LA PRIVACY AI TEMPI DEL CORONAVIRUS

15 maggio 2020

Dott. Stefano Bacchiocchi

Dottore Commercialista in Brescia
Responsabile della Protezione dei Dati (DPO)

info@bacchiocchistudio.it
www.bacchiocchistudio.it

CORONAVIRUS E PRIVACY

E’ INTERESSANTE VEDERE COME ANCHE IN AMBITO PRIVACY IL CORONAVIRUS ABBIA MONOPOLIZZATO L’ATTENZIONE

Da febbraio in poi il Garante si è occupato di decine di materie diverse tra loro:

- Ricetta elettronica
- Ricerca scientifica
- Misurazione della temperatura
- Didattica a distanza
- Coronavirus e social media (troppi dati sui social…)
- App per il tracciamento
- Processo penale
- Ecc.

TUTTE LE RACCOMANDAZIONI HANNO PERÒ UNA MEDESIMA RADICE COMUNE:

- le norme devono prevedere deroghe temporanee;
- deve esserci sempre un bilanciamento costante con gli altri diritti;
- devono essere chiare le prerogative dei vari attori coinvolti (medici, autorità sanitarie, datori di lavoro ecc.);

«Non è vero che la privacy è il lusso che non possiamo permetterci in questo tempo difficile, perché essa consente tutto ciò che è ragionevole, opportuno e consigliabile fare per sconfiggere il coronavirus. La chiave è nella proporzionalità, lungimiranza e ragionevolezza dell'intervento. Oltre che nella sua temporaneità.»

(Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali, "Agenda Digitale", 29 marzo 2020)

QUESTE DISPOSIZIONI NON VALGONO SOLO PER I PRIVATI CITTADINI

DOTT. STEFANO BACCHIOCCHI – Dottore Commercialista

ANCHE LE ISTITUZIONI NON SONO IMMUNI (ANZI!) DA PROBLEMI RELATIVI ALLA PRIVACY

UN ESEMPIO? LA VIOLAZIONE DATI DEL SITO INPS, IN OCCASIONE DEI FAMOSI 600 EURO

IL GARANTE: «Quella della mancanza di sicurezza delle banche dati e dei siti delle amministrazioni pubbliche è una questione che si ripropone costantemente, segno di una ancora insufficiente cultura della protezione dati nel nostro Paese».

COME APPLICARE LE NORMATIVE PRIVACY IN OCCASIONE DEI PROTOCOLLI DI SICUREZZA COVID-19

DOTT. STEFANO BACCHIOCCHI – Dottore Commercialista

INGRESSO IN STUDIO

COME COMPORTARCI NEI NOSTRI STUDI PROFESSIONALI?

CI SONO ALMENO 2 PIANI DIVERSI DI ANALISI:

1. La normativa privacy «generale».
2. La normativa privacy «particolare», dedicata al periodo dell'emergenza COVID-19.

INGRESSO IN STUDIO

<u>LA NORMATIVA PRIVACY «GENERALE»</u>
alla luce del GDPR e D.lgs 101/18

DOTT. STEFANO BACCHIOCCHI – Dottore Commercialista

PRINCIPIO DELLA 'PRIVACY *BY DESIGN*'

La 'privacy' ora incide anche sull'organizzazione della gerarchia aziendale e sulle modalità di lavoro.

Ad esempio: dovranno essere nominate figure di riferimento, designate per contratto, anche esternamente all'organizzazione.

L'ottemperanza alle norme dovrà essere costruita in MANIERA SARTORIALE.

(NO, non basta acquistare un software)

Con l'avvento del GDPR non esistono più schemi prestabiliti.

PRINCIPIO DELLA 'PRIVACY *BY DEFAULT*'

l'adeguamento alla normativa dovrà essere un'impostazione predefinita dell'organizzazione aziendale.

Ogni nuovo processo adottato, adempimento, attività svolta ecc. dovrà prevedere la protezione dei dati trattati e l'adeguamento alla normativa vigente di '*default*': si tratteranno solo i dati personali strettamente necessari per le finalità che si intendono perseguire, per il tempo minimo necessario.

Alcuni casi molto banali, per capire: cambio di ufficio o di arredamento, nuove assunzioni, imprese di pulizie, cambio di server, telefoni aziendali ecc.

ALTRI PRINCIPI CHIAVE

- NON ECCEDENZA, ADEGUATEZZA, PERTINENZA, MINIMIZZAZIONE, DATA RETENTION: bisogna ridurre al minimo l'uso di dati personali; devono essere pertinenti ed adeguati rispetto alle finalità perseguite; conservati per il tempo minimo necessario;
- LICEITÀ E CORRETTEZZA: il trattamento deve avvenire in maniera lecita e corretta informando i soggetti interessati circa la raccolta, l'utilizzo e la consultazione dei loro dati o ulteriori tipologie di trattamenti, ecc.
- TRASPARENZA: le informazioni e le comunicazioni devono essere facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro;

QUANDO UN TRATTAMENTO È LECITO?

- (nei casi previsti) è stato ottenuto il consenso dell'interessato;
- vi siano obblighi contrattuali;
- vi siano obblighi di legge cui è soggetto il titolare del trattamento;
- vi sia interesse pubblico o esercizio di pubblici poteri;
- vi sia interesse legittimo prevalente del Titolare o di terzi cui i dati vengono comunicati (sempre che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato).

A CHI SI APPLICA IL REGOLAMENTO:

A CHIUNQUE EFFETTUI UN TRATTAMENTO DEI DATI PERSONALI IN MANIERA NON DOMESTICA, nel territorio dell'Unione, con queste precisazioni:

- Si applica ai Titolari e ai Responsabili del trattamento stabiliti nell'Unione ed indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
- Si applica ai Titolari e ai Responsabili del trattamento non stabiliti nell'Unione che trattano dati di Interessati che si trovano nell'Unione, se le attività di trattamento riguardano:

1. offerta di beni o prestazione di servizi agli Interessati dell'Unione;
2. monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo nell'Unione.

QUANDO SI EFFETTUA UN «TRATTAMENTO»?

Il trattamento è una qualsiasi operazione (o insieme di operazioni) applicata ai dati personali.

ESEMPI:

la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, l'utilizzo, la comunicazione, la diffusione, la cancellazione ecc.

A QUALI DATI SI APPLICA LA NUOVA NORMATIVA?

Ad ogni informazione concernente una **PERSONA FISICA IDENTIFICATA** o identificabile («INTERESSATO», art. 4.1)

«Sono, pertanto, esclusi dall'ambito di applicazione delle disposizioni del regolamento i trattamenti dei dati relativi alle persone giuridiche: è evidente che in tal caso le disposizioni del GDPR troveranno applicazione con riferimento al trattamento dei dati personali del rappresentante legale.»

(cit. dal documento aprile 2018 Gruppo di Lavoro Privacy FNC)

A QUALI DATI SI APPLICA LA NUOVA NORMATIVA?
(CONTINUA)

Dati particolari (sensibili) (art. 9):

dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale.

VI È UN DIVIETO GENERALE di trattamento per questi dati ad eccezione di taluni casi espressamente elencati.

A QUALI DATI SI APPLICA LA NUOVA NORMATIVA?
(SEGUE)

ECCEZIONI AL DIVIETO:

- Quando c'è il **Consenso** dell'Interessato;
- Il trattamento è necessario per assolvere gli obblighi del titolare o per tutelare i diritti dell'interessato nel rapporto di lavoro;
- Il trattamento è necessario per tutelare un interesse vitale dell'Interessato;
- Il trattamento è necessario per accertare o difendere un diritto
- ecc.

A QUALI DATI SI APPLICA LA NUOVA NORMATIVA?

(SEGUE)

DATI PERSONALI RELATIVI A
CONDANNE PENALI E REATI (ART. 10):

Il trattamento deve avvenire soltanto sotto il controllo dell'autorità pubblica; oppure deve essere autorizzato dal diritto dell'Unione o degli Stati membri prevedendo garanzie appropriate per i diritti e le libertà degli interessati.

IL CONSENSO

Deve essere espresso mediante un atto inequivocabile con il quale l'interessato manifesta l'intenzione di accettare il trattamento dei dati personali.

Non è espressione del consenso il silenzio, l'inattività o la **preselezione di caselle**.

Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e neutrale.

LE FIGURE CHIAVE

IL TITOLARE DEL TRATTAMENTO:
(art. 24 GDPR)

«È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali»

IL CONTITOLARE DEL TRATTAMENTO (art. 26 GDPR)

«Laddove due o più titolari del trattamento decidano congiuntamente le finalità e i mezzi del trattamento»

I contitolari dovranno regolare i reciproci rapporti attraverso un accordo volto a stabilire i reciproci ruoli, il riparto degli obblighi, i rapporti reciproci nei rapporti con gli interessati.

Gli interessati, hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari che operano congiuntamente per far valere i propri diritti.

RESPONSABILE DEL TRATTAMENTO
(art. 28 GDPR)

«Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento».

Deve essere scelto dal Titolare **<u>TRA SOGGETTI CHE PRESENTINO GARANZIE SUFFICIENTI</u>** per mettere in atto misure tecniche e organizzative adeguate per garantire la sicurezza dei dati.

Deve essere nominato dal Titolare o da altro Responsabile previa autorizzazione scritta del Titolare.

La nomina dei responsabili «esterni» è obbligatoria, deve essere fatta per contratto.

COMPITI DEL RESPONSABILE DEL TRATTAMENTO

ESEMPI:

- tratta dati soltanto su istruzione documentata del titolare;
- consente i trattamenti solo a persone autorizzate
- adotta tutte le misure di sicurezza (es. cifratura; pseudonimizzazione; recupero da backup);
- rispetta le condizioni per ricorrere a un sub-responsabile del trattamento (vedi slide seguente);
- assiste il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- mette a disposizione del titolare le informazioni per dimostrare il rispetto degli obblighi.

I SUB-RESPONSABILI

Il responsabile può nominare sub-responsabili per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e «responsabile primario».

ATTENZIONE:

Il «responsabile primario» **risponde dinanzi al titolare dell'inadempimento del sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

I SOGGETTI AUTORIZZATI AL TRATTAMENTO

La nuova normativa non prevede espressamente la figura dell'«incaricato» del trattamento (come il vecchio Codice *ex* art. 30). Cita invece le "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (in particolare, art. 4, n. 10).

QUINDI:

L'AUTORIZZATO al trattamento è un soggetto che, agendo su incarico e sotto la diretta responsabilità del Titolare del trattamento (o del Responsabile), dopo essere stato **istruito e formato**, tratta dati personali.

ESEMPIO: dipendenti e collaboratori del Titolare

RESPONSABILE DELLA PROTEZIONE DEI DATI
(DPO)
(artt. 37, 38, 39 GDPR)

È UNA DELLE NOVITA' PIÙ IMPORTANTI

A questa figura sono demandati non solo compiti di controllo in ordine a livello di protezione dei dati all'interno della organizzazione del titolare, ma anche compiti di supporto strategico alle decisioni del Titolare in materia di trattamento dei dati.

SI PROFESSIONALIZZA LA 'PRIVACY'

DOTT. STEFANO BACCHIOCCHI – Dottore Commercialista

RESPONSABILE DELLA PROTEZIONE DEI DATI (SEGUE)

La nomina del DPO talvolta è obbligatoria:

- quando il trattamento è effettuato da una Autorità Pubblica, Pubblica Amministrazione (ESCLUSA l'autorità giudiziaria);
- quando vengono posti in essere trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- quando le attività principali del Titolare o del Responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati personali (dati relativi alla salute, dati genetici, dati biometrici, ecc.) o di dati relativi a condanne penali e a reati.

Il DPO può essere comunque nominato anche al di fuori dei casi appena citati (CONSIGLIATO!).

RESPONSABILE DELLA PROTEZIONE DEI DATI

(SEGUE)

REQUISITI:

- adeguata conoscenza della normativa, delle prassi di gestione dei dati personali e delle misure tecniche e organizzative per garantire la sicurezza dei dati;
- Indipendenza (!);
- Può essere interno od esterno all'organizzazione.

RESPONSABILE DELLA PROTEZIONE DEI DATI (SEGUE)

COSA FA: (PER LEGGE!)

- Sorveglia l'osservanza del Regolamento
- Collabora con il Titolare/Responsabile nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- informa e sensibilizza il Titolare nonché i dipendenti, riguardo agli obblighi «privacy»;
- Coopera con il Garante e funge da punto di contatto;
- Supporta il Titolare o il Responsabile in ogni attività connessa al trattamento dei dati (ES: registro dei trattamenti).

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (GARANTE PRIVACY)

- Il Collegio è costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato
- L'incarico di presidente e quello di componente hanno durata settennale e non sono rinnovabili.
- a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile; b) trattare i reclami; c) promuovere l'adozione di regole deontologiche; d) denunciare i fatti configurabili come reati perseguibili d'ufficio; e) trasmettere la relazione predisposta annualmente; f) cooperare con le altre autorità amministrative; g) adottare linee guida di indirizzo; h) limitare, sospendere o vietare i trattamenti in violazione delle norme; i) irrogare sanzioni correttive.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

(SEGUE)

Per le attivazioni ed i relativi riscontri operativi, il Garante attiva il Nucleo Speciale Privacy, quale reparto della Guardia di Finanza individuato per assicurare su tutto il territorio nazionale o previo interessamento del Reparto territorialmente competente gli adempimenti connessi all'attività di collaborazione.

LA DOCUMENTAZIONE E LE PRASSI

IL REGISTRO DEI TRATTAMENTI

L'obbligo di redigere il Registro riguarda i titolari o responsabili del trattamento con queste caratteristiche:

- chiunque effettui trattamenti che possano presentare un rischio, anche non elevato, per i diritti e le libertà dell'interessato;
- Chiunque effettui **trattamenti non occasionali**;
- Chiunque effettui trattamenti delle categorie particolari di dati o di dati personali relativi a condanne penali e a reati;
- Chiunque abbia almeno 250 dipendenti.

È quindi chiaro che sono obbligati a tenere e redigere il registro dei trattamenti dei dati personali buona parte di imprese e professionisti.

ANCHE I RESPONSABILI DEL TRATTAMENTO DEVONO TENERE IL REGISTRO

IL REGISTRO DEI TRATTAMENTI

Tale registro contiene almeno le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento, del contitolare, del rappresentante del titolare e del DPO;
- le finalità del trattamento;
- descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- i trasferimenti di dati verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
- i termini ultimi previsti per la cancellazione;
- una descrizione delle misure di sicurezza tecniche e organizzative.

IL REGISTRO DEI TRATTAMENTI
(SEGUE)

le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro possono beneficiare di alcune misure di semplificazione.

In tal caso l'obbligo di redazione del registro riguarderà soltanto le specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

Il Garante ha pubblicato l'8 ottobre 2018 due modelli relativi al registro semplificato per il responsabile del trattamento e per il titolare.

IL REGISTRO DEI TRATTAMENTI (SEGUE)

I registri sono tenuti in forma scritta, anche in formato elettronico.

Su richiesta, il titolare del trattamento o il responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

L'INFORMATIVA PRIVACY

Per ogni pratica, processo, adempimento ecc. che porti a trattare dati bisognerà informare l'interessato tramite la cd. «Informativa privacy»:

Consiglio sia in forma scritta, sintetica, chiara e leggibile; dovrà riportare i dati del titolare e l'indicazione dei responsabili del trattamento e, se nominato, i recapiti del DPO.

Dovrà riportare inoltre i diritti dell'interessato e le modalità per esercitarli.

Dovrà contenere inoltre le indicazioni di massima delle caratteristiche dei dati trattati, delle finalità, della base giuridica, delle modalità, degli eventuali trasferimenti, dei processi adottati per la sicurezza, del periodo di conservazione ecc.

IL CONSENSO

L'informativa ha anche lo scopo di permettere che l'interessato possa rendere un valido consenso, se richiesto come base giuridica del trattamento.

In questo caso l'informativa non è solo dovuta in base al principio di trasparenza e correttezza, ma è anche una **condizione di legittimità del consenso**.

I CONTRATTI DI NOMINA

DOVRANNO ESSERE ADOTTATI, ALMENO:

- nomina degli autorizzati;
- nomina dei responsabili;
- accordo tra contitolari;
- (eventuale) nomina DPO, con comunicazione al Garante.

PRINCIPALI NOVITÀ DEL D. LGS. 101/2018:

- CONSENSO DEI MINORI: a 14 anni si può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta di servizi della società dell'informazione. Il Regolamento prevede quale età minima 16 anni.
- MISURE DI GARANZIA PER IL TRATTAMENTO DEI DATI GENETICI, BIOMETRICI E RELATIVI ALLA SALUTE: il Garante dovrà stabilire le misure di garanzia per il trattamento dei dati genetici, biometrici, e relativi alla salute.
- TRATTAMENTO DI DATI RELATIVI A CONDANNE PENALI E REATI: l'art. 2 octies stabilisce i principi e le condizioni per il trattamento di detti dati.

PRINCIPALI NOVITÀ DEL D. LGS. 101/2018: (SEGUE)

- CONTROLLI A DISTANZA: viene fatta espressamente salva la disciplina dell'art. 4 Statuto dei Lavoratori, restando confermate le sanzioni penali in relazione alla violazione delle disposizioni di cui agli art. 4 e 8 della L. 300/1970.
- CURRICULUM VITAE: l'informativa privacy deve essere fornita al momento del primo contatto utile successivo all'invio del curriculum (art. 111 bis).
- SEMPLIFICAZIONE PER LE PMI: l'art. 154 bis, comma 4, del Codice Privacy prevede che il Garante, nel rispetto delle disposizioni del Regolamento e del codice stesso, promuova modalità semplificate di adempimento degli obblighi del titolare del trattamento per le PMI.

NUOVE PRASSI DA ADOTTARE

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura e del rischio per i diritti e le libertà delle persone fisiche, bisognerà porre in atto misure tecniche e organizzative adeguate, ad esempio:

- la pseudonimizzazione e la cifratura dei dati personali;
- backup tali da assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi;
- prassi volte a ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- bisognerà periodicamente testare l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

NUOVE PRASSI DA ADOTTARE

Software gestionali e le configurazioni di rete (es. firewall) dovranno garantire, ad esempio:

- la tracciabilità dei *log*, cioè gli accessi dovranno essere personali, monitorabili.
- che ogni utente (es. dipendente, collaboratore) possa vedere, trattare solo i dati per i quali è autorizzato.
- che tutti gli accessi da remoto avvengano da e per una rete sicura e cifrata.

NUOVE PRASSI DA ADOTTARE (SEGUE)

NON LIMITIAMOCI ALLA PARTE INFORMATICA, AD ESEMPIO:

- Gli uffici dovranno essere messi in sicurezza (per quanto possibile) da furti ed accessi non autorizzati.
- Gli armadi con i documenti cartacei non devono essere accessibili ai non autorizzati;
- Le scrivanie e gli schermi dovranno essere orientati correttamente;
- Gli uffici dovranno essere dotati di distruggidocumenti a norma;
- Anche i documenti cartacei andranno pseudonimizzati;
- Le fotocopiatrici, i fax e le stampati dovranno essere a norma;
- Anche le imprese di pulizie sono un rischio da calcolare.

L'ANALISI DEI RISCHI E LA DPIA

(*Data Protection Impact Assessment)*

Deve essere svolta nell'ambito della valutazione d'impatto sulla protezione dei dati (DPIA).

Cioè: una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento; una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; una **valutazione dei rischi** per i diritti e le libertà degli interessati; le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alla normativa vigente, tenuto conto dei diritti e degli interessi legittimi degli interessati.

LA GESTIONE DEI DATA BREACH

COSA È IL DATA BREACH:

«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 trasmessi, conservati o comunque trattati» (Art. 4).

La violazione, ad esempio, può essere determinata da accesso abusivo ai sistemi informatici, ovvero da sottrazione o perdita di dati e supporti di memorizzazione.

LA GESTIONE DEI DATA BREACH (SEGUE)

In generale, notificare entro 72 ore al Garante l'avvenuto data breach

TRANNE QUANDO sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche; se la probabilità del rischio per gli interessati è elevata, si dovrà informare delle violazioni anche gli interessati senza ingiustificato ritardo.

BISOGNERA' QUINDI:

- mettere in essere procedure standard per il rilevamento e la comunicazione dei data breach;
- valutare il rischio per i diritti e le libertà delle persone;
- tenere traccia delle violazioni e delle valutazioni effettuate;

LA FORMAZIONE

NON SI È OTTEMPERANTI ALLA NORMATIVA SE NON SI EFFETTUA LA CORRETTA FORMAZIONE, anche dei dipendenti e dei collaboratori

ATTENZIONE:

Come già ricordato, per la «nomina» dei responsabili e degli autorizzati al trattamento bisognerà verificare anche questo aspetto.

L'«ANTIVIRUS» DEL FATTORE UMANO È LA FORMAZIONE.

DOTT. STEFANO BACCHIOCCHI – Dottore Commercialista

INGRESSO IN STUDIO

LA NORMATIVA PRIVACY «PARTICOLARE»
COVID-19

DOTT. STEFANO BACCHIOCCHI – Dottore Commercialista

CONTRASTI NORMATIVI E BILANCIAMENTO DEI DIRITTI

- L'art 2087 c.c. e l'intero decreto legislativo n. 81/2008 impongono al datore di lavoro di tutelare l'integrità psico-fisica e la personalità morale dei prestatori di lavoro.
- Con l'art 5 dello Statuto dei Lavoratori da un lato si tenta di prevenire la realizzazione di condotte discriminatorie da parte datoriale e dall'altro garantire l'obiettività degli accertamenti medici.
- I protocolli anti COVID-19 prevedono segnalazioni alle autorità, rilevazione della temperatura, ecc.

CONTRASTI NORMATIVI E BILANCIAMENTO DEI DIRITTI

- **ARTICOLO 5 STATUTO LAVORATORI:**

«Sono vietati accertamenti da parte del datore di lavoro sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente.

Il controllo delle assenze per infermità può essere effettuato soltanto attraverso i servizi ispettivi degli istituti previdenziali competenti, i quali sono tenuti a compierlo quando il datore di lavoro lo richieda.

Il datore di lavoro ha facoltà di far controllare la idoneità fisica del lavoratore da parte di enti pubblici ed istituti specializzati di diritto pubblico.»

LA PROVA DELLA TEMPERATURA NEI PROTOCOLLI ANTI COVID-19
COME FARE

1. fornire l'informativa sul trattamento dei dati personali.
2. rilevare a temperatura e non registrare il dato acquisito.
3. è possibile identificare l'interessato e registrare il superamento della soglia di temperatura solo qualora sia necessario a documentare le ragioni che hanno impedito l'accesso ai locali aziendali;

LA PROVA DELLA TEMPERATURA NEL CONTENTUTO DELL'INFORMATIVA

1. Si ricorda che l'informativa può omettere le informazioni di cui l'interessato è già in possesso e può essere fornita anche oralmente.
2. Con riferimento alla finalità del trattamento potrà essere indicata la prevenzione dal contagio da COVID-19 e con riferimento alla base giuridica può essere indicata l'implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020 e con riferimento alla durata dell'eventuale conservazione dei dati si può far riferimento al termine dello stato d'emergenza;
3. la durata della conservazione del dato: deve essere conservato in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario allo scopo per il quale sono raccolti (es. durata stato di emergenza).

LA PROVA DELLA TEMPERATURA:
ALTRE MISURE ORGANIZZATIVE/BUROCRATICHE

1. definire le misure di sicurezza e organizzative adeguate a proteggere i dati. In particolare, sotto il profilo organizzativo, occorre individuare i soggetti preposti al trattamento e fornire loro le istruzioni necessarie.
2. i dati non devono essere diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali "contatti stretti di un lavoratore risultato positivo al COVID-19);
3. in caso di isolamento momentaneo dovuto al superamento della soglia di temperatura, assicurare modalità tali da garantire la riservatezza e la dignità del lavoratore. Tali garanzie devono essere assicurate anche nel caso in cui il lavoratore comunichi all'ufficio responsabile del personale di aver avuto, al di fuori del contesto aziendale, contatti con soggetti risultati positivi al COVID-19 e nel caso di allontanamento del lavoratore che durante l'attività lavorativa sviluppi febbre e sintomi di infezione respiratoria e dei suoi colleghi.

1. Il datore di lavoro può rilevare la temperatura corporea del personale dipendente o di utenti, fornitori, visitatori e clienti all'ingresso della propria sede?

Si, se i protocolli di sicurezza lo prevedono anche nei confronti di utenti, visitatori e clienti nonché dei fornitori; ad esempio ove per questi ultimi non sia stata predisposta una modalità di accesso separata.

In ragione del fatto che la rilevazione in tempo reale della temperatura corporea, quando è associata all'identità dell'interessato, costituisce un trattamento di dati personali, non è ammessa la registrazione del dato relativo alla temperatura corporea rilevata, bensì, nel rispetto del principio di "minimizzazione", è consentita la registrazione della sola circostanza del superamento della soglia stabilita dalla legge e comunque quando sia necessario documentare le ragioni che hanno impedito l'accesso al luogo di lavoro.

Diversamente nel caso in cui la temperatura corporea venga rilevata a clienti (ad esempio, nell'ambito della grande distribuzione) o visitatori occasionali anche qualora la temperatura risulti superiore alla soglia indicata nelle disposizioni emergenziali non è, di regola, necessario registrare il dato relativo al motivo del diniego di accesso.

2. Il datore di lavoro può richiedere ai propri dipendenti di rendere informazioni, anche mediante un'autodichiarazione, in merito all'eventuale esposizione al contagio da COVID-19 quale condizione per l'accesso alla sede di lavoro?

Il dipendente ha uno specifico obbligo di segnalare al datore di lavoro qualsiasi situazione di pericolo per la salute e la sicurezza sui luoghi di lavoro (art. 20 del d.lgs. 9 aprile 2008, n. 81). In tale quadro il datore di lavoro può invitare i propri dipendenti a fare, ove necessario, tali comunicazioni anche mediante canali dedicati.

Vi è la preclusione dell'accesso alla sede di lavoro a chi, negli ultimi 14 giorni, abbia avuto contatti con soggetti risultati positivi al COVID-19 o provenga da zone a rischio secondo le indicazioni dell'OMS. A tal fine, anche alla luce delle successive disposizioni emanate nell'ambito del contenimento del contagio, è possibile richiedere una dichiarazione che attesti tali circostanze anche a terzi (es. visitatori e utenti).

In ogni caso dovranno essere raccolti solo i dati necessari, adeguati e pertinenti rispetto alla prevenzione del contagio da Covid-19, e astenersi dal richiedere informazioni aggiuntive in merito alla persona risultata positiva, alle specifiche località visitate o altri dettagli relativi alla sfera privata.

3. Quali trattamenti di dati personali sul luogo di lavoro coinvolgono il medico competente?

In capo al medico competente permane il divieto di informare il datore di lavoro circa le specifiche patologie occorse ai lavoratori.

Nell'ambito dell'emergenza, il medico competente collabora con il datore di lavoro e le RLS/RLST al fine di proporre tutte le misure di regolamentazione legate al Covid-19 e, nello svolgimento dei propri compiti di sorveglianza sanitaria, segnala al datore di lavoro "situazioni di particolare fragilità e patologie attuali o pregresse dei dipendenti" (cfr. paragrafo 12 del predetto Protocollo).

Ciò significa che, nel rispetto della normativa privacy, il medico competente provvede a segnalare al datore di lavoro i casi specifici in cui reputi che la particolare condizione di fragilità connessa anche allo stato di salute del dipendente ne suggerisca l'impiego in ambiti meno esposti al rischio di infezione.

A tal fine, non è invece necessario comunicare al datore di lavoro la specifica patologia eventualmente sofferta dal lavoratore.

4. Il datore di lavoro può comunicare al Rappresentante dei lavoratori per la sicurezza l'identità dei dipendenti contagiati?

I datori di lavoro non possono comunicare il nome del dipendente o dei dipendenti che hanno contratto il virus a meno che il diritto nazionale lo consenta.

In base al quadro normativo nazionale il datore di lavoro deve comunicare i nominativi del personale contagiato alle autorità sanitarie competenti e collaborare con esse per l'individuazione dei "contatti stretti" al fine di consentire la tempestiva attivazione delle misure di profilassi.

Tale obbligo di comunicazione non è, invece, previsto in favore del Rappresentante dei lavoratori per la sicurezza, né i compiti sopra descritti rientrano, in base alle norme di settore, tra le specifiche attribuzioni di quest'ultimo.

Il Rappresentante dei lavoratori per la sicurezza, proprio nella fase dell'attuale emergenza epidemiologica, dovrà continuare a svolgere i propri compiti consultivi, di verifica e di coordinamento, offrendo la propria collaborazione al medico competente e al datore di lavoro (ad esempio, promuovendo l'individuazione delle misure di prevenzione più idonee a tutelare la salute dei lavoratori nello specifico contesto lavorativo; aggiornando il documento di valutazione dei rischi; verificando l'osservanza dei protocolli interni).

DOTT. STEFANO BACCHIOCCHI – Dottore Commercialista

5. Può essere resa nota l'identità del dipendente affetto da Covid-19 agli altri lavoratori da parte del datore di lavoro?

No! spetta alle autorità sanitarie competenti informare i "contatti stretti" del contagiato, al fine di attivare le previste misure di profilassi.

Il datore di lavoro è, invece, tenuto a fornire alle istituzioni competenti e alle autorità sanitarie le informazioni necessarie, affinché le stesse possano assolvere ai compiti e alle funzioni previste anche dalla normativa d'urgenza adottata in relazione alla predetta situazione emergenziale (cfr. paragrafo 12 del predetto Protocollo).

La comunicazione di informazioni relative alla salute, sia all'esterno che all'interno della struttura organizzativa di appartenenza del dipendente o collaboratore, può avvenire esclusivamente qualora ciò sia previsto da disposizioni normative o disposto dalle autorità competenti in base a poteri normativamente attribuiti (es. esclusivamente per finalità di prevenzione dal contagio da Covid-19 e in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali "contatti stretti di un lavoratore risultato positivo).

DOTT. STEFANO BACCHIOCCHI – Dottore Commercialista

GRAZIE PER L'ATTENZIONE!

Dott. Stefano Bacchiocchi
Dottore Commercialista in Brescia
Responsabile della Protezione dei Dati (DPO)

info@bacchiocchistudio.it
www.bacchiocchistudio.it