

L' USO DEI SOCIAL NETWORK NELL'AMBITO LAVORATIVO

WEBINAR DI FORMAZIONE TECNICO PRATICA

12 maggio 2022 - ORE 14,00/17,00

1. PREMESSA

REGOLE E LIMITI IN MATERIA DI PROTEZIONE DEI DATI

Le modalità di relazione via social in ambito lavorativo sono oggi fondamentali. I social network offrono certamente vantaggi: la creazione di una community virtuale, lo sfruttamento di piattaforme che hanno visibilità per promuovere i prodotti, l'accesso a notizie in tempo reale. Tuttavia l'utilizzo per scopi lavorativi dei social network all'interno delle comunicazioni quotidiane presuppone l'applicazione del GDPR.

In conformità al Provvedimento del Garante n. 303 del 13 luglio 2016 e alle Linee Guida in materia di privacy nei servizi di social network del 20/11/2009 nonché a tutti i provvedimenti in materia emanati, i social sono ritenuti *strumenti di lavoro destinati non solo ad uso domestico o per scopi personali pertanto la relazione via social nei confronti di colleghi, superiori, fornitori, clienti deve essere quindi molto accurata.*

PERCHÈ?

- Quello che viene comunicato sul web è permanente, veloce e potenzialmente virale.

La rapidità dello strumento della *chat* presta spesso il fianco a notevoli rischi per le aziende nello scambio di ogni genere di comunicazioni di lavoro, compresi i furti di identità.

Molte aziende, infatti, hanno perso, anche nel recente passato, *il controllo dei propri dati personali* - proprio a causa di queste app di micro chat - mentre operavano.

I contenuti che pubblichiamo possono essere registrati dai nostri contatti *e dai componenti dei gruppi cui abbiamo aderito* e poi diffusi contro la nostra volontà permettendo facilmente anche l'azione di ladri di identità o truffatori di ogni genere.

- Le comunicazioni via social nell'ambito di lavoro fra colleghi non sono mai solo professionali e brevi ma purtroppo sono spesso utilizzate anche per

condividere dati sensibili o inviare informazioni critiche dell'azienda per cui si lavora, fotografare documenti o audio di lavoro riservati e spedirli a terzi.

Si registrano anche durante le attività svolte fra colleghi comunicazioni con scambi di password aziendali, numeri delle carte di credito, dati dei clienti, piani strategici, informazioni bancarie e salariali, persino risultati dei test Covid-19 dei dipendenti con relative prescrizioni sanitarie, veicolando documenti di estrema criticità con dettagli di attività che dovrebbero restare segrete.

– Nella nuova era dei social media gli utenti trovano in una chat o in post o in un tweet il "brand" della Società che contattano identificando nel messaggio la Società mittente della comunicazione.

Un dipendente, che gestisce i profili social dell'azienda, parla a nome della stessa perciò deve fare molta attenzione ai contenuti che vengono pubblicati, facendo in modo che siano perfettamente in linea con le esigenze, i valori e gli interessi del datore. E anche quando esce dall'ufficio, non smette di essere dipendente della propria azienda, **di conseguenza, sui propri profili social non può pubblicare qualsiasi cosa senza alcuna conseguenza.**

– Ogni social ha suoi caratteri specifici che lo rendono adatto a un suo obiettivo specifico e dunque vanno saputi gestire in base ad un proprio funzionamento, alle differenti prerogative di ciascuno e alle proprie modalità di utilizzo

Un'azienda che decide di stare sui social network quindi prima di inviare un messaggio, deve fare delle valutazioni preliminari e stabilire cosa vuole veicolare, rimanendo coerente con la percezione che gli utenti hanno del suo brand.

Decidere "tone of voice" è fondamentale (istituzionale, ironico, provocatorio) perché ciò va poi ad incidere nel modo in cui gli utenti interni o esterni comunicheranno con l'azienda.

2. SCOPO

Evitare il "Reputation disaster" dovuto ad errori di comunicazione (sostanziali o formali) che hanno come conseguenza danni economici seri perché il cliente identifica l'impresa nel messaggio secondo quanto previsto dalla disciplina della Protezione dei dati.

3. DESTINATARI

Sono tutti coloro che utilizzano i social esclusivamente durante l'attività lavorativa e a motivo della stessa:

- i vertici aziendali.
- i dipendenti che utilizzano e amministrano gli account aziendali;
- i dipendenti che utilizzano i propri account privati;
- i collaboratori che si interfacciano con la pagina aziendale attraverso account aziendali o attraverso i propri profili privati;

- tutte le persone esterne all'azienda che interloquiscono tramite social con l'azienda clienti:
 - . fornitori;
 - . visitatori dei siti dell'azienda;
 - . stakeholder.

Ma anche coloro che:

- con cadenza aggiornano i profili;
- detengono le password aziendali;
- si occupano di amministrare i canali social;
- parlano a nome dell'organizzazione.

4. RELATORI

- **Avv. Gianluca DI ASCENZO** - Presidente CODACONS
- **Avv. Anna CLEMENTI** - DPO e consulente privacy Certificato - Svolge attività di DPO a favore di alcune SRL - Docente in vari corsi per la formazione di figure che opereranno nel settore della Privacy ed esperta giusconsumerista
- **Dott. Delli Veneri Luciano** - Consulente in materia di privacy e diritto dell'informazione - Data protection officer.
- **Luca DI LEO** - Consulente in materia di privacy - Data protection officer -Vice Presidente Associazione Protezione Diritti e Libertà Privacy

I Relatori collaborano con Autorità Garante.

5. ARGOMENTI TRATTATI

- Come Redigere la Social Media Policy - SMP
- Obiettivi della social media policy (Interna ed Esterna)
- Ruoli privacy e responsabilità
- Regole del Garante comuni all'uso di tutti i Social network nell'ambito dell'attività lavorativa
- SOCIAL MEDIA POLICY interna ed esterna
- Regole nella pubblicazione dei contenuti all'interno delle chat nell'ambito lavorativo
- Analisi dei rischi sui social in caso di utilizzo di account personali dei collaboratori per comunicazioni di lavoro:
 - . a livello di gestione dei canali social
 - . a livello di gestione dei canali social ufficiali
- La gestione dei dati e la sicurezza sui social
- Come gestire un account aziendale di Facebook, Instagram, Twitter
- Come segnalare una violazione
- Dati conservati su smartphone e tablet

6. DURATA

La giornata formativa si svilupperà su 3 periodi di 55 minuti dalle ore 14,00 alle ore 17,00 (con 1 pausa caffè di 15 minuti al termine del secondo periodo).

Il corso sarà svolto con modalità WEBINAR su Piattaforma Zoom.

Per contenere i tempi e consentire di trattare tutti gli argomenti, i partecipanti all'attività formativa potranno chiedere successivamente eventuali specifici approfondimenti o chiarimenti scrivendo all'indirizzo mail che sarà loro fornito nel corso della seduta formativa.

7. ISCRIZIONE E COSTO

L'attività formativa è gratuita per tutti gli iscritti a Federmanager.

Gli associati accedono al network di servizi e consulenze della galassia Federmanager.

Scopri di più sul nostro sito www.federmanager.roma.it



**NON SEI ANCORA ISCRITTO A FEDERMANAGER?
SCANSIONA IL CODICE!**
Entra a far parte dell'Associazione di manager
più grande d'Italia.

INFO E CHIARIMENTI ➔ segreteria@federmanager.roma.it - T. 06 44170810

Con il patrocinio dell'Associazione protezione diritti e libertà privacy
www.associazionedirittiprivacy.it

