MTS CONSULENZE

EMERGENZA COVID-19

GESTIONE SALUTE E SICUREZZA SUI LUOGHI DI LAVORO

GESTIONE SMART WORKING

Riflessi in tema di trattamento dei dati personali

MTS CONSULENZE SRL
via Cuma, 2 00183 Roma - contatti@mtsconsulenze.it - tel. 06.72634465
capitale sociale € 10.000,00 i.v. - Iscrizione Registro imprese P.Iva e CF 15203041007

Sommario

1. Premessa

Il presente documento vuole essere una guida operativa per affrontare i riflessi sul piano della protezione dei dati personali conseguenti alle misure di contrasto alla diffusione del COVID-19.

Gli approfondimenti traggono spunto dalla normativa di emergenza che ha introdotto i presidi necessari per il contrasto alla pandemia, nonché dalla normativa in ambito trattamento e protezione dei dati personali[1].

Per facilità di lettura le tematiche sono trattate in modo schematico e diretto e sono inseriti link alla documentazione ritenutile utile per gli opportuni approfondimenti.
In ambito salute e sicurezza sul luogo di lavoro si invita ad approfondire la tematica con i propri consulenti ed il medico competente.

2. Salute e sicurezza, rilevazione dati e tematiche data Protection.

a. Introduzione

Come noto, Il 14 marzo 2020, le parti sociali hanno sottoscritto con il Governo *un protocollo di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro*.
Tale documento è stato integrato in data 24 aprile 2020. In analoga data sono stati adottati protocolli condivisi di regolamentazione per il contenimento della diffusione del COVID-19 nei settori dei cantieri, trasporti e logistica e trasporto pubblico[2].

I protocolli impattano sia su aspetti riferibili alla macro-tematica della salute di dipendenti, collaboratori, utenti e fornitori, sia su tematiche propriamente legate al trattamento di dati personali.

Occorre premettere, che il datore di lavoro, ai sensi art. 2087 del Codice civile e del Testo Unico della Sicurezza (D.lgs. 81/08), ha l'obbligo di garantire l'integrità fisica dei propri lavoratori ed un ambiente di lavoro salubre ed esente da rischi, tra cui sicuramente l'esposizione da rischio biologico. Tale aspetto può essere rilevante anche in relazione ai profili di responsabilità amministrativa da reato delle società e degli enti per come previsti dal D. Lgs. n. 231/2001.

[1] nel testo troverete i riferimenti agli atti e documenti ed anche dei link per raggiungere i testi ufficiali.
[2] Tutti i protocolli sono contenuti nel del Decreto 26 aprile 2020 il cui testo integrale è reperibile al link che segue: https://www.gazzettaufficiale.it/atto/vediMenuHTML;jsessionid=rjj4DliwBhOwdmxuyRNizg__.ntc-as5guri2b?atto.dataPubblicazioneGazzetta=2020-427&atto.codiceRedazionale=20A02352&tipoSerie=serie_generale&tipoVigenza=originario

In relazione a quanto attualmente indicato nei vari provvedimenti di contrasto alla diffusione del Covid-19, ma anche in relazione a quanto sarà in futuro indicato dalle autorità, è fondamentale il coinvolgimento e la fattiva sinergia con medico competente ed il servizio di prevenzione e protezione in quanto l'adozione di presidi di prevenzione e gestione di eventuali rischi è parte integrante del sistema di gestione della sicurezza in ambito lavorativo in ogni sua declinazione.

Gli aspetti e le circostanze che giustificano trattamenti in ambito "sanitario" devono essere individuati dal medico competente in quanto rientranti nella sua specifica funzione. In merito si suggerisce di confrontarsi anche con il proprio consulente in ambito salute e sicurezza sui luoghi di lavoro, nonché con il proprio Rspp e RLS al fine di condividere e definire protocolli di intervento adeguati.

Tali protocolli devono definire anche le azioni di gestione della rilevazione delle temperature corporee e quelle di gestione delle "temperature anomale" o dei soggetti che presentino sintomi correlabili alla patologia "Covid-19". In tale contesto devono essere stabilite anche le modalità di intervento e di raccolta di dati personali in base ai protocolli interni e a quelli sanitari emanati dalla autorità.

Anche la comunicazione da e per il medico competente deve essere effettuata in modo chiaro, tenendo conto di quanto già prevede la disciplina in tema di trattamento dati relativi allo stato di salute dei dipendenti. Si suggerisce, quindi, di implementare i processi in ambito salute e sicurezza sui luoghi di lavoro prevedendo anche un allegato al DVR che prenda in considerazione l'esposizione al virus quale agente patogeno.
In merito oltre agli approfondimenti che potranno essere forniti dai consulenti in materia di tematiche di cui al D.lgs. 81/08 segnaliamo il Documento tecnico sulla possibile rimodulazione delle misure di contenimento del contagio da SARS-CoV-2 nei luoghi di lavoro e strategie di prevenzione pubblicato sul sito dell'INAIL[3].

[3] Il documento è rinvenibile al seguente indirizzo internet: https://www.inail.it/cs/internet/comunicazione/pubblicazioni/catalogo-generale/pubbl-rimodulazione-contenimento-covid19-sicurezza-lavoro.html

b. Adempimenti specifici previsti dai protocolli condivisi in tema di ingresso in azienda e gestione di una persona sintomatica

(1) Il datore di lavoro informa preventivamente il personale, e chi intende fare ingresso in azienda, della preclusione dell'accesso 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. L'informazione è data tramite cartellonistica, avvisi affissi, e deve essere parimenti fornita l'informativa sul trattamento dati prevista dall'art 13 del Reg. UE 2016/679;

(2) l'ingresso in azienda di lavoratori già risultati positivi all'infezione da COVID -9 dovrà essere preceduto da una preventiva comunicazione avente ad oggetto la certificazione medica da cui risulti la "avvenuta negativizzazione" del tampone secondo le modalità previste e rilasciata dal dipartimento di prevenzione territoriale di competenza. La procedura di gestione di tale comunicazione deve essere definita e gestita con il Medico Competente;

(3) qualora, per prevenire l'attivazione di focolai epidemici, nelle aree maggiormente colpite dal virus, l'autorità sanitaria competente disponga misure aggiuntive specifiche, come ad esempio l'esecuzione del tampone per i lavoratori, il datore di lavoro dovrà fornire la massima collaborazione con le medesime autorità;

(4) in caso di lavoratori dipendenti di aziende terze operanti nello stesso sito produttivo (es. manutentori, fornitori, addetti alle pulizie o vigilanza) che risultassero positivi al tampone COVID-19, l'appaltatore dovrà informare immediatamente il committente ed entrambi dovranno collaborare con l'autorità sanitaria fornendo elementi utili all'individuazione di eventuali contatti stretti. La procedura di gestione di tale comunicazione deve essere definita e gestita con il Medico Competente;

(5) il lavoratore deve informare tempestivamente e responsabilmente il datore di lavoro della presenza di qualsiasi sintomo influenzale durante l'espletamento della prestazione lavorativa, avendo cura di rimanere ad adeguata distanza dalle persone presenti. In merito è opportuno che siano definiti gli adeguati canali di comunicazione da un lato per facilitare il Dipendente, dall'altro per garantire la riservatezza delle informazioni;

(6) l'acquisizione di dichiarazioni e la rilevazione in tempo reale della temperatura corporea costituiscono un trattamento di dati personali e, pertanto, devono avvenire ai sensi della disciplina privacy vigente (Regolamento Privacy UE 2016/679 – GDPR);

(7) il personale, i fornitori e gli addetti alle pulizie prima di accedere al luogo di lavoro potranno essere sottoposti al controllo della temperatura corporea. Se tale temperatura risulterà superiore ai 37,5° non sarà consentito l'accesso al luogo di lavoro.
Le persone in tale condizione saranno momentaneamente isolate e dotate di mascherine; non dovranno recarsi al Pronto Soccorso e/o nelle infermerie di sede, ma dovranno contattare nel più breve tempo possibile il proprio medico curante e seguire le sue indicazioni. Le misurazioni devono essere effettuate da personale autorizzato ed istruito, sia in tema di "tecniche" di misurazione sia in tema di protocolli da seguire e protezione dei dati personali;

(8) nel caso in cui una persona presente in azienda sviluppi febbre e sintomi di infezione respiratoria quali la tosse, deve immediatamente comunicarlo all'ufficio del personale. Si dovrà procedere all'isolamento di quest'ultimo, in base alle disposizioni dell'autorità sanitaria, e a quello degli altri presenti dai locali. L'azienda dovrà procedere immediatamente ad avvertire le autorità sanitarie competenti e i numeri di emergenza per il COVID-19 forniti dalla Regione o dal Ministero della Salute. Il lavoratore al momento dell'isolamento, deve essere subito dotato ove già non lo fosse, di mascherina chirurgica. Anche in questo caso occorre facilitare le procedure di comunicazione ed essere organizzati per gestire l'emergenza senza ledere la dignità del soggetto interessato, tutelandolo sia fisicamente sia nelle comunicazioni (non dovrà essere divulgato senza ragione nome e cognome del soggetto potenzialmente colpito dal Virus).

c. Adempimenti in materia di protezione di dati personali

L'emergenza sanitaria e gli adempimenti previsti a carico del datore di lavoro richiedono che il titolare del trattamento tratti i dati personali garantendo la maggior tutela degli interessati.
A tal fine si forniscono alcune indicazioni essenziali:

(1) occorre fornire adeguata informativa sul trattamento dei dati personali, anche esponendola all'ingresso della sede aziendale. In relazione 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, mentre con riferimento alla durata dell'eventuale conservazione dei dati si può far riferimento al termine dello stato d'emergenza. In merito si ribadisce che non devono essere registrati/conservati dati non necessari;

(2) Il soggetto incaricato di rilevare la temperatura corporea, se interno all'azienda e quindi sotto la responsabilità del Titolare del trattamento/Datore di lavoro, deve essere:

- dotato dei Dispositivi di Protezione Individuali previsti, come indicato nel documento integrativo alla valutazione dei rischi;
- istruito in merito alle misure di prevenzione da adottare, come indicato nel suddetto documento;
- istruito in merito alle modalità per la rilevazione della temperatura o di eventuali altri parametri fisiologici;
- nominato come "autorizzato al trattamento dei dati personali in relazione alle finalità del trattamento", ai sensi e per gli effetti di cui all'art. 29 e 32 del GDPR con specifiche istruzioni.

Nel caso di soggetto esterno, ovvero se appartiene ad un'altra Organizzazione questa deve essere nominata Responsabile del trattamento;

(3) I dati possono essere trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19 e 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"). In merito si ribadisce che non può essere resa nota l'identità del dipendente affetto da Covid-19 nemmeno agli altri lavoratori da parte del datore di lavoro. In sostanza è necessario prevedere delle procedure per la corretta gestione delle informazioni;

(4) è possibile identificare il dipendente e registrare il superamento della soglia di temperatura solo qualora sia necessario a documentare le ragioni che hanno impedito l'accesso ai locali aziendali. Si raccomanda di prestare attenzione a dove viene registrata la temperatura, avendo cura di definire tramite il medico competente quale procedura adottare (ad esempio una scheda cartacea da conservare dove? Sotto la custodia di chi? Con quali presidi per garantirne la riservatezza?).

Non devono essere realizzati sistemi che registrano le temperature di default, come si desume dai protocolli condivisi di regolamentazione per il contenimento della diffusione del COVID-19 sottoscritti il 24 aprile 2020. In merito si rammenta che il termine rilevare ha un significato differente da registrare e che se non serve conservare il dato non registrarlo è la soluzione che semplifica gli aspetti di gestione.

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;

(5) I datori di lavoro, nell'ambito dell'adozione delle misure di protezione e dei propri doveri in materia di sicurezza dei luoghi 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;

(6) In capo al medico competente permane, anche nell'emergenza, 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 Protocollo sottoscritto il 14 marzo ed aggiornato il 24 aprile). Ciò significa che, nel rispetto di quanto previsto dalle disposizioni di settore in materia di sorveglianza sanitaria e da quelle di protezione dei dati personali, il medico competente provvede a segnalare al datore di lavoro quei 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;

(7) occorre definire e adottare le misure di sicurezza procedurale, informatiche ed organizzative adeguate a proteggere i dati personali. In particolare, sotto il profilo organizzativo, occorre individuare i soggetti preposti al trattamento e fornire loro le istruzioni necessarie, definire adeguatamente le procedure di rilevazione e quelle per gestire eventuali anomalie tenendo in debita considerazione la dignità del soggetto interessato;

(8) è necessario assicurare modalità tali da garantire la riservatezza e la dignità del lavoratore (e di eventuali soggetti che devono essere isolati) in caso di isolamento momentaneo dovuto al superamento della soglia di temperatura. Tali garanzie devono essere assicurate anche nel caso in cui il lavoratore comunichi all'ufficio responsabile del personale o al referente di tale funzione 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;

(9) tra le misure di prevenzione e contenimento del contagio che i datori di lavoro devono adottare in base al quadro normativo vigente, 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.
Qualora si richieda ai propri dipendenti il rilascio di una dichiarazione attestante la non provenienza dalle zone a rischio epidemiologico e l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19, si ricorda che l'acquisizione di tale dichiarazione costituisce un trattamento dati e, pertanto, non devono essere richiesti dati ultronei rispetto all'esigenza di sicurezza (a titolo esemplificativo, perché sei andato in quel determinato luogo, etc.etc.). Alla luce delle successive disposizioni emanate nell'ambito del contenimento del contagio (v. Protocolli condivisi di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro fra il Governo e le parti sociali), è possibile richiedere una dichiarazione che attesti tali circostanze anche a terzi (es. visitatori e utenti). In merito si sottolinea che se si richiede una dichiarazione sui contatti con persone risultate positive al COVID-19, occorre astenersi dal richiedere informazioni aggiuntive in merito alla persona risultata positiva. Se si richiede una dichiarazione sulla provenienza da zone a rischio epidemiologico, è necessario astenersi dal richiedere informazioni aggiuntive in merito alle specificità dei luoghi.

(10) **occorre prestare la dovuta attenzione anche gli strumenti scelti per la rilevazione di dati personali e, in particolare, all'acquisto dei sistemi di rilevazione delle temperature corporee**. I tale contesto sistemi con riconoscimento biometrico, sistemi che interconnettono accessi e timbrature temporali, che conservano i dati sono rischiosissimi in tema trattamento dati personali.
Al fine di evitare l'acquisizione di strumenti con caratteristiche tecniche che non consentono di rispettare le norme in materia di protezione di dai personali è preferibile prediligere quelli utili alla misurazione della temperatura senza l'effettuazione di trattamenti ultronei.
Si segnala che in commercio sono presenti strumenti per la misurazione di diversa natura e caratterizzate da tecnologie diverse: strumenti di rilevazione "laser", termoscanner, strumenti legati a telecamere ad infrarossi o con tecnologie e sensori atti alla rilevazione della temperatura, sino a giungere a sistemi complessi ed evoluti che permettono riconoscimento biometrico del volto, l'interconnessione con i sistemi di rilevazione presenze, strumenti che riconoscono comportamenti (spostamento della mascherina o meno), sistemi che interconnettono videosorveglianza e sensori termici, e sistemi in

generale tecnologicamente evoluti. In merito si sottolinea che è necessario prestare attenzione a tutti quegli strumenti che, oltre alla temperatura, rilevino ulteriori dati ad esempio biometria dei volti o altri dati personali e che permettono di raggiungere anche altre finalità (ad esempio sostitutivi del badge presenze tramite riconoscimento biometrico), finendo per avere impatti rilevanti da un punto di vista privacy.
Non va, inoltre, sottovalutato il fatto che sistemi a "basso impatto" privacy hanno anche costi minori rispetto a sistemi particolarmente complessi ed evoluti.

(11) occorre considerare che eventuali sistemi complessi prevedono l'adozione di precise procedure privacy tra cui:
- analisi tecnica delle potenzialità dello strumento;
- valutazione della liceità e legittimità dei trattamenti complessi ultronei al precetto normativo;
- redazione di una Valutazione di impatto (DPIA) il cui risultato potrebbe anche prevedere il coinvolgimento dell'Autorità Garante;

(12) nella scelta degli strumenti per la rilevazione delle temperature corporee occorre valutare se gli impianti risultino anche potenzialmente idonei al controllo a distanza dell'attività lavorativa, tenendo conto di quanto stabilito dall'art. 4 della legge n. 300/1970 (Statuto dei lavoratori).

Per gli eventuali ulteriori approfondimenti ritenuti necessari si segnalano i seguenti riferimenti:

- Dichiarazione EDPB in tema di **trattamento dei dati personali nel contesto dell'epidemia di COVID-19** https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9295504

- Autorizzazioni generali trattamento dati aggiornate https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510

- Raccolta delle principali disposizioni adottate in relazione allo stato di emergenza epidemiologica da Covid-19 aventi implicazioni in materia di protezione dei dati personali (aggiornata al 9 aprile 2020) https://www.garanteprivacy.it/temi/coronavirus

3. Smart working

a. Introduzione

Il termine “lavoro agile” o meglio “smart working” indica un metodo di lavoro dinamico svolto dai dipendenti a distanza, all’esterno dei locali dell’azienda.

Tale definizione è stata introdotta dalla Legge n. 81 del 2017 fissando alcune regole sulle modalità e sugli ambiti di applicazione di tale tipologia di lavoro, caratterizzata da flessibilità organizzativa, dalla volontarietà delle parti che sottoscrivono un accordo individuale, nonché dall'utilizzo degli strumenti tecnologici (laptop, tablet etc..) che permettono al lavoratore di operare da remoto. L’esecuzione del rapporto di lavoro subordinato viene stabilita mediante l’accordo tra le parti, anche con forme di organizzazione per fasi, cicli ed obiettivi, senza vincoli di orario o di luogo di lavoro.

Attualmente, con il diffondersi dell'emergenza epidemiologica da COVID-19 (coronavirus), nell’ambito delle ulteriori misure adottate dal Governo per il contenimento e la gestione dell’emergenza da coronavirus, il Presidente del Consiglio dei ministri ha emanato il 1° marzo 2020 un nuovo decreto che interviene sulle modalità di accesso allo smart working, confermate dal Decreto 4 marzo 2020 e dal DPCM del 26 aprile 2020. Si tratta di una versione “semplificata” dello smart working, estesa per l’intera durata dello stato di emergenza, ad ogni tipo di lavoro subordinato su tutto il territorio nazionale, anche in assenza degli accordi individuali previsti dalla relativa normativa, al fine di evitare gli spostamenti e contenere i contagi.

Si segnala che lo smart working, attivato in questo momento di emergenza, non darà diritto a proseguire nel periodo successivo all’emergenza coronavirus con la medesima modalità, salvo diversi accordi/intendimenti che l’Organizzazione intenda assumere nei confronti del singolo lavoratore.

L’attivazione — pur nel rispetto delle doverose comunicazioni tra cui l’Inail — è più snella rispetto a quella, più rigida e macchinosa, prevista dagli artt. 18 e ss. della Legge 81/2017.

b. Adempimenti in materia di protezione di dati personali.

L’emergenza conseguente al diffondersi della pandemia di COVID-19 ha costretto, pertanto, a gestire in tempi ristrettissimi l’implementazione dell’attività lavorativa in modalità Smart working, non permettendo un’adeguata pianificazione che, invece, avrebbe dovuto essere effettuata nell’ambito di un corretto percorso di sviluppo ed organizzazione aziendale.

Ciò nonostante si sottolinea che lo smart working richiede un ponderato uso dell’innovazione digitale ed un’adeguata evoluzione dei modelli organizzativi aziendali, ivi compresi gli aspetti legati alla protezione dei dati personali.

A tal fine si forniscono alcune indicazioni essenziali:

(1) lo smart working rientra nel processo di trattamento dati riferibile al personale dipendente, conseguentemente devono essere adottate tutte le accortezze e prescrizioni normative ad esso correlate;

(2) è fondamentale la valutazione di strumenti, modalità procedurali operative e funzionalità tecniche che si intendono adottare e loro gestione anche in relazione alle prescrizioni contenute nell'art.4 della legge 300/1970 (statuto dei lavoratori).

Nel suggerire il coinvolgimento, su tale aspetto, del proprio consulente del lavoro/consulente legale giuslavorista, si rammenta che la disposizione normativa sopra richiamata prevede che gli strumenti di controllo a distanza, dai quali derivi anche la possibilità di controllo dei lavoratori, possono essere installati:

- esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale;
- ed esclusivamente previo accordo sindacale o, in assenza, previa autorizzazione della Direzione Territoriale del Lavoro o del Ministero.

La modifica all'articolo 4 dello Statuto, introdotta dall'art. 23 del D.lgs. n. 151/2015, attuativo della legge delega n. 183/2014 (c.d. "Jobs Act"), e dopo, dal D.lgs. n. 185/2016, contenente disposizioni integrative del D.lgs. n. 151/2015, chiarisce, poi, che non possono essere considerati "strumenti di controllo a distanza" gli strumenti che vengono assegnati al lavoratore "per rendere la prestazione lavorativa" (per meglio comprendere "attrezzi di lavoro"), come pc, tablet e cellulari.

L'accezione "per rendere la prestazione lavorativa" non deve essere interpretata in modo estensivo. Lo strumento viene considerato quale mezzo che "serve" al lavoratore solo quando strettamente ed inevitabilmente correlato all'adempimento della prestazione: ciò significa che nel momento in cui tale strumento viene modificato, integrato, o di fatto ha funzionalità ultronee (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio etc.etc.) che hanno la potenzialità di controllare il lavoratore, non integra più uno strumento per rendere la prestazione lavorativa, divenendo di fatto apparecchiatura (applicativo, hardware o software) che ha la potenzialità di controllo della prestazione a distanza;

(3) le attività in smart working impattano anche su altri soggetti interessati e non solo sui dipendenti (o clienti, fornitori…) e quindi la mancanza di procedure e misure di sicurezza adeguate può generare trattamenti non conformi anche per tali soggetti (perdita di dati, condivisione di informazioni con terzi non autorizzati…);

(4) per poter trovare un giusto equilibrio tra esigenza organizzativa aziendale e diritti degli interessati, oltre che in tema di presidi di sicurezza, si ritiene necessario effettuare una chiara e concreta analisi dei sistemi e dei processi posti in essere per garantire la fattibilità tecnica delle attività lavorative e realizzare una specifica valutazione del rischio (o aggiornare quella già effettuata) ed un DPIA;

(5) devono assolutamente essere prese in considerazione tematiche fondamentali tra cui si ricorda:

- la possibilità di utilizzare o meno strumenti personali e regolare e gestire il così detto BYOD (utilizzo di dispositivi e strumenti personali). Tale aspetto è delicatissimo perché può rappresentare un rischio notevole in tema di commistione di dati personali e lavorativi, in quanto al pc di casa possono avere accesso anche soggetti terzi rispetto al lavoratore autorizzato al trattamento (familiari, figli). Devono essere valutati anche i presidi di sicurezza implementabili su tali strumenti, la genuinità di sistemi operativi ed applicazioni, i sistemi di connessione alla rete (router, firewall) e di accesso da remoto ai sistemi aziendali;

- l'Implementazione di ulteriori misure di sicurezza relative alle nuove modalità di gestione delle attività lavorative che si rendono necessarie (crittografia dei device, antivirus, antispam, strumenti antintrusione, chiare politiche e strumenti per accesso, gestione ed archiviazione documenti);

- la predisposizione di un disciplinare che informi il dipendente delle misure di sicurezza che deve attivare e deve garantire.

Per gli eventuali ulteriori approfondimenti ritenuti necessari si segnalano i seguenti riferimenti:

- indicazioni e procedure previste in ambito giuslavoristico https://www.lavoro.gov.it/strumenti-e-servizi/smart-working/Pagine/default.aspx
- Controlli a distanza: Ministero del Lavoro, Comunicato stampa https://www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/20150618-Controlli-a-distanza.aspx
- DPIA - specifiche indicazioni dell'Autorità Garante per la protezione dei dati personali https://www.garanteprivacy.it/regolamentoue/DPIA

4. Aspetti essenziali per ogni trattamento

È necessario tener presente che:

a. ogni trattamento deve essere pensato e organizzato secondo i principi di privacy by design e privacy by default e cioè:
   - "data Protection by design" - è necessario configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati;
   - “data Protection by default” - è necessario che misure e presidi di sicurezza (tecnici, organizzativi, procedurali, operativi) siano applicati per impostazione predefinita;

b. deve essere aggiornata/effettuata la valutazione del rischio e la DPIA. In merito occorre ricordare che la valutazione del rischio non riguarda solo aspetti informatici ma deve prendere in considerazione i rischi su libertà e dignità di tutti i soggetti interessati oltre che garantire riservatezza integrità e disponibilità dei dati;

c. deve essere adeguatamente aggiornato il registro dei trattamenti sia in relazione a nuovi processi di trattamento che in relazione alle misure di sicurezza implementate. In merito occorre aver riguardo agli opportuni spunti di riflessione legati al registro dei trattamenti predisposti dall’Autorità Garante[4];

d. devono essere predisposti piani di formazione ed azioni comprovabili di istruzioni documentate per il personale aziendale;

e. occorre prestare particolare attenzione anche ai servizi forniti in cloud (riunioni virtuali ad esempio) al fine di valutare i riflessi in tema di protezione dei dati personali, come ad esempio il luogo di conservazione dei dati che potrebbe essere collocato anche in un paese extra UE.

[4] https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili#registro
“Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.”;

5. Coinvolgimento del Responsabile per la protezione dei dati

Si ricorda che la designazione del DPO, ove previsto, ed il suo coinvolgimento adeguato prima di realizzare dei trattamenti riflette l'approccio responsabilizzante che è proprio del GDPR essendo finalizzata a facilitarne l'attuazione da parte del titolare/del responsabile.

Costituisce, pertanto, elemento essenziale di accountability il coinvolgimento del DPO non a trattamenti avviati (c.d. a giochi fatti), ma precedentemente all'effettivo avvio di processi di trattamento: solo in questo modo sarà possibile sfruttare positivamente la funzione di "consiglio" e sensibilizzazione dello stesso e non solo la funzione di controllo ex post.

6. Check di primo livello

Al fine di consentire una verifica preliminare in modo autonomo dello stato di gestione delle due tematiche trattate si forniscono due specifiche check che, ancorché non esaustive o sostitutive di una consulenza specifica, possono essere strumenti di aiuto ed orientamento.

MISURA	SI	NO
ASPETTO SICUREZZA "COVID"		
Ho definito con Medico, Rspp, RLS, protocollo di sicurezza anti- contagio ed aggiornato il DVR? Tale protocollo prevede anche come comportarsi in caso di "positivi" e come gestire segnalazioni ed azioni concrete?		
Ho definito la gestione degli ingressi in azienda e che tipologia di azioni effettuerò anche in relazione ai dati personali? (solo rilevazione o registro? E se registro per quale ragione?		
I dati che tratto sono legati solo alla finalità di "gestione emergenza coronavirus"?		
Ho evitato di installare sistemi evoluti che trattano dati non necessari (biometria etc.etc.)?		
Se è stato previsto di registrare dei dati ho individuato la motivazione ed i tempi di cancellazione?		
Ho affisso informativa prima di rilevare la temperatura? Ho affisso cartellonistica con le regole di accesso alla sede?		
Ho individuato i soggetti autorizzati ad effettuare misurazione temperatura e trattamenti connessi alla gestione "prevenzione" contagi? Sono stati istruiti?		
In caso di appalti ho previsto i protocolli indicati nel dpcm del 26 aprile 2020?		
Ho previsto come gestire casi di "superamento soglia" temperatura?		
Ho aggiornato il registro dei trattamenti?		

MISURA	SI	NO
ASPETTO SMART WORKING		
Ho valutato che non ci siano strumenti “potenzialmente idonei al controllo dei lavoratori”?		
Ho fornito istruzioni ai dipendenti in relazione alle modalità di lavoro e comportamenti da tenere?		
Ho fornito informativa aggiornata (ove necessaria)?		
Ho valutato i rischi e adottato misure di sicurezza adeguate?		
Ho considerato se i lavoratori utilizzano strumenti personali o aziendali e regolato tale aspetto?		
Ho aggiornato di registro dei trattamenti?		
Ho verificato e regolato eventuali trattamenti su strumenti in paesi extra UE (sistemi di videoconferenza ad esempio)		

7. Alcuni degli errori più comuni

a. non considerare le azioni di prevenzione segnalate;
b. installare impianti complessi con trattamento di dati ultronei rispetto alle finalità previste dai vari decreti emessi durante la fase emergenziale;
c. non tenere in considerazione che la finalità perseguibile nel corso del trattamento dei dati nella fase emergenziale è soltanto quella di prevenzione del contagio e attuazione di protocolli sanitari;
d. non valutare preventivamente quanto proposto da fornitori tecnologici per verificare se le caratteristiche degli strumenti sono effettivamente adeguate alle esigenze derivanti dalla raccolta dei soli dati personali connessi alla gestione della fase emergenziale;
e. non tenere in considerazione che i dati non necessari da un lato possono rappresentare un illecito trattamento, dall’altro determinano anche costi aziendali maggiori per il loro trattamento (raccolta, salvataggio, manutenzione) e possono essere tra le altre cose inutilizzabili;
f. non considerare che trattamenti illeciti in ambito “gestione risorse umane” spesso hanno risvolti sia in ambito privacy sia in ambito giuslavoristico;
g. non definire adeguate regole di comportamento e non istruire il personale;
h. non aggiornare/effettuare una valutazione del rischio effettiva.

04.05.2020

MTS CONSULENZE SRL.