

Come comportarsi nel caso in cui si venga a conoscenza di un dipendente (collega), affetto da VIRUS?

In primis contattare il RSPP, verosimilmente, il **datore di lavoro**, sarà già stato avvisato dai sanitari.

L'Ente, l'Azienda, la Ditta, la Società è composta da molti dipendenti, molti utenti, molti avventori? valutiamo quanti potrebbero essere i potenziali contagiati.

Ovviamente a questo punto nasce un nuovo trattamento di dati (che terminerà 60 gg dopo la conclusione dell'emergenza).

Non occorrerà fare DPIA.

Occorrerà, invece, effettuare una **nuova analisi dei rischi**, al fine della minimizzazione dei rischi Privacy: dato atto che la frequenza dell'evento dannoso non varierà e la classificazione rimarrà **"BASSA"** muterà, di fatto, la quantificazione del possibile danno, che diverrà **"GRAVE"**, da qui calcoleremo la QUANTIFICAZIONE ed avremo un valore nuovo da gestire, utilizzando procedure standard:

- a) formazione ai dipendenti (ulteriore e specifica) da specificare nell'atto di designazione (ex art.29 GDPR) od in altro modo efficace (lettera d'incarico aggiuntiva).
- b) applicazione articolo 32 del GDPR.

Il **Titolare del Trattamento** si vedrà obbligato a "costringere" il numero dei designati per la gestione dell'emergenza COVID-19, per due ordini di motivi:

- profilassi
- protezione dei dati.

Vademecum del designato alla gestione dei dati per l'Emergenza CORONAVIRUS:

1. Non comunicare il nominativo del contagiato a :PUBBLICHE AMMINISTRAZIONI E/O SOGGETTI ANCHE PRIVATI che abbiano le medesime finalità di: gestione della prevenzione, protezione, diagnosi e cura DELL'EPIDEMIA IN CORSO.
2. Osservare, rigorosamente il segreto d'Ufficio o quello professionale, per i pubblici dipendenti attenersi al dispositivo di cui all'articolo 28 della l. 241/90;
3. Non rilasciare interviste agli organi di stampa se non autorizzati dal Dirigente o dal Funzionario.
4. Non comunicare alcuna informazione se non – formalmente – autorizzati;
5. Distruggere le copie cartacee, di documenti non più utili.

6. NON USARE penne USB od HARD DISK esterni. Se indispensabile, utilizzare chiavi di crittografia, i più moderni device di backup esterno sono già muniti della suddetta tecnologia, in alternativa scaricate <https://www.veracrypt.fr/en/Home.html> od altro applicativo consigliato dai vostri consulenti informatici.
7. La crittografia deve essere utilizzata anche sui computer FISSI e sui NOTEBOOK
8. non sussiste alcun divieto di comunicare all'ASL, alla Regione ed alla protezione civile i nominativi delle persone potenzialmente contagiate, al contrario – detta comunicazione si rappresenta quale obbligo di contrasto all'epidemia. Corretta, comunque, sarà la individuazione di un soggetto quale “portavoce” con gli Organi Istituzionali.
9. Il titolare del Trattamento provvederà alla individuazione di CONTITOLARI del trattamento, in favore di quei soggetti che abbiano le medesime finalità di: gestione della prevenzione, protezione, diagnosi e cura DELL'EPIDEMIA IN CORSO come ad esempio: PROTEZIONE CIVILE, ASL, ARCA, ETC...;
10. In questa fase di emergenza si è esentati da formalismi per la eventuale integrazione della **Informativa Privacy e per la nomina degli incaricati/designati** come previsto dall'articolo 14 del DL 14/20 e dal Provvedimento dei Garanti d'Europa (EPDB), del 16 marzo 2020.

Si allegano i più recenti provvedimenti dell'Autorità Garante per la Protezione dei dati Personali; il Provvedimento dell'EPDB 16/03/2020.

Roma addì 25 marzo 2020

Federico Bergaminelli