le libertà degli interessati resti elevato, ovvero nel caso in cui le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti, è necessario consultare l'autorità di controllo.

La valutazione di impatto sulla protezione dei dati deve essere condotta prima di procedere al trattamento, in fase di definizione dello stesso, e deve essere sottoposta a un continuo riesame, ripetendo la valutazione a intervalli regolari o, comunque, appena intervengono sostanziali modifiche al contesto del trattamento.

La Direzione centrale per l'organizzazione digitale, insieme al RPD, valuta la necessità di predisporre le valutazioni di impatto sulla protezione dei dati, e rende disponibile la metodologia di valutazione.

Nella predisposizione delle valutazioni di impatto, le Strutture forniscono il contributo per gli aspetti di loro competenza.

Informative specifiche, comunicazioni agli interessati (artt. 12, 13 e 14 del GDPR) e gestione del consenso al trattamento (artt. 7 e 8 del GDPR)

L'informativa all'interessato rappresenta uno degli adempimenti principali in capo al titolare del trattamento.

Tenuto conto di tutte le informazioni disponibili grazie al registro delle attività di trattamento, l'Inail, in qualità di titolare del trattamento, deve:

- definire o aggiornare le informative, che devono essere adeguate nella forma e nel linguaggio alla tipologia di soggetto interessato (per esempio: dipendenti, clienti, utenti, minori, ecc.) e devono contenere tutte le informazioni necessarie a comprendere l'identità e i dati di contatto del titolare e del RPD, la descrizione delle modalità e le finalità del trattamento, la base giuridica, ecc.;
- garantire che le informative, una volta diffuse e condivise:
  - siano sempre disponibili o, comunque, facilmente reperibili attraverso canali individuati (fisici e telematici);
  - vengano aggiornate a valle dell'attività di valutazione e modifica del registro delle attività di trattamento.

La Direzione centrale per l'organizzazione digitale predispone i modelli generali per le informative e cura la redazione dell'informativa pubblicata sul portale istituzionale, valida per tutti i servizi erogati in modalità digitale.

Qualora fossero necessarie informative di dettaglio, relative a trattamenti specifici, le Strutture di competenza contribuiscono alla definizione dei contenuti delle informative, nonché alla distribuzione delle stesse agli interessati.

Nel caso di trattamenti basati sul consenso degli interessati, le Strutture di competenza, sempre in accordo con il RPD, ne identificano le modalità di raccolta e revoca.

Sorveglianza (art. 24 del GDPR)

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi e degli impatti per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, e a essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (articolo 24, paragrafo 1 del GDPR).

La sorveglianza in ambito *privacy*, che rappresenta anche uno dei compiti espliciti che il GDPR assegna al RPD (articolo 39 paragrafo 1.b) consiste nel sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione Europea o nazionali, relative alla protezione dei dati personali.

Le attività di sorveglianza comprendono, tra l'altro:

- la verifica della completezza e della correttezza delle informazioni inserite nel registro dei trattamenti;
- la verifica della corretta predisposizione e gestione delle attività inerenti e connesse al trattamento (gestione dell'informativa, gestione del consenso, gestione dei diritti dell'interessato, gestione del rischio, valutazione d'impatto, gestione dei *data breach*);
- la verifica dell'applicazione e dell'efficacia delle misure di sicurezza adottate;
- la verifica dell'applicazione delle istruzioni per la corretta gestione dei trattamenti.

In questo ambito tutte le Strutture supportano il RPD nelle attività di sorveglianza, fornendo quando richiesto ogni evidenza necessaria all'espletamento di tale attività.

Gestione delle violazioni di dati personali - *data breach* (artt. 33 e 34 del GDPR)

Un *data breach* è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati. A titolo esemplificativo, un *data breach* può essere causato dalla perdita di un dispositivo contenente dati personali, dall'invio per errore di dati personali a terzi non autorizzati, dalla condivisione di informazioni non adeguatamente protette, ecc.

In caso di *data breach*, ossia in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati, il GDPR prevede che il titolare lo notifichi all'autorità competente, ed eventualmente anche agli interessati.

Per consentire una corretta segnalazione e gestione dei *data breach*, le Strutture coinvolte:

- segnalano al RPD ogni situazione di violazione dei dati personali di cui sono a conoscenza;
- forniscono l'eventuale supporto richiesto per le attività di indagine;

- concorrono, in relazione alla propria competenza, alla gestione dei *data breach*.

La violazione dei dati personali può riguardare anche il contesto non informatico, per esempio il furto di faldoni cartacei contenenti pratiche con dati degli infortunati, oppure un incendio o allagamento di siti in cui risiedono faldoni cartacei, contenenti dati personali non disponibili in altro modo.

Nella gestione di questi *data breach*, le Strutture centrali e territoriali coinvolte hanno un ruolo di primaria importanza, in particolare:

- devono acquisire e fornire i dettagli relativi alla violazione dei dati, quali il tipo di dati violati, la quantità, la modalità, ecc.
- predisporre la **Scheda di *Data Breach***, coinvolgendo il Dirigente generale di riferimento per la Struttura. Qualora lo ritenga necessario, la Struttura attiva il Cert Inail riconducendo il processo alla gestione degli incidenti IT. Discrezionalmente, in accordo con il RPD, può gestire il caso di *data breach* in autonomia.

Si rammenta che sul tema dei *data breach*, e più in generale sulla protezione dei dati personali, le Strutture centrali e territoriali possono comunicare, richiedere informazioni e collaborare anche con l'Ufficio preposto della Dcod.

Gestione dell'esercizio dei diritti degli interessati (artt. da 15 a 22 del GDPR)

Il GDPR riconosce a tutti gli interessati importanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al titolare del trattamento. L'Istituto è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica e organizzativa a ciò idonea.

Nella fattispecie, il canale principale che l'Istituto ha predisposto al fine di ricevere le richieste degli interessati, in relazione ai propri diritti sanciti nel GDPR, è il servizio del portale "Inail Risponde", come indicato nell'informativa pubblicata sul portale istituzionale.

Le Strutture centrali e territoriali forniscono, su richiesta del RPD o dell'Ufficio preposto della Dcod, le informazioni necessarie al fine di gestire le istanze di esercizio dei predetti diritti nel rispetto dei principi previsti dal GDPR.

Qualora gli interessati sottoponessero una richiesta in relazione ai propri diritti non utilizzando il canale principale di "Inail Risponde" (per esempio attraverso mail o pec), l'Istituto ha comunque il dovere di fornire un riscontro in merito. Pertanto, le Strutture devono inoltrare tempestivamente queste richieste alla casella **protezionedati@inail.it**.

Gestione dei contratti e delle convenzioni che prevedono trattamenti e scambio di dati

L'Inail, nell'ambito delle sue attività e finalità, instaura convenzioni e protocolli d'intesa con altri enti e organizzazioni, nonché stipula contratti e accordi con terze parti. Tutti questi atti devono esplicitamente e adeguatamente indirizzare gli aspetti di protezione dei dati personali.

La nomina di un responsabile del trattamento è richiesta nel caso si verifichi la situazione in cui un'altra persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo

tratta dati personali per perseguire le finalità del titolare del trattamento (l'Istituto), condividendo con quest'ultimo gli strumenti e le modalità da utilizzare.

Per la nomina a responsabile, il soggetto deve presentare garanzie sufficienti e l'accertamento di tali garanzie deve essere documentato (ai sensi dell'art 28), tenendo presente che Titolare e Responsabile del trattamento assumono in solido (art 82) le responsabilità di danni cagionati agli interessati. La nomina a responsabile del trattamento è un atto contrattuale (art 28) che può essere incorporato nel contratto di fornitura o in un articolo della convenzione, oppure configurarsi come allegato che ne rappresenta comunque un'estensione e quindi firmato per conto dell'Istituto dallo stesso soggetto che stipula e firma il contratto o la convezione da cui la responsabilità scaturisce.

In questo senso, tutte le Strutture che gestiscono contratti e/o convenzioni che comportano trattamenti e/o scambio di dati ai sensi del regolamento:

a. verificano che le organizzazioni e i fornitori individuati, che si configurano come responsabili esterni del trattamento, presentino garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate, in modo che il trattamento soddisfi i requisiti del GDPR;
b. in caso di convenzioni che prevedano scambio dati, valutano accuratamente la rispondenza ai principi del GDPR e in particolare alle condizioni di liceità del trattamento e alle esigenze di minimizzazione dei dati personali. Inoltre, le modalità di scambio dati e le relative misure di sicurezza devono essere tali da rispettare gli *standard* e le indicazioni generali dell'Istituto in materia di sicurezza delle informazioni;
c. provvedono, ove necessario, all'atto di nomina dei responsabili del trattamento utilizzando lo schema-tipo definito e pubblicato nel sistema documentale e trasmettendo al RPD copia di tale atto.

La nomina a responsabile del trattamento non deve essere conferita nel caso in cui l'organizzazione terza o il fornitore persegua le proprie finalità, definendo autonomamente gli strumenti e le modalità operative del trattamento. A titolo esemplificativo la nomina non deve essere conferita nel caso di convenzioni con strutture sanitarie pubbliche e/o private per l'erogazione di prestazioni integrative riabilitative e sanitarie. In tal caso infatti tali strutture svolgono le attività oggetto di convenzione operando come titolari autonomi del trattamento.

In relazione ai punti di cui sopra, le Strutture si avvalgono del supporto del RPD.

Gestione degli aspetti comunicativi e di formazione

Il Responsabile della protezione dei dati e la Direzione centrale per l'organizzazione digitale promuovono adeguate iniziative finalizzate al raggiungimento della maturità e della consapevolezza in tema di protezione dati.

La Direzione centrale risorse umane assicura la formazione del personale e in particolare di coloro che effettuano trattamenti di dati personali, avvalendosi della collaborazione delle Strutture competenti per materia.

La Direzione centrale pianificazione e comunicazione assicura la divulgazione al personale delle informazioni e delle *policy* in materia di sicurezza e protezione dei dati, avvalendosi della collaborazione delle Strutture competenti per materia.

La Direzione centrale per l'organizzazione digitale promuove adeguate iniziative finalizzate all'accrescimento della consapevolezza e della cultura sulla sicurezza delle informazioni.

Gestione dei documenti informatici e cartacei

Le Strutture centrali e territoriali devono attenersi, in generale, alle linee guida, alle *policy* di sicurezza dell'Istituto presenti nella sezione sicurezza del *repository* ufficiale di Inail.

In seguito si riportano alcune prescrizioni relative ad aspetti di interesse comune su tematiche specifiche:

- Gestione di stampanti e fax

Relativamente a stampanti condivise e fax, ma anche nel caso di stampanti personali, è importante che queste vengano usate nel modo appropriato al fine di non diffondere, anche involontariamente, dati personali eventualmente contenuti nelle stampe.

È quindi fondamentale agevolare l'uso sicuro delle stampanti e dei fax, posizionandoli opportunamente (per esempio i fax andrebbero posti in stanze chiuse) e facendo sì che il personale stampi dati personali solo quando strettamente necessario all'attività lavorativa e protegga le stampe usando le funzionalità di sicurezza native dei dispositivi (per esempio l'uso di un Pin di protezione che permetta il recupero della stampa solo a chi ne è a conoscenza).

- Gestione cartaceo

Le informazioni e quindi i dati personali, oltre a essere mantenute sui sistemi informatici, possono per diverse esigenze essere presenti su supporto cartaceo.

Alle informazioni presenti su supporto cartaceo va comunque garantita la stessa riservatezza di quelle mantenute su sistemi informatici. Pertanto, i supporti cartacei devono essere opportunamente custoditi e deve essere impedito qualunque tipo di accesso non autorizzato.

- Archiviazione dei dati personali

Il rispetto delle regole di sicurezza delle informazioni è imprescindibile nell'attività lavorativa e fa parte dei doveri quotidiani verso l'Istituto, ma soprattutto nei confronti di lavoratori e aziende dei quali l'Inail detiene e gestisce dati personali.

L'atteggiamento consapevole e informato nell'utilizzo degli strumenti che l'Istituto mette a disposizione (dispositivi, internet e posta elettronica) è sempre più determinante per proteggere il patrimonio informativo.

Non è ammesso archiviare dati su strumentazione non autorizzata, come per esempio chiavette o dischi esterni personali, né scambiare dati con soggetti o strumenti non autorizzati.

Qualora fosse necessario, sempre comunque nel rispetto dei principi del GDPR come quello della minimizzazione, condividere documenti con colleghi e persone esterne autorizzate o archiviare i documenti e recuperarli in mobilità, è possibile utilizzare InailOneDrive e gli altri strumenti della piattaforma istituzionale (Teams, Sharepoint).

- Protocollo e caselle di posta di Struttura

In generale il protocollo rappresenta per l'Istituto uno dei punti di ingresso di dati personali, in quanto adibito alla ricezione e gestione di documenti, richieste, istanze e pratiche.

Pertanto, risulta di fondamentale importanza che le persone operanti in questo ambito siano sensibilizzate rispetto alla materia dei dati personali, in modo che ogni informazione venga gestita adeguatamente e con le corrette misure di sicurezza delle informazioni.

La responsabilizzazione del personale che opera al protocollo, e che quindi può ricevere mail, fax o pec contenenti dati di qualsiasi natura, è necessaria al fine di evitare violazioni dei dati personali.

In particolare, per le caselle di posta di Struttura e per lo smistamento dei documenti gestiti nell'ambito del protocollo è necessario organizzarsi in modo che l'accesso sia consentito solo al personale autorizzato e opportunamente sensibilizzato.

Particolare attenzione va posta all'inoltro di mail e comunicazioni, dove è fondamentale verificare sempre che i dati personali contenuti siano condivisibili con i destinatari dell'inoltro, eliminando quelli non necessari.

Gestione dei dati per la videosorveglianza

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali e pertanto gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata.

Il Garante per la protezione dei dati personali nel Provvedimento in materia di videosorveglianza dell'8 aprile 2010 aveva individuato un modello semplificato di informativa.

Tuttavia, l'autorità Garante per la protezione dei dati personali e le Linee guida 3/2019 sul trattamento di dati attraverso apparecchiature video del Comitato europeo per la protezione dei dati (EDPB), entrate in vigore il 29 gennaio 2020, puntualizzano come l'informativa debba avere invece un approccio a più livelli.

Pertanto con l'introduzione delle predette Linee guida europee, la precedente informativa semplificata non è più sufficiente a trasmettere agli interessati tutte le informazioni necessarie.

Le Strutture competenti devono gestire l'informativa nel modo seguente:

- prevedere e collocare i cartelli della videosorveglianza prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; i cartelli:
    - devono avere un formato e un posizionamento tale da essere chiaramente visibili in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
    - possono inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate;
    - devono contenere i riferimenti per l'accesso all'informativa estesa (per esempio riportando un *link* o un codice QR per visionarla in formato digitale);

- predisporre l'informativa estesa che deve:
    - identificare il "titolare" e, nel caso, il suo rappresentante;
    - specificare la finalità della sorveglianza;
    - informare l'interessato dell'esistenza dei suoi diritti;
    - riportare informazioni sugli aspetti più impattanti del trattamento, quali per esempio: gli interessi legittimi perseguiti dal titolare o da una terza parte;
    - menzionare chiaramente se le immagini vengono registrate e riportare informazioni sugli aspetti del trattamento che potrebbero non essere ovvi e scontati per l'interessato, per esempio: se sia prevista la trasmissione dei dati a terzi (in particolare se al di fuori dell'UE) e il periodo di conservazione. In assenza di queste ulteriori specifiche l'interessato potrà supporre che esista il solo monitoraggio dal vivo (senza alcuna registrazione o trasmissione di dati a terzi);
    - fornire informazioni di contatto del titolare e del RPD, indicando tutti i riferimenti per la consultazione dell'informativa estesa, sia essa raggiungibile *online* o *offline*.

A ogni modo, i dati raccolti devono essere protetti con misure di sicurezza tecniche, organizzative e preventive che abbattano "i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini". Esempi di misure da adottare sono: credenziali di autenticazione idonee, livelli diversi di accesso, protezione dei rischi in caso di apparati di ripresa digitali connessi a reti informatiche.

Le Strutture devono accertarsi che siano designate per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia a utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Tale designazione, che normalmente si riferisce a personale esterno all'Istituto, può essere predisposta dal fornitore nominato responsabile esterno dalla Struttura di competenza.

La conservazione dei dati personali relativi a tale trattamento è limitata secondo la normativa vigente a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire a una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze e previa autorizzazione del Garante, è possibile estendere il tempo di conservazione dei dati che non dovrà comunque superare la settimana.

La normativa giuslavoristica, e nel dettaglio lo Statuto dei Lavoratori, all'articolo 4 comma 1 prevede che "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano

nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro".

Gestione dei dati nelle attività di contenimento dell'emergenza Covid

Il Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 sottoscritto il 14 marzo 2020 e integrato il 24 aprile 2020 e il Protocollo quadro "rientro in sicurezza" (Protocollo quadro per la prevenzione e la sicurezza dei dipendenti pubblici sui luoghi di lavoro in ordine all'emergenza sanitaria da Covid-19), sottoscritto il 24 luglio 2020 dal Ministro per la pubblica amministrazione e dalle organizzazioni sindacali contengono le linee guida per agevolare le organizzazioni nell'adozione di protocolli di sicurezza anti-contagio negli ambienti di lavoro.

La prosecuzione delle attività produttive può avvenire solo in presenza di condizioni che assicurino alle persone che lavorano adeguati livelli di protezione. La mancata attuazione del Protocollo che non assicuri adeguati livelli di protezione determina la sospensione dell'attività fino al rispristino delle condizioni di sicurezza.

Le Strutture competenti:

- informano, attraverso le modalità più idonee ed efficaci, tutti i lavoratori e chiunque abbia accesso alle Sedi Inail circa le disposizioni delle autorità, consegnando e/o affiggendo all'ingresso e nei luoghi maggiormente visibili dei locali aziendali apposite comunicazioni e informazioni;
- forniscono, con un'informativa adeguata sulla base delle mansioni e dei contesti lavorativi, il complesso delle misure adottate cui il personale deve attenersi;
- prevedono opportune modalità e istruzioni operative, con riferimento alla gestione dei dati personali, tra cui indicazioni per l'accesso alle Sedi (es. rilevamento della temperatura corporea) e la relativa uscita, procedure di gestione persona sintomatica in azienda, ecc.

Gestione delle informative per i visitatori alle Sedi Inail

I dati personali dei visitatori sono registrati per finalità di controllo della sicurezza dei locali e della incolumità fisica delle persone che vi accedono e vanno mantenuti per il solo tempo necessario a espletare dette finalità e protetti da adeguate misure di sicurezza.

In questo contesto le Strutture competenti:

- individuano gli addetti alla vigilanza e/o gli addetti alle funzioni dell'Istituto che curano gli aspetti relativi alla sicurezza dei locali e le squadre di emergenza, come autorizzati al trattamento dei dati sopra descritti;
- rendono disponibile l'informativa sull'utilizzo dei dati personali prima dell'accesso, per esempio al momento della consegna del documento di riconoscimento richiesto per la raccolta dei dati personali;
- prevedono apposite procedure operative che descrivono il processo di richiesta del permesso di accesso allo stabile dei visitatori e/o personale esterno.

Gestione dei dati personali nelle attività sanitarie (sale d'attesa, ambulatori e visite mediche)

Nell'ambito delle prestazioni sanitarie e/o socio-sanitarie erogate dall'Istituto e da strutture pubbliche e private convenzionate con l'Inail, l'impianto normativo del Codice *privacy* (decreto legislativo 30 giugno 2003, n. 196) prevedeva alcune misure per il rispetto dei diritti degli interessati con l'abrogato articolo 83.

Tali misure continuano a trovare applicazione, in quanto compatibili con il GDPR, per effetto delle disposizioni transitorie di cui all'articolo 22, comma 11 del decreto legislativo 10 agosto 2018, n. 101, sino all'adozione delle corrispondenti misure di garanzia che il Garante dovrà emanare.

Per quanto detto le Strutture, ove di competenza, al fine di garantire il rispetto dei diritti, libertà fondamentali e dignità degli interessati devono:

- prevedere soluzioni volte a rispettare, in caso di attesa all'interno delle strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa (sala d'attesa);
- istituire appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere (linea gialla);
- prevedere soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute (visite mediche);
- prevedere cautele volte a evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvengano in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti (visite mediche);
- garantire il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati (visite mediche);
- garantire che eventuali autorizzati al trattamento esterni non dipendenti che non sono tenuti per legge al segreto professionale seguano regole di condotta analoghe;
- garantire che anche per la documentazione sanitaria cartacea acquisita tramite scanner siano applicate le misure di sicurezza relative alla "Gestione dei documenti informatici e cartacei".

Medico competente

Il Garante per la protezione dei dati personali ha precisato che la disciplina di settore (decreto legislativo 9 aprile 2008, n. 81) individua la funzione del medico competente come autonoma rispetto a quella che, pure in tale ambito, deve essere svolta dal datore di lavoro, assegnando specifici e distinti obblighi in capo all'una e all'altra figura, così delineando l'ambito del rispettivo trattamento consentito.

In particolare, nello svolgimento dei compiti che la legge gli attribuisce in via esclusiva (attività di sorveglianza sanitaria e tenuta delle cartelle sanitarie e di rischio dei singoli lavoratori), il medico competente è l'unico legittimato *ex lege* a trattare in piena autonomia e competenza tecnica i dati personali di natura sanitaria indispensabili per tale finalità, come chiarito dal Garante in un provvedimento nel quale è stato precisato, tra gli altri profili, che il medico competente tratta dati personali di natura sanitaria indispensabili ai fini dell'applicazione della normativa in materia di igiene e di sicurezza

del lavoro in qualità di titolare del trattamento (Provvedimento 27 aprile 2016, n. 194, doc. web n. 5149198).

Sulla base di tali valutazioni, il Garante ha quindi sempre considerato il medico competente un autonomo titolare e anche lo stesso GDPR considera in via autonoma le funzioni del medico competente con riguardo ai trattamenti necessari per le finalità di medicina del lavoro (art. 9, lett. h, del GDPR), diversamente dai trattamenti del datore di lavoro necessari per adempiere i propri obblighi normativi in materia di salute e sicurezza sul lavoro (art. 9, lett. b, e art. 88 del GDPR).

Il Direttore generale
f.to Giuseppe Lucibello