



LECIS CANNELLA GRASSI  
STUDIO LEGALE ASSOCIATO

**WEBINAR, 11 MAGGIO 2020**

***LE IMPRESE ALL'ALBA DELLA FASE 2:  
SPUNTI PER UNA GESTIONE  
CONSAPEVOLE DEI RISCHI***

---

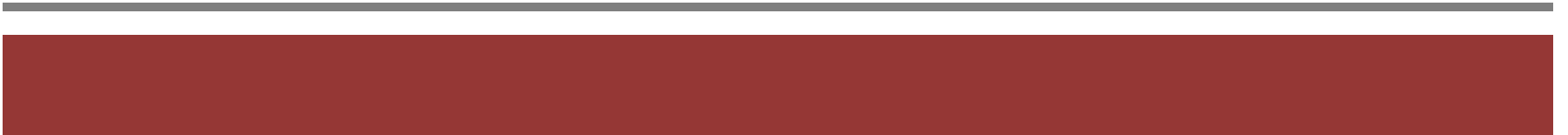




LECIS CANNELLA GRASSI  
STUDIO LEGALE ASSOCIATO

# ***La ripresa tra sicurezza e privacy***

***Avv. Giuseppe M. Cannella***



*«La Costituzione non contempla un diritto speciale per i tempi eccezionali, ma offre la bussola anche per navigare per l'alto mare aperto nei tempi di crisi».*

Lo stesso Presidente della Corte Costituzionale ha affermato che, anche in una situazione di emergenza sanitaria come quella attuale, tutti gli strumenti eccezionali adottati dal Governo hanno fatto salvi i principi generali in tema di tutela dei diritti fondamentali dell'uomo.

**INTERVENTI ECCEZIONALI MEDIANTE UTILIZZO DI NORME ORDINARIE**

Le misure imposte tutelano il **diritto alla salute**, ma incidono necessariamente su alcuni altri diritti fondamentali dell'uomo - costituzionalmente garantiti – quali la **libertà personale, la libera circolazione e la protezione dei dati personali**.

Tali limitazioni circoscritte nel tempo attraverso espresse previsioni normative.

Infatti, l'emergenza sanitaria non fa venir meno la tutela dei diritti, ma **la norma viene utilizzata come guida proprio per garantire la tutela dei diritti** in tale contesto.

Così come fatto dal Governo, i **Datori di Lavoro si trovano quindi a dover adottare strumenti eccezionali nel rispetto della normativa.** Non vi sono eccezioni dettate dall'emergenza che giustifichino il mancato rispetto della normativa ordinaria.

Non viene meno l'obbligo del Datore di Lavoro di «*adottare nell'esercizio dell'impresa le misure ....necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro*» (art. 2087 c.c.), nonché di rispettare le disposizioni del Testo Unico in materia di sicurezza.

Unica eccezione in materia di trattamento dei dati personali nel contesto emergenziale è stata prevista dal Governo, con parere positivo del Garante della Privacy espresso il 2 febbraio 2020, che autorizza le **autorità sanitarie** ad uno **scambio di dati sanitari in modalità semplificata** (art. 17 bis Cura Italia).

In questo caso, però, si tratta solo di soggetti qualificati (enti sanitari ed enti dediti alla tutela della sanità pubblica).

**Attenzione:** tale eccezione non coinvolge le aziende private.

Vediamo alcune delle norme ordinarie che vengono applicate nel contesto emergenziale.

**RISCHIO DA CONTAGIO COVID-19**  
=  
**RISCHIO BIOLOGICO DA ESPOSIZIONE AD AGENTI  
BIOLOGICI**  
(Titolo X del D.Lgs. 81/2008)

Nonostante la norma possa apparire letteralmente non applicabile al caso di contagio da Covid-19, in quanto inerente ad aspetti ambientali connessi alle sostanze ed agli strumenti utilizzati nel processo produttivo, la stessa è suscettibile di un'interpretazione estensiva alla luce del ***generale obbligo del datore di lavoro di tutelare i propri dipendenti dai rischi connessi all'attività lavorativa*** art. 2087 c.c.

Il Datore di Lavoro ha dunque l'obbligo di svolgere la valutazione del rischio da contagio (art. 271 Testo unico sicurezza), con il coinvolgimento del **RSPP** e del **Medico Competente**.

Quali gli adempimenti successivi?

- ✓ adozione di **misure di prevenzione**
- ✓ elaborazione **addendum al DVR**
- ✓ aggiornamento **DUVRI e POS**
- ✓ attività di **informazione e formazione** per i lavoratori
- ✓ effettuazione di **controlli** sul rispetto ed efficacia delle misure di prevenzione



Ai sensi del DPCM del 26 aprile 2020 ogni impresa deve:

- definire ed adottare un **Protocollo aziendale** che sulla base delle prescrizioni del *Protocollo Condiviso nazionale* definisca le misure di prevenzione, organizzazione e protezione della singola realtà aziendale;
- istituire un **Comitato per l'attuazione e il controllo** sul rispetto del Protocollo e definizione del relativo programma di controllo

## Alcuni esempi di misure di prevenzione del rischio

**ATTIVAZIONE SMARTWORKING**

**DISTANZIAMENTO SOCIALE E UTILIZZO DPI**

**DEFINIZIONE DI PROCEDURE IN INGRESSO IN AZIENDA  
PER DIPENDENTI E TERZI  
(autodichiarazioni e misurazione della temperatura)**

**SANIFICAZIONI AMBIENTI E IGIENIZZAZIONI  
PERSONALI**

**RIMODULAZIONE POSTAZIONI, ORARI E PROCESSI  
AZIENDALI**

Tra le misure eccezionali che i Datori di Lavoro sono stati chiamati ad attuare il più importante è senz'altro lo smartworking.

Smartworking significa svolgere la stessa attività lavorativa in un contesto completamente diverso, con diversi problemi e maggiori rischi.

Quali i principali rischi per il Datore di Lavoro?



### **LA DEFINIZIONE DELL'ACCORDO RELATIVO ALLA MODALITA' DI ESPLETAMENTO DEL LAVORO AGILE**

La normativa sul lavoro agile (L. 81 del 2017) prevede che le parti concludano un accordo scritto in cui disciplinare le modalità di esecuzione della prestazione, l'esercizio del potere direttivo, gli strumenti da utilizzare ed i tempi di riposo (il c.d. diritto alla disconnessione).

### **OBBLIGHI DEL DATORE DI LAVORO**

Il datore di lavoro è responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici assegnati al lavoratore per lo svolgimento dell'attività lavorativa. Ha l'obbligo di rendere un'informativa al dipendente sui rischi per la salute e sicurezza.

### **OBBLIGHI DEL LAVORATORE**

Il lavoratore è tenuto a cooperare all'attuazione delle misure di prevenzione predisposte dal datore di lavoro per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali.

Per la durata dello stato di emergenza di cui alla deliberazione del Consiglio dei ministri del 31 gennaio 2020 (6 mesi), il datore di lavoro può applicare la modalità di lavoro agile ad ogni lavoratore dipendente, **anche in assenza dell'accordo individuale** di cui all'art. 19 della legge 81/2017.

Gli **obblighi di informativa** di cui all'art. 22 della legge 81/2017 (relativamente ai rischi generali e specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro), sono assolti in **via telematica anche ricorrendo alla documentazione resa disponibile sul sito dell'INAIL.**

Ai sensi dell'art. 32 GDPR è opportuno che ogni Azienda che utilizzi lo strumento dello smartworking:

- ✓ adotti linee guida atte a definire le modalità di utilizzo di dispositivi aziendali e/o personali
- ✓ definisca le regole da osservare nello svolgimento dell'attività lavorativa al di fuori dei locali aziendali (es. adeguata conservazione del materiale cartaceo, adozione di cautele idonee a garantire la riservatezza delle conversazioni, ecc.)
- ✓ rafforzi le misure di sicurezza adottate, ad esempio attivando un sistema di doppia autenticazione (per l'accesso al pc e per l'accesso al server)
- ✓ fornisca specifiche istruzioni finalizzate alla prevenzione di fenomeni di phishing ed altri attacchi malware
- ✓ attui misure atte a consentire al personale IT di supportare il singolo dipendente e di intervenire nella gestione di eventuali breach.

Potrebbe essere utile, quindi, che all'interno del Regolamento sullo smartworking o tramite lettera di autorizzazione al trattamento dei dati personali, il Titolare del Trattamento fornisca ai propri dipendenti le istruzioni riguardanti:

1. Utilizzo della strumentazione e della «sede» lavorativa
2. Configurazione dispositivi (distinguendo tra aziendali e personali)
3. Gestione di credenziali e password
4. Gestione dei data breach

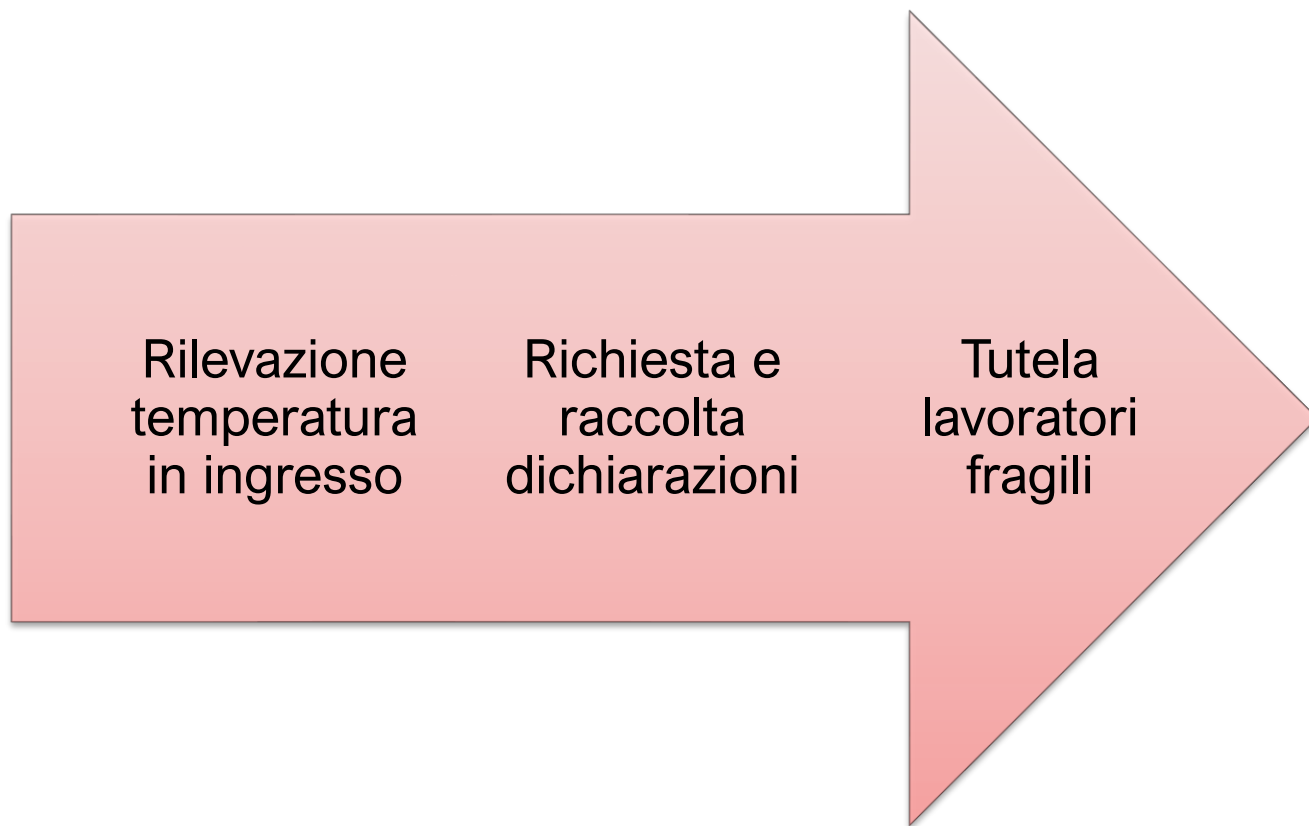
In assenza dell'accordo, che in ogni caso non potrà mai prevedere modalità in contrasto con l'art. 4 dello Statuto, il datore di lavoro non può avvalersi di modalità di controllo a distanza dello svolgimento della prestazione lavorativa da parte del dipendente (ad es. software di monitoraggio sull'uso del PC, accessi alla VPN aziendale, ecc.).

Il datore di lavoro potrà legittimamente prevedere modalità alternative di esercizio del proprio potere di direzione e controllo, come ad esempio **sistemi di rendicontazione giornaliera o settimanale sulle prestazioni effettuate.**

Il datore potrà, inoltre, svolgere su beni aziendali (pc, cellulari, casella e-mail) controlli mirati, proporzionati e non invasivi, finalizzati a riscontrare il sospetto di commissione di illeciti da parte del dipendente.



Alcune misure di prevenzione che il Datore di Lavoro deve/può adottare comportano un trattamento di dati personali, anche sanitari:



E' suggerito ai Datori di Lavoro di procedere alla misurazione della temperatura in fase di accesso in azienda sia dei dipendenti, sia dei terzi (visitatori, fornitori etc.).

Ai fini della legittimità del trattamento in oggetto, tuttavia, è necessario porre in essere alcuni adempimenti:

- **coinvolgimento del Medico Competente** nell'individuazione delle persone incaricate della misurazione e delle istruzioni tecniche;
- il **dato deve essere registrato (e dunque conservato) solo nei casi in cui la temperatura superi la soglia di 37,5°** e pertanto si determini la necessità di precludere l'ingresso all'interessato;
- nel caso in cui sia rilevata una temperatura superiore a 37,5° , è necessario che il soggetto sia posto in **isolamento momentaneo**, in un luogo appartato, e l'informazione sia trasmessa solamente ad una risorsa interna appositamente istruita (es. dipendente dell'ufficio HR).

Le aziende possono chiedere informazioni circa i contatti con soggetti risultati positivi al COVID, nonché sui recenti spostamenti nelle zone maggiormente colpite di dipendenti e visitatori.

Tali informazioni potranno essere raccolte anche attraverso questionari e autodichiarazioni.

In ogni caso, le Aziende sono tenute:

- a raccogliere esclusivamente i dati necessari ai fini di prevenzione (no nomi soggetti positivi, no luoghi precisi visitati),
- ad adempiere agli obblighi privacy connessi al trattamento eseguito (es. resa dell'informativa)
- a gestire le informazioni trattate con modalità idonee a garantire la riservatezza e l'integrità.

## La tutela dei lavoratori più fragili

Il Protocollo prevede che *«il medico competente segnali all'azienda situazioni di particolare fragilità e patologie attuali o pregresse dei dipendenti e l'azienda provvede alla loro tutela nel rispetto della privacy»*.

E' opportuno quindi che il datore di lavoro:

- ✓ istituisca un canale comunicativo apposito che abbia possibilmente come destinatario il medico competente
- ✓ informi i lavoratori di tale possibilità

Si applicano le norme che regolano la sorveglianza sanitaria in casi ordinari (il medico competente deve riferire al datore di lavoro l'identità del lavoratore **senza specificare patologie**. Il medico competente dà istruzioni sulla mansione che potrebbe svolgere il lavoratore o su particolari DPI da utilizzare).

- Informative privacy
- Aggiornamento del Registri dei trattamenti
- Valutazione del rischio sui nuovi trattamenti
- Eventuale Valutazione d'impatto
- Istruzioni ai soggetti autorizzati
- Definizione di procedure e policy

Grazie!



LECIS CANNELLA GRASSI  
STUDIO LEGALE ASSOCIATO

[www.lexlecis.com](http://www.lexlecis.com)

---

A solid dark red horizontal bar spanning the width of the page at the bottom.