**Consulenza e Formazione**

Sicurezza, Medicina del Lavoro, Sistemi
dii Gestione Qualità, Ambiente, Privacy
E Modelli Organizzativi

# Fase 2
# Adempimenti previsti dal GDPR al tempo del COVID-19

FRAREG
FRAFOR


info@frareg.com

Buongiorno a Tutti

Tra pochi minuti inizierà il Webinar

Durante la presentazione Vi preghiamo di disattivare i microfoni del vostro device per ridurre il rumore di fondo e permettere a tutti un ascolto senza interferenze.

Al termine dell'evento rimarremo a Vs disposizione per rispondere alle domande e per gli approfondimenti necessari .

# Adempimenti previsti dal GDPR al tempo del COVID-19


1. Inquadramento normativo: cosa ha introdotto la normativa d'urgenza;
2. HR e controllo degli accessi alla sede aziendale;
3. Lavoro da remoto - come regolamentarlo e gestirlo;
4. Buone prassi in materia di sicurezza informatica.


1

Inquadramento normativo: cosa ha introdotto la normativa d'urgenza?

# Efficacia

*Delibera del Consiglio dei Ministri del 31 gennaio 2020. Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*

È dichiarato, per **6 mesi** dalla data del presente provvedimento, lo stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili.



# La normativa di riferimento

- **DPCM 26 aprile 2020**

*Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, applicabili sull'intero territorio nazionale.*

- **L. 81/2017**

*Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato.*

- **Reg. UE 2016/679 (GDPR)**

*General Data Protection Regulation*

- **D.lgs. n. 196/2003**

*Codice Privacy*

# DPCM 26 aprile 2020

**Art. 1 – let. gg)**

*fermo restando quanto previsto dall'art. 87 del decreto-legge 17 marzo 2020, n. 18, per i datori di lavoro pubblici,* ***la modalità di lavoro agile disciplinata dagli articoli da 18 a 23 della legge 22 maggio 2017, n. 81, può essere applicata dai datori di lavoro privati a ogni rapporto di lavoro subordinato****, nel rispetto dei principi dettati dalle menzionate disposizioni,* ***anche in assenza degli accordi individuali ivi previsti****; gli obblighi di informativa di cui all'art. 22 della legge 22 maggio 2017, n. 81, sono assolti in via telematica anche ricorrendo alla documentazione resa disponibile sul sito dell'Istituto nazionale assicurazione infortuni sul lavoro;*

# DPCM 26 aprile 2020



**Art. 1 – let. hh)**

*si raccomanda in ogni caso ai datori di lavoro pubblici e privati di* ***promuovere la fruizione dei periodi di congedo ordinario e di ferie****, fermo restando quanto previsto dalla lettera precedente e dall'art. 2, comma 2*;

# DPCM 26 aprile 2020

1 Inquadramento normativo:
Cosa ha introdotto la normativa d'urgenza?

2 HR e controllo degli accessi alla sede aziendale

3 Lavoro da remoto Come regolamentarlo e gestirlo?

4 Buone prassi in materia di sicurezza informatica

***Allegato n. 6 - Protocollo per tutelare la salute e la sicurezza dei lavoratori dal possibile contagio da nuovo coronavirus e garantire la salubrità dell'ambiente di lavoro***


Disciplina le regole per l'accesso ai locali aziendali!

# DL. 81/2017



**Artt. 18 – 24**

**Disciplinano le regole di svolgimento del lavoro c.d. «*agile*»**

- **Art. 18 –** *Lavoro agile*
- **Art. 19 –** *Forma e recesso*
- **Art. 20 –** *Trattamento, diritto all'apprendimento continuo e certificazione delle competenze del lavoratore*
- **Art. 21 –** *Potere di controllo e disciplinare*
- **Art. 22 –** *Sicurezza sul lavoro*
- **Art. 23 –** *Assicurazione obbligatoria per gli infortuni e le malattie professionali*
- ***Art. 24 –*** *Aliquote contributive applicate agli assistenti domiciliari all'infanzia, qualificati o accreditati presso la provincia autonoma di Bolzano*

# Reg. UE 2016/679 (GDPR)



**Disciplina il trattamento dei dati personali all'interno dell'Unione Europea!**

# D.lgs. n. 196/2003 (Codice Privacy)



**Disciplina il trattamento dei dati personali ove non trova applicazione il GDPR.**

# 2

# HR
# e
# controllo degli accessi alla sede aziendale

1
Inquadramento normativo:
Cosa ha introdotto la normativa d'urgenza?

2
HR e controllo degli accessi alla sede aziendale

3
Lavoro da remoto Come regolamentarlo e gestirlo?

4
Buone prassi in materia di sicurezza informatica

# Allegato n. 6 - Protocollo per tutelare la salute e la sicurezza dei lavoratori dal possibile contagio da nuovo coronavirus e garantire la salubrità dell'ambiente di lavoro

- In presenza di febbre (oltre i 37.5) o altri sintomi influenzali vi è l'obbligo di rimanere al proprio domicilio e di chiamare il proprio medico di famiglia e l'autorità sanitaria.

- Mantenere la distanza di sicurezza, osservare le regole di igiene delle mani e tenere comportamenti corretti sul piano dell'igiene.

- L'impegno a 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.




Dato personale è **qualsiasi informazione (es. nome) concernente una persona fisica identificata o identificabile (art. 4 GDPR), anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari.**

La persona a cui si riferiscono i dati soggetti al trattamento si definisce "interessato". È importante tenere presente che l'interessato può essere solo una persona fisica e non un'azienda.




**È vietato** trattare dati personali che rivelino **l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona**.

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

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 (art. 4, par. 1, 2) del Regolamento (UE) 2016/679), non è ammessa la registrazione del dato relativo alla temperatura corporea rilevata,** bensì, nel rispetto del principio di "minimizzazione" (art. 5, par.1, lett. c) del Regolamento cit.), 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.

**Fonte FAQ Garante Privacy**



# L'amministrazione o l'impresa possono 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?

In base alla disciplina in materia di tutela della salute e della sicurezza nei luoghi 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)**. Al riguardo la direttiva n.1/2020 del Ministro per la pubblica amministrazione ha specificato che in base a tale obbligo il dipendente pubblico e chi opera a vario titolo presso la P.A. deve segnalare all'amministrazione di provenire (o aver avuto contatti con chi proviene) da un'area a rischio. In tale quadro il datore di lavoro può invitare i propri dipendenti a fare, ove necessario, tali comunicazioni anche mediante canali dedicati.

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.

**Fonte FAQ Garante Privacy**



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

In capo al medico competente **permane**, anche nell'emergenza, **il divieto di informare il datore di lavoro circa le specifiche patologie occorse ai lavoratori**.

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.

Il medico competente ha il compito di **informare il lavoratore fragile assicurandolo sulle misure messe in atto a tutela della sua salute sul posto di lavoro, correlate alla situazione di fragilità e presenza patologie attuali o pregresse che lo riguardano. Queste informazioni non saranno trasmesse al Datore di lavoro.**

**Fonte FAQ Garante Privacy**

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

**No.** In relazione al fine di tutelare la salute degli altri lavoratori, in base a quanto stabilito dalle misure emergenziali **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).

**Fonte FAQ Garante Privacy**

# 3

## Lavoro da remoto
## Come regolamentarlo e gestirlo?

# Definizione

**Art. 18**

*[…] modalità di esecuzione del rapporto di lavoro subordinato stabilita* ***mediante accordo tra le parti****, anche con forme di organizzazione per fasi, cicli e obiettivi e* ***senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa****. La prestazione lavorativa viene eseguita,* ***in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa****, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva.*

# Lo smart working 1/3



Regole generali da adottare per lo smart working:

| | | |
|---|---|---|
| Ottemperare alle regole di riservatezza e/o alle procedure già previste dall'Azienda (es. Policy sul corretto utilizzo dei dispositivi aziendali). | Massima diligenza nell'uso della strumentazione assegnata ai fini dell'esecuzione dell'attività lavorativa, (inclusa la sicurezza, anche fisica, dei dati contenuti nei dispositivi aziendali in uso) | Non comunicare e/o diffondere a terzi dati ed informazioni trattati e/o comunque appresi in ragione dell'esecuzione del rapporto di lavoro, anche nel caso di familiari. |

# Lo smart working 2/3



La modalità di lavoro in smart working prevede il rispetto di alcune norme per lavorare in sicurezza e proteggere i dati personali e le informazioni inerenti l'Ente anche fuori dai luoghi istituzionali.

| | | |
|---|---|---|
| Svolgere l'attività se possibile in un locale in cui sia impedito l'accesso anche ai familiari durante l'attività lavorativa, in alternativa non lasciare mai incustoditi i dispositivi utilizzati per la prestazione lavorativa (es. screen saver con password) | Utilizzare gli strumenti di condivisione messi a disposizione dall'azienda o da esso autorizzati (es. Sharepoint, Google Drive, posta elettronica) evitando applicazioni con utenze private (es. utenza Drop Box privata, WhatsApp). | Effettuare con regolarità gli aggiornamenti del sistema operativo e dell'antivirus presenti sul dispositivo utilizzato. |

# Lo smart working 2/3

Se non si è dotati di un dispositivo di proprietà aziendale o non è stato possibile portare con se quelli in dotazione, nel caso sia permesso l'utilizzo dei dispositivi privati devono essere adottate policy BYOD ("Bring Your Own Device" – Porta con se il tuo dispositivo) con le indicazioni di utilizzo in sicurezza.

**Aggiornare** regolarmente il sistema operativo e le applicazioni installate sui dispositivi

Effettuare con regolarità il **back up** dei dati presenti sul dispositivo

Evitare la **memorizzazione** di dati azienali su app non approvate

Loggarsi con **utenza dedicata** all'attività lavorativa e differente da quella utilizzata per uso privato (pc, tablet)

Evitare di effettuare **modifiche** alle configurazioni software dei dispositivi, perché questi potrebbero eludere i controlli di sicurezza.

**Custodire** i dispositivi mobili con diligenza in caso di spostamenti e non consentirne l'utilizzo promiscuo, in alternativa creare utenze diverse da quelle utilizzate per il lavoro

Mantenere **pin** e **password** su tutti i dispositivi

Segnalare sempre eventuali dispositivi **smarriti** o **violazioni** di dati

# Lo smart working 3/3



Attenzione all'utilizzo di connessioni private, assistenti digitali e phishing

Disattivare l'**assistente digitale** quando non viene utilizzato (Alexa, Google Home, ecc.)

**Non** utilizzare gli smart assistant per effettuare operazioni di lavoro

Nel caso non fosse fornita una **connessione** aziendale, cambiare le password dei default della connessione ADSL/Wi-fi o del router qualora queste non fossero sufficientemente complesse (es. 123456, Admin, 0000, ecc.).

Controllare sempre l'**attendibilità** delle mail: lay-out del messaggio, firma, ora dell'invio.

Non aprire mai allegati eseguibili, ovvero file che hanno come estensione ".exe", ".zip", ecc.

Nel dubbio chiedere al mittente se ha davvero inviato il messaggio.

In caso di richieste di pagamento o di dati riservati confermare sempre con il mittente via telefono per verificare che siano reali e autorizzate.

# Focus

Nella maggior parte delle piccole e medie imprese non è possibile dotare tutto il personale di dispositivi aziendali. Le ordinarie attività sono svolte utilizzando *devices* **personali**.

Tutto ciò rende **alto** il rischio di violazioni informatiche dei sistemi aziendali.

Consigliamo l'adozione di **linee guida specifiche** in materia di sicurezza informatica.

**Poche regole ma chiare aiutano la corretta prosecuzione delle ordinarie attività imprenditoriali!**

# 4

# Buone prassi in materia di sicurezza informatica

# Il principio di accountability

- È il principio cardine su cui si fonda l'impianto normativo del GDPR.
- Il Titolare del trattamento è **competente** per il rispetto dei principi enunciati nell'art. 5 del GDPR (liceità, correttezza, trasparenza; Limitazione delle finalità, minimizzazione dei dati; Esattezza; Limitazione della conservazione; Integrità e riservatezza) **ed in grado di comprovarlo** (art. 5).

- Il Titolare del trattamento deve mettere in atto (nonché riesaminare ed aggiornare) **adeguate misure tecniche ed organizzative**, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina (art. 24).



# Il data breach

**Attacchi informatici, accessi abusivi, incidenti** o **eventi avversi** (come incendi o altre calamità) che possono **causare la perdita, la distruzione o la diffusione indebita di dati personali trattati** dall'operatore.

Il Regolamento 2016/679 (GDPR) introduce nuove prescrizioni che in parte superano quelle preesistenti del Garante italiano.

Il Regolamento prevede che nel caso in cui si verifichi un data breach è necessario provvedere ad una **notifica al Garante entro 72 ore** dalla scoperta dell'evento.

# Esempi di misure di sicurezza adeguate:

## Organizzative

- Formazione del personale
- Procedure di Back up e disaster recovery
- Manutenzione impianti
- Piani di autocontrollo
- Controllo dei responsabili del trattamento

## Fisiche

- Gestione degli accessi (chiavi e allarmi)
- Armadi chiusi a chiave
- Distruggi documenti
- Sala server
- Gruppi di continuità
- Confomità al D.lgs 81/08



# Misure di sicurezza Logiche:

- Identificazione dell'Incaricato e/o Utente
- Antivirus
- Firewall
- Cifratura dei dati trasmessi
- Sospensione automatica delle sessioni di lavoro

# È importante non sottovalutare l'errore umano: per ridurre al minimo il rischio è necessario formare il personale!

# Grazie per l'attenzione… qualche domanda?

Per qualsiasi informazione:

**v.gilardoni@frareg.com**

**l.serra@frareg.com**