
Associazione Nazionale Commercialisti
FIRENZE

SINERGIA
RISK MANAGEMENT

# Vademecum legale per gestire l'emergenza Coronavirus

Smart Working - Privacy&DataProtection - Cybersecurity - Sicurezza sul lavoro - D.lgs. n. 231/2001

# Indice

# Introduzione

Il presente documento, redatto da ANC Firenze e Sinergia srl (società che opera nel settore della compliance aziendale, specializzata in Privacy e Data Protection, Sicurezza nei luoghi di Lavoro, Antiriciclaggio e d.lgs 231/2001), ha lo scopo di orientare il professionista nell'attuale contesto emergenziale.

Le misure di contenimento e prevenzione del Covid-19 introdotte dal dpcm 11 marzo 2020 e dal Protocollo condiviso dalle parti sociali il 14 marzo 2020 incidono sull'organizzazione lavorativa sotto il profilo della privacy&data protection, della cybersecurity, della sicurezza sui luoghi di lavoro e del d.lgs. 231/2001.

Questo vademecum, pertanto, si propone di supportare gli studi nella gestione delle problematiche aperte dal Decreto e dal Protocollo e relative allo smart working, al trattamento dei dati relativi alla salute di dipendenti e fornitori, ai modelli di organizzazione e gestione ed alla sicurezza nei luoghi di lavoro, suggerendo indicazioni e linee guida

# Smart Working

# Definizione

Il lavoro agile è una modalità di esecuzione del rapporto di lavoro subordinato che avviene in parte all'interno dell'impresa ed in parte all'esterno, disciplinato dal capo II, artt. 18-24, L. n. 81/2017, ed è definito quale "modalità flessibile di esecuzione del rapporto di lavoro subordinato allo scopo di incrementare la produttività e agevolare la conciliazione dei tempi di vita e di lavoro".

Le legge prevede una serie di requisiti per la sua instaurazione; tuttavia l'attuale situazione emergenziale ha portato il legislatore a semplificare l'accesso, proprio perché esso costituisce una misura idonea a prevenire la diffusione del Covid-19.

La novità più rilevante è l'assenza dell'accordo preventivo individuale scritto tra datore di lavoro e lavoratore (art. 7 del DPCM 11 marzo 2020).

# Smart Working

Nell'attuale contesto emergenziale, lo smart working costituisce una modalità di esecuzione del lavoro in grado di assicurare la **business continuity**.

La prestazione lavorativa, tuttavia, venendo eseguita dal dipendente al di fuori dell'azienda o dello studio (che sono ambienti "protetti"), espone i dati personali e aziendali del titolare a rischi rilevanti sotto il profilo della privacy e della cybersecurity.

# Privacy e Cybersecurity

Nello scenario in esame, l'imprenditore, ai sensi dell'art. 32 del Regolamento UE n. 679/2016 (GDPR), deve individuare:

- le misure di protezione adeguate per proteggere
  - i dati personali del lavoratore
  - il patrimonio aziendale;
- il contenuto del suo potere di controllo da esercitare sulle misure di protezione adottate.

Diventa necessario, quindi, per il datore comprendere esattamente i rischi operativi sottesi allo smart working.

# I Rischi Operativi

L'accesso remoto alla rete aziendale, attraverso strumenti di lavoro (ad esempio laptop, smartphone…) **forniti dal datore di lavoro o di proprietà del dipendente**, amplifica le **vulnerabilità dei sistemi** di protezione adottati e, quindi, estende la **superficie d'attacco** dei soggetti esterni.

L'**integrità** e la **disponibilità** dei dati e dei backup assieme alla **resilienza** dei sistemi devono, quindi, essere in ogni caso garantite a prescindere dallo strumento di lavoro utilizzato.

Vediamo, dunque, quali sono gli accorgimenti da adottare nel caso di utilizzo di uno strumento aziendale o personale per svolgere la prestazione lavorativa.

# Dotazioni aziendali

- Il datore deve fornire al dipendente i dispositivi di proprietà aziendale, predisposti per una funzionalità remota, con un livello di sicurezza determinato dal Responsabile IT, in accordo con l'eventuale DPO o con il consulente privacy.
- L'utilizzo di questi strumenti è soggetto alla policy aziendale sull'utilizzo delle risorse informatiche.
- Il lavoratore deve essere edotto circa le modalità di impiego delle stesse (ad esempio se sono utilizzabili solo per finalità legata all'esecuzione della prestazione di lavoro o possono essere utilizzati anche per fini personali) e le possibili modalità di controllo datoriale.

# Misure tecniche di sicurezza da adottare

Le misure di sicurezza da adottare dipendono da due fattori principali:

1) struttura IT dello studio o dell'impresa: la dislocazione e configurazione dei Server, dei database applicativi e software in uso, se client/server, cloud, service ecc…;

2) tipo di client utilizzato: in tal caso, dobbiamo verificare che sia configurato in compliance al GDPR, alle linee guida di settore ed al regolamento interno aziendale.

# Misure tecniche di sicurezza da adottare

Le misure da adottare sui client aziendali sono, quindi:

1) Sistema Antivirus, preferibilmente di tipo Managed
2) Password di accesso complessa (anche a due fattori), con avviso di cambiamento automatico ogni 3 mesi
3) Sistema di Firewall locale (sempre necessario quando il dispositivo esce dalla rete aziendale o comunque entra in una rete priva di Firewall perimetrale)
4) Utente di utilizzo privo di diritti di amministrazione del client
5) Elenco degli applicativi limitato e soggetto a controllo e revisione
6) Protezione della postazione dopo 5 minuti di inutilizzo
7) Aggiornamento automatico del sistema operativo attivato
8) Sistema di Backup su supporto cifrato o cloud
9) Nel caso di cloud backup, sistema di accesso a doppia autenticazione (es. Pwd + sms)
10) Cifratura del disco o di cartelle locali di lavoro
11) Divieto di installare applicazioni non approvate dal datore

# Collegamento sicuro alla rete aziendale

L'utilizzo del dispositivo aziendale in uso allo smart worker, configurato con le misure viste in precedenza, necessita di accorgimenti aggiuntivi per rendere sicuro l'accesso da remoto al perimetro aziendale dalla rete domestica, consistenti nell'adozione di:

1) VPN per il collegamento del dispositivo alla rete aziendale
2) firewall software locale per protegge il dispositivo quando sconnesso dalla VPN

La configurazione di queste misure permette al client di essere proiettato in maniera sicura sulla rete aziendale e di operare su applicativi intranet dello studio, come ad esempio TeamSystem Polyedro.
Nel caso lo smart worker necessiti di utilizzare applicativi client server (es. TeamSystem Gamma, CGN, ecc…) dovrà essere predisposta una connessione RDP sempre su canale VPN su un client o server dedicato.

# Client personale dello smart worker

Quando il dispositivo utilizzato è **di proprietà** dello smart worker, il datore di lavoro non ha il potere di imporre direttamente le misure di sicurezza viste in precedenza.

Dunque, per rendere sicuro il dispositivo personale occorre dotarsi di una policy **BYOD**-Bring Your Own Device (traducibile "utilizza il tuo dispositivo personale") che il lavoratore deve sottoscrivere e che, oltre all'adozione di tutti gli accorgimenti prima indicati, deve prevedere in sintesi:

- la regolamentazione dei controlli casuali a campione della configurazione dei dispositivi mobili per garantire la loro conformità alla policy BYOD medesima;
- il divieto di memorizzare i dati aziendali o dello studio in applicazioni non approvate dal datore sul dispositivo mobile;
- la distinzione dei dati di lavoro da quelli privati;
- il collegamento di dispositivi mobili (pen-drive, hdd-esterno, etc) solo di provenienza sicura;
- la comunicazione al datore ogni tipo di violazione dei dati che il dispositivo dovesse subire.

# Sistemi Sandboxes di isolamento

Una misura di sicurezza che è possibile utilizzare in questo contesto è rappresentata dai sistemi di isolamento, come ad esempio il Sandbox ( Windows 10 Pro ne ha integrato uno ma ne esistono anche free per chi ha la versione Home) o un sistema con macchina virtuale.

Un Sandbox è un sistema pulito, delimitato e logicamente separato dal dispositivo che lo ospita.
Una volta creato il sistema isolato possiamo proteggere l'interazione fra il sistema fisico (ad es. il notebook del dipendente) ed il nostro nuovo sistema isolato.
Per proteggere l'interazione basterà mettere in sicurezza il flusso dei dati e la memoria operativa (es. con la cifratura della memoria virtuale e della tastiera con un Anti-Keylogger).
Protetta l'interazione, basterà applicare al sistema isolato viste in precedenza ed avremo quindi un sistema sicuro di lavoro separato dai programmi e dai dati personali del dipendente.

**Ricordiamo che queste sono indicazioni generali: il progetto di messa in sicurezza deve essere sempre fatto da un tecnico esperto previa analisi dell'intera infrastruttura.**

# Misure di sicurezza organizzative

- Regolamento sullo smart working;
- formazione dei dipendenti sui rischi inerenti lo smart working;
- previsione di una figura di coordinamento per tutti i lavoratori che operano da remoto.

# Poteri di controllo del datore di lavoro

Ciascun datore ha il diritto-dovere di svolgere controlli sul corretto svolgimento della prestazione dei propri dipendenti, senza distinzioni sulle modalità di esecuzione e - quindi - anche nel contesto dello smart working, a patto che siano rispettati i limiti fissati dagli artt. 2,3 e 4 dello Statuto dei Lavoratori (L. 300/1970).

I dati acquisiti con strumenti che - potenzialmente - possono configurare un controllo a distanza del dipendente sono utilizzabili se:

- è stata fornita una policy aziendale che disciplina le modalità d'uso degli strumenti e l'effettuazione dei controlli;
- viene rispettata la normativa sul trattamento dei dati personali, in primo luogo mediante consegna dell'informativa ex art 13 del GDPR, esaustiva di tutti i trattamenti di dati del lavoratore.

Nello scenario in esame, la dotazione di un SIEM costituisce un mezzo efficace per esercitare il potere di controllo datoriale.

# Smart Working e
# Sicurezza sul Luogo di Lavoro

# Smart Working e Sicurezza sul Luogo di Lavoro

Premessa: “Le misure di contenimento del Virus se rimarranno sulla carta, non raggiungeranno nessun obiettivo”.

L’attuale contesto emergenziale non intacca le prescrizioni sulla sicurezza e la salute dei dipendenti. L’art. 22 dell Legge n°81/2017 sul lavoro agile ne è l’esempio: “Il datore di lavoro garantisce la salute e la sicurezza del lavoratore”.

L’emergenza, proprio nell’ottica di contenimento e prevenzione della diffusione del Covid-19, esige un rispetto puntuale delle norme a tutela della salute e sicurezza nei luoghi di lavoro primo tra tutti, ma non solo, il d.lgs. 81/08.

Questo obiettivo è perseguibile solo coinvolgendo il tessuto datoriale per le scelte operative.

Al riguardo, il Protocollo per la lotta al virus condiviso dalle parti sociali del 14/03/2020 costituisce un elemento utile e prezioso, il cui contenuto deve essere proceduralizzato in ogni singola realtà lavorativa.

# Smart Working e Sicurezza sul Luogo di Lavoro

L'esecuzione della prestazione da remoto, quindi, non esonera il datore di lavoro dal rispetto delle prescrizioni indicate dal d.lgs. n. 81/08. **Risulta necessario in via generale**:

- effettuare la valutazione dei rischi incidenti sulla nuova modalità di lavoro, in particolare sugli strumenti forniti dal datore;
- formare i lavoratori e il vertice della struttura aziendale;
- controllare il rispetto delle norme di sicurezza (nel limite della ragionevolezza imposta dal caso concreto).

Facciamo notare che dall'art 173 Dlgs 81/08 deriva l'obbligo di nominare il medico competente del lavoro peri rischi da videoterminale (smart working).

# Principio Generale

L'ambiente di lavoro per l'esecuzione della prestazione in smart working deve essere individuato in locali privi di pericoli per la salute e sicurezza dei collaboratori/dipendenti.

In via generale, il dipendente svolge la prestazione presso il proprio/a domicilio/dimora/residenza abituale nel rispetto delle disposizioni contenute nell'art. 20 del d.lgs. 81/2008 e secondo indicazioni ispirate al criterio della ragionevolezza.

# Indicazioni Generali

**1**. L'attività non può essere svolta in locali tecnici o in locali non abitabili (ad es. soffitte, seminterrati, rustici, box).

**2**. Vi deve essere un'adeguata disponibilità di servizi igienici e acqua potabile e presenza di impianti a norma.

**3**. Le superfici interne delle pareti non devono presentare tracce di condensazione permanente (muffe).

**4**. Devono essere collocate le lampade in modo tale da evitare abbagliamenti diretti e/o riflessi e la proiezione di ombre che ostacolino il compito visivo mentre viene svolta l'attività lavorativa.

**5**. Deve esserci il ricambio dell'aria naturale o con ventilazione meccanica.

**6**. I locali debbono fruire di illuminazione naturale diretta, adeguata alla destinazione d'usi e devono altresì essere muniti di impianti d'illuminazione artificiale, generale e localizzata.

# Requisiti delle abitazioni

1. Abitabilità
2. Conformità degli impianti
3. Spazio sufficiente ed idoneo
4. Temperatura adeguata allo svolgimento della prestazione
5. Luminosità il più possibile naturale
6. Seduta con postura idonea

# Impiego corretto di tablet, smartphone e pc

1. Frequenti pause
2. Evitare di scrivere lunghi testi
3. Utilizzo di auricolari per il cellulare
4. Non tenere il volume su livelli elevati

# La sicurezza dei dipendenti in azienda

# Protocollo condiviso di regolamentazione delle misure per il contrasto ed il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro

## PRECAUZIONI IGIENICHE PERSONALI

- lavaggio delle mani;
- obbligo per il datore di dotarsi di mezzi detergenti;
- preparazione da parte dell'azienda del liquido detergente secondo le indicazioni dell'OMS;
- raccomandare pulizia frequente delle mani.

# DISPOSITIVI DI PROTEZIONE PERSONALI

- dotarsi di mascherine conformi alle indicazioni dell'Organizzazione mondiale della sanità;
- in caso di difficoltà di approvvigionamento, dotarsi di mascherine corrispondenti alle indicazioni dell'autorità sanitaria;
- qualora il lavoro impone di lavorare a distanza interpersonale minore di un metro e non siano possibili altre soluzioni organizzative, utilizzare - oltre alle mascherine - altri dispositivi di protezione (guanti, occhiali, tute, cuffie, camici, ecc…) conformi alle disposizioni delle autorità scientifiche e sanitarie.

# GESTIONE DEGLI SPAZI COMUNI

- contingentamento dell'accesso agli spazi comuni (area fumatori, mensa..);
- ventilazione degli spazi;
- predeterminazione di un tempo di sosta all'interno dell'area;
- mantenimento della distanza di un metro;
- sanificazione periodica e pulizia giornaliera degli spazi comuni.

# SPOSTAMENTI INTERNI, RIUNIONI, EVENTI INTERNI E FORMAZIONE

- limitare gli spostamenti interni al minimo indispensabile;
- vietare le riunione, salvo che non siano necessarie ed urgenti, garantendo comunque il rispetto della distanza di un metro tra i partecipanti e l'aerazione e pulizia del locale;
- sospendere le attività formative, anche obbligatorie, in aula. Ove possibile, incentivare la formazione a distanza.

# GESTIONE DI UNA PERSONA SINTOMATICA SUL LUOGO DI LAVORO

- nel caso in cui una persona presenti sintomi di infezione respiratoria, procedere al suo isolamento;
- avvertire immediatamente le autorità sanitarie competenti e i numeri di emergenza per il COVID-19 forniti dalla Regione o dal Ministero della Salute;
- collaborare con l'autorità per la ricostruzione della "filiera", in caso di esito positivo del tampone;
- sospendere le attività formative, anche obbligatorie, in aula. Ove possibile, incentivare la formazione a distanza.

# SORVEGLIANZA SANITARIA E MEDICO COMPETENTE

- evitare di interrompere la sorveglianza sanitaria periodica: essa rappresenta una ulteriore misura di prevenzione di carattere generale, perché può intercettare possibili casi e sintomi sospetti del contagio ed ha la funzione di informare e formare i lavoratori sui comportamenti idonei ad evitare la diffusione del contagio;
- integrare e proporre tutte le misure di regolamentazione legate al Covid-19 con il medico competente e le RLS/RLST;
- costituire il comitato per l'applicazione e la verifica delle regole del protocollo di regolamentazione con la partecipazione delle rappresentanze sindacali aziendali e del RLS.

# Ordinanza del Presidente della Giunta Regionale Toscana n. 38 del 18 aprile 2020...

**Ambito**

Le misure di contenimento previste nell'ordinanza valgono per tutti gli ambienti di lavoro esclusi quelli sanitari, i cantieri e le aziende di tutti i servizi pubblici locali, che hanno sempre assicurato lo svolgimento dei servizi applicando il Protocollo condiviso del 14 marzo 2020.

**Monitoraggio della siero prevalenza**

Il datore deve garantire spazi e informazioni ai dipendenti e collaboratori che intendano volontariamente sottoporsi allo screening sierologico.

# ...Ordinanza del Presidente della Giunta Regionale Toscana n. 38 del 18 aprile 2020...

**Gestione degli spazi e delle procedure di lavoro**

- uso della mascherina, dei guanti protettivi monouso e pulizia/sanificazione delle mani prima e dopo l'utilizzo degli stessi per lo spostamento dal domicilio al posto di lavoro e viceversa;
- distanza interpersonale di 1,8 metri. Ove non sia possibile nonostante la riorganizzazione dei processi produttivi, occorre dotare il lavoratore mascherine FFP2 senza valvola per gli operatori che lavorano nello stesso ambiente. Qualora le mascherine FFP2 non fossero reperibili è sufficiente utilizzare contemporaneamente due mascherine chirurgiche;
- uso della mascherina obbligatorio in spazi chiusi ed in ambienti aperti ove non è garantito il rispetto della distanza interpersonale;
- verifica quotidiana del datore di lavoro, all'inizio di ogni turno, della presenza dei sintomi del Covid-19, anche mediante autocertificazione del dipendente;

# ...Ordinanza del Presidente della Giunta Regionale Toscana n. 38 del 18 aprile 2020...

- fornitura ai dipendenti di idonei mezzi detergenti per le mani, mascherine protettive e guanti monouso per tutte le fasi lavorative - controllo del rispetto di tali prescrizioni;
- sanificazione degli ambienti con frequenza giornaliera e in funzione dei turni di lavoro, ricambio dell'aria;
- sanificazione eseguita secondo i requisiti dell'ordinanza e registrata su supporto cartaceo o informatico con autodichiarazione;
- sanificazione periodica degli impianti di areazione, secondo le indicazioni contenute nel "Rapporto ISS COVID-19 n. 5/2020. Indicazioni ad interim per la prevenzione e gestione degli ambienti indoor in relazione alla trasmissione dell'infezione da virus SARS-CoV-2.", o spegnimento, garantendo la massima ventilazione dei locali;
- servizio mensa organizzato in modo da garantire la distanza interpersonale e sanificazione dei tavoli dopo ogni singolo pasto;
- obbligo di informare efficacemente sulle presenti disposizioni.

# ...Ordinanza del Presidente della Giunta Regionale Toscana n. 38 del 18 aprile 2020...

**Obblighi per esercizi commerciali**

- Previsione di accessi regolamentati e scaglionati dell'utenza per garantire la distanza interpersonale di almeno 1,8 metri (in caso di spazi fino a 40 mq. l'accesso è consentito uno alla volta);
- differenziare, ove possibile, i percorsi di entrata e di uscita;
- posizionamento di pannelli di separazione tra i lavoratori e l'utenza;
- consentire l'accesso solo a chi indossa mascherina protettiva, che copra naso e bocca, e dopo sanificazione delle mani e aver indossato guanti monouso; predisporre dispenser con liquido per la disinfezione delle mani e guanti monouso all'ingresso del negozio;
- predisposizione degli avvisi sul mantenimento del rispetto della distanza interpersonale prescritta;
- consentire l'ingresso ad una sola persona per nucleo familiare;
- posizionamento presso la zona di prelievo dei carrelli e cestelli, dispenser con liquido disinfettante e carta assorbente per il cliente.

# ...Ordinanza del Presidente della Giunta Regionale Toscana n. 38 del 18 aprile 2020

**Protocollo Anti-contagio**

- Obbligo di redigere un protocollo di sicurezza anti-contagio che preveda l'impegno all'attuazione delle misure indicate nell'ordinanza per garantire la sicurezza e la tutela della salute e dei lavoratori;
- per le imprese aperte, trasmissione del protocollo alla mail protocolloanticontagio@regione.toscana.it entro 30 giorni dalla pubblicazione dell'ordinanza; per le altre attività la trasmissione del protocollo entro 30 giorni dalla riapertura.
-

# Il controllo delle misure di sicurezza

# Circolare del Ministero dell'Interno del 14 aprile 2020

Corpo Guardia di Finanza:

- verifica la veridicità del contenuto delle comunicazioni prodotte dalle aziende; in pratica, controllerà che nelle fabbriche aperte si lavori effettivamente alla produzione di beni delle categorie autorizzate o comunque appartenenti alle varie filiere consentite.

Ispettorato del Lavoro:

- controllo sulle modalità di attuazione, da parte dei datori di lavoro, delle procedure organizzative e gestionali oggetto del Protocollo Governo-parti sociali del 14 marzo 2020, e, più in generale, sull'osservanza delle precauzioni dettate per la messa in sicurezza dei luoghi di lavoro e la sussistenza di adeguati livelli di protezione dei lavoratori (sanificazione, distanziamento sociale, prodotti igienizzanti e uso dei dispositivi di protezione individuale).

# La rilevazione della temperatura corporea

# Protocollo condiviso di regolamentazione delle misure per il contrasto ed il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro

Il personale **può essere sottoposto a misurazione della temperatura corporea** purché il datore di lavoro abbia definito ed implementato tutte le misure di sicurezza tecniche ed organizzative previste dalla normativa sul trattamento e la protezione dei dati personali.

Il trattamento descritto ha ad oggetto un dato "particolare" (ex dato sensibile) ai sensi dell'art. 9 del GDPR, per cui devono essere rispettati determinati principi a garanzia dei diritti e delle libertà dei soggetti interessati.

**N.B.: “è possibile”, non “si deve”.**

La misurazione della temperatura corporea è un trattamento invasivo, adottabile quando è ritenuto strettamente necessario. Il datore di lavoro è, quindi, tenuto ad effettuare una valutazione in termini di “necessità del trattamento” e documentare il motivo per cui ha ritenuto che quella misura fosse indispensabile e necessaria.

# Principi di necessità e proporzionalità

L'impresa che decide di rilevare la temperatura:

- può registrare il dato
- ed identificare l'interessato
- solo nell'eventualità in cui sia necessario documentare le ragioni che hanno impedito l'accesso ai locali aziendali.

Il trattamento deve essere effettuato garantendo la **massima riservatezza e dignità** del dipendente:

- garantire che nessun dipendente possa assistere all'operazione;
- adeguata protezione delle informazioni rilevate;
- astenersi dal richiedere informazioni aggiuntive in merito alla persona risultata positiva.

Il trattamento descritto deve essere eseguito, di regola, dal **medico del lavoro**.

Qualora non sia possibile (ad esempio, impresa non obbligata alla nomina), i soggetti che procederanno all'operazione devono sottoscrivere l'**autorizzazione al trattamento** prevista dall'art. 29 GDPR che contenga:

- un impegno alla riservatezza;
- istruzioni specifiche per impedire che i dati vengano visualizzati da soggetti non autorizzati, diffusi o altrimenti divulgati.

# Divulgazione della rilevazione

La divulgazione della rilevazione è ammessa solo:

- per le **finalità previste dalle disposizioni di legge** (es. richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali "contatti stretti" di un lavoratore risultato positivo al COVID-19);
- qualora occorra indicare il nome del dipendente o dei dipendenti che hanno contratto il virus per **finalità di prevenzione**: in tal caso i dipendenti interessati devono essere informati in anticipo di tale trattamento (Comitato europeo per la protezione dei dati - EDPB Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19 Adottata il 19 marzo 2020).

La divulgazione di queste informazioni deve avvenire su canali sicuri.

# Comunicazione dei dati sanitari del dipendente affetto da Covid-19 agli altri colleghi

**Condizioni di ammissibilità - lettura orientata dell'art. 14 II° comma del d.l. n. 14/2020**

- la **comunicazione** dei dati sanitari è ammessa quando risulta indispensabile per lo svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto;
- rispetto dei principi di necessità e proporzionalità ex art. 5 GDPR;
- adozione di misure adeguate per tutelare l'interessato.

In questo caso, il trattamento ha un fondamento giuridico di tipo lavoristico, ravvisabile nell'art. 2087 c.c. piuttosto che nelle norme relative alla data protection.

# Informativa sul trattamento dei dati personali

Prima della rilevazione della temperatura, dovrà essere resa al dipendente l'informativa sul trattamento dei dati personali ai sensi dell'art. 13 GDPR, che potrà essere fornita oralmente o appesa nei locali in cui viene rilevata la temperatura.

# Contenuto dell'informativa

**Finalità**: prevenzione del contagio da COVID-19.

**Base giuridica**: secondo l'EDPB, art. 9.2 lett. i - motivi di interesse pubblico rilevante nel settore della sanità pubblica; art. 9.2 lett. c - necessità di proteggere gli interessi vitali dell'interessato (vd. Considerando 46 GDPR). Per il Protocollo, art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020 (implementazione dei protocolli di sicurezza anti-contagio). No consenso.

**Periodo di conservazione**: fino al perseguimento delle finalità (es. isolamento del lavoratore, ricostruzione della filiera dei contatti) e al massimo fino al termine dello stato d'emergenza (solo qualora si renda necessaria la conservazione delle informazioni rilevate).

# Autocertificazione

# Protocollo condiviso di regolamentazione delle misure per il contrasto ed il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro

L'imprenditore può richiedere al dipendente una dichiarazione che attesti:

- la non provenienza dalle zone a rischio epidemiologico e
- l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19.

Ulteriori informazioni non possono essere richieste in quanto violano i principi di necessità e proporzionalità previsti dal GDPR.

Per questo trattamento valgono le medesime regole individuate per il trattamento precedente.

# Gestione dei rapporti con i fornitori

# Comunicare e Richiedere

L'imprenditore **deve**:

- comunicare che l'accesso in azienda è precluso a chi, negli ultimi 14 giorni, ha avuto contatti con soggetti risultati positivi al COVID-19 o proviene da zone a rischio secondo le indicazioni dell'OMS.

L'imprenditore **può**:

- richiedere 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.

# Il trattamento dei dati

Le operazioni di trattamento sui dati personali dei fornitori devono rispettare le medesime garanzie ed indicazioni viste per i dipendenti

# La responsabilità ai sensi del d.lgs. n. 231/2001

Il DPCM 11 marzo 2020 ed il Protocollo condiviso di regolamentazione delle misure per il contrasto ed il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro introducono delle prescrizioni in tema di sicurezza e salute sui luoghi di lavoro dirette a scongiurare le conseguenze pregiudizievoli della permanenza in azienda o nello studio.

Inoltre, l'instaurazione dello smart working, oltre alle problematiche già affrontate, comporta l'emersione di rischi anche sotto il profilo dei reati informatici.

Risulta evidente che il datore di lavoro è esposto a conseguenze pregiudizievoli (civili-risarcitorie o addirittura penali) nel caso di contagi da Covid-19 avvenuti in occasione dello svolgimento delle prestazioni lavorative o di violazioni del sistema o dei dei dati.

Di conseguenza, si può configurare, a seconda dei caso, una responsabilità dell'ente datoriale ai sensi del d.lgs. n. 231/2001.

La prevenzione di questi rischi passa attraverso i seguenti accorgimenti:

- valutare l'adempimento degli obblighi previsti dal d.lgs. 81/2008 alla luce del DPCM 11 marzo 2020 e del Protocollo sottoscritto dalle parti sociali con il Responsabile del Servizio Prevenzione e Protezione (RSPP);
- aggiornamento del documento di valutazione dei rischi (DVR);
- aggiornarnamento del modello di organizzazione, gestione e controllo dei rischi sia sotto il profilo della responsabilità in tema di salute e sicurezza sul luogo di lavoro che sotto il profilo dei reati informatici.

# Informazioni

Per chiarimenti e informazioni sulle tematiche affrontate in questo documento è possibile contattare l'ANC Firenze all'indirizzo di posta elettronica segretario@ancfirenze.it o al numero **800.962.967**