Gatti Pavesi Bianchi

COVID-19 Update
GARANTE DELLA PRIVACY

20 Marzo 2020

GARANTE DELLA PRIVACY

In data 11 marzo 2020, il Governo italiano, preso atto dell'ulteriore ed eccezionale aggravarsi dell'epidemia di COVID-19, ha raccomandato ai datori di lavoro di assumere misure anti-contagio (DPCM dell' 11 marzo 2020 art. 1 n. 7 lett. d), il quale espressamente dispone che *"in ordine alle attività produttive e alle attività professionali si raccomanda che si assumano protocolli di sicurezza anti-contagio e, laddove non fosse possibile rispettare la distanza interpersonale di un metro come principale misura di contenimento, con adozione di strumenti di protezione individuale"*. In data 14 marzo 2020 il Governo e i maggiori *stakeholders* (rappresentanti d'azienda e sindacati) hanno siglato un ulteriore protocollo che include misure per contrastare e contenere il diffondersi del COVID-19 (da qui in seguito il "**Protocollo**"), che incorpora una serie di prescrizioni e raccomandazioni in tema di trattamento dei dati personali risultante dall'implementazione di dette misure. Tra queste, specifica attenzione è stata dedicata alla possibilità di munire i locali aziendali di dispositivi per la rilevazione in tempo reale della temperatura corporea di dipendenti e visitatori che facciano ingresso in azienda.
Le misure idonee a garantire la sicurezza del luogo di lavoro possono essere sintetizzate come segue.

Doveri informativi

Da attuarsi tramite affissione di comunicati nei locali aziendali per informare visitatori e dipendenti riguardo a:

(i) Obbligo di rimanere al proprio domicilio con presenza di febbre (oltre 37,5) o altri sintomi influenzali e obbligo di avvertire il proprio medico;
(ii) Consapevolezza di non poter entrare o rimanere in azienda e di dichiararlo immediatamente, se successivamente all'ingresso, sussistano condizioni di pericolo (inclusi contatti con persone risultate positive negli ultimi 14 giorni);
(iii) Obbligo di rispettare misure di sicurezza (in particolare distanze e igiene);
(iv) Obbligo di avvisare immediatamente il datore se nell'orario di lavoro insorgano sintomi influenzali di qualsiasi tipo.

Misure di prevenzione (Misurazione della febbre tramite Termoscan)

Per regolare l'ingresso in azienda di dipendenti e visitatori il datore di lavoro potrà:

(i) sottoporre i dipendenti a rilevazione della temperatura corporea, impedendo l'accesso a coloro che registrino un valore superiore a 37,5, anche senza il necessario ricorso a personale del sistema sanitario nazionale o della Protezione civile, come inizialmente indicato dal Garante nella comunicazione del 2 marzo;
(ii) Disporre isolamento temporaneo del lavoratore e fornitura allo stesso di mascherina (i lavoratori in tale condizione non dovranno recarsi al Pronto

Soccorso o all'Infermeria, ma dovranno contattare il medico curante e seguire le sue indicazioni);

(iii) Informare preventivamente il personale e chi intende entrare in azienda della preclusione dell'accesso a chi, negli ultimi 14 giorni, abbia avuto contatti con soggetti risultati positivi a COVID-19 ovvero provenga da zone a rischio secondo le indicazioni dell'OMS.

Con specifico riferimento alla misurazione della temperatura queste le linee guida da seguire:

- Rilevare la temperatura e **non registrare il dato**; è possibile identificare l'interessato e registrare il superamento della soglia di temperatura solo per documentare le ragioni che hanno impedito l'accesso ai locali aziendali;
- fornire l'informativa, **anche oralmente, indicando che tra le finalità vi è la prevenzione da contagio COVID-19 e che la durata del trattamento è riconducibile allo stato di emergenza**
- definire **specifiche misure di sicurezza,** individuando **soggetti preposti al trattamento e fornendo loro specifiche istruzioni;**
- **garantire modalità idonee a tutelare riservatezza e dignità dell'interessato per il momentaneo isolamento del lavoratore**

I nostri suggerimenti operativi:

- Apporre cartelli informativi riguardo alle procedure di sicurezza nelle aree immediatamente antistanti i Termoscan e in altri locali quali mense, aree operative, servizi.
- Predisporre specifiche informative, che siano concise, ma complete, e che indichino gli elementi essenziali sopra individuati.
- Per impianti industriali con un numero rilevante di addetti si suggerisce il rilascio anche in forma cartacea e, ove possibile, la consegna di una copia per presa conoscenza;
- Predisporre istruzioni specifiche per i dipendenti che saranno incaricati del trattamento dei dati sensibili raccolti tramite Termoscan.
- Verificare che le misure di sicurezza di protezione dei dati siano correttamente implementate e adeguate ad evitare la dispersione dei dati.
- Laddove si richieda a dipendenti e visitatori il rilascio di una dichiarazione riguardo a possibili elementi di esposizione al rischio (contatti con soggetti risultati positivi a COVID-19 ovvero provenienza da zone a rischio secondo le indicazioni dell'OMS), questa sarà considerata come trattamento di dati personali e pertanto, previa comunicazione di idonea informativa, sarà necessaria la predisposizione di specifiche misure di sicurezza (inclusa l'individuazione di soggetti debitamente istruiti) e dovranno essere raccolti solo i dati necessari, adeguati e pertinenti rispetto alla finalità di prevenzione del contagio, con esclusione di dati identificativi delle persone risultate positive, ovvero di precisazioni sulle zone a rischio epidemiologico.

Cybersecurity: smart working e protezione dei dati personali e non personali

Per quanto riguarda le modalità di lavoro da remoto, fortemente consigliate dal DPCM e già adottate da molte aziende italiane, è necessario che esse siano il più possibile orientate alla protezione dei dati, siano essi personali o non personali.
L'accesso da remoto al sistema aziendale, se non adeguatamente presidiato, si espone a *data breaches* con rischi di dispersione dei dati personali e del *Know How* aziendale.
Da qui la necessità di dotarsi di un'adeguata infrastruttura informatica per far fronte a tale esigenza.

I nostri suggerimenti operativi:

1. Protezione dei dispositivi.

Rammentiamo che si connettono alla rete aziendale da remoto: i dispositivi, comunemente detti *Endpoint*, devono soddisfare determinati requisiti:

- *Strong-password:* è fortemente raccomandato l'utilizzo di password complesse, composte da numeri, lettere maiuscole e minuscole, caratteri speciali, etc.
- Cifratura dei dati salvati sul dispositivo: per proteggere i dati contenuti nel disco fisso dei PC è importante criptare l'hard disk. In questo modo in caso di furto/smarrimento del proprio PC i dati non sarebbero accessibili a qualche malintenzionato.
- Aggiornamento del sistema operativo, dell'antivirus, e dell'antispam: i software operativi e di protezione devono essere costantemente aggiornati al fine di garantire la miglior protezione possibile del dispositivo contro eventuali *malware* o virus.

2. Protezione dell'accesso alla rete aziendale:

- *Virtual Private Nework* (VPN): la VPN è una tecnologia di connessione che permette agli *endpoint* di collegarsi in modo sicuro – tipicamente le VPN utilizzano connessioni criptate - alla rete locale dell'azienda utilizzando la rete pubblica Internet. Tramite la VPN gli *endpoint* accedono a tutte le risorse condivise come se fossero fisicamente collegati alla rete aziendale.
- *Strong-Authentication:* è un sistema di protezione che rende più complicato l'accesso da remoto degli hacker alla rete aziendale. Infatti, per effettuare l'accesso, non è sufficiente la sola password ma anche un altro codice o certificato digitale o impronta biometrica.
- Gestione delle identità e degli accessi: l'accesso alle risorse condivise non può essere completo deve essere garantito principalmente in base:
  - al ruolo: è possibile identificare e separare i compiti dei dipendenti e dei collaboratori in modo da garantire gli accessi in base al loro ruolo (ad esempio la contabilità non avrà accesso ai documenti delle risorse umane e viceversa).
  - agli attributi: gli accessi possono essere garantiti tramite altri attributi personalizzati, ad esempio l'orario di accesso o alla posizione dove sono salvati files.

TEAM

Counsel
Massimiliano Patrini
Massimiliano.patrini@gpblex.it

Assistiamo i clienti dello Studio nella valorizzazione degli asset immateriali, nei diversi settori dell'Industria e dei Servizi (moda, lusso, pubblicità, commercio elettronico, bancario e finanziario, meccanico, chimico e farmaceutico), assicurando una consulenza organica, a livello domestico e internazionale, nei processi di trasferimento di tecnologia, acquisizione e fusione di società, negoziazione di accordi di licenza e cessione di privative industriali. La vasta esperienza maturata in ambito giudiziario ci consente di affiancare i clienti dello Studio in ogni contenzioso relativo a marchi, design, segreti industriali, concorrenza sleale e diritto d'autore.

Ci occupiamo di tematiche relativa alla data protection, valorizzazione e gestione dei dati personali e non personali, diritto delle nuove tecnologie.

CONTATTI

Milano
Piazza Borromeo, 8
20123 Milano (MI)
Tel. +39 02 8597 51
Fax +39 02 8094 47
studio@gpblex.it

Roma
Piazza dei Caprettari, 70
00186 Roma (RM)
Tel. +39 06 6813 4961
Fax +39 06 6813 4701
studioroma@gpblex.it

gpblex.it