GLI IMPATTI SULLA TUTELA DELLA PRIVACY DURANTE L'EMERGENZA COVID-19: COME CONCILIARE INTERESSE PUBBLICO E TUTELA DELLA PRIVACY DEI LAVORATORI

La gestione della Privacy è un tema estremamente attuale anche in tempo di crisi da Covid-19. Bisogna infatti essere sicuri che le informazioni condivise e utilizzate siano adeguate, aggiornate ed esatte.

Questo avviene attraverso un uso lecito e corretto delle stesse, garantendone integrità e sicurezza.

Dal 31 gennaio 2020, giorno successivo alla dichiarazione dell'OMS, il Governo italiano ha sancito lo stato di emergenza della durata di 6 mesi (vale a dire fino al 31 luglio 2020, salve possibili proroghe) con la conseguente attivazione delle prime misure di contenimento del contagio e affidando al Capo del Dipartimento della Protezione Civile il coordinamento di tutti gli interventi nazionali necessari a fronteggiare la conseguente emergenza.

Dopo aver ricevuto parere favorevole del Garante per la protezione dei dati personali, il Capo della Protezione Civile, Angelo Borrelli, ha firmato l'Ordinanza Nr. 630, emessa ai sensi degli Artt. 7 e 25 comma 1 del D.lgs. 1/2018, che norma i primi interventi urgenti relativi "al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili" e in continuità con le misure urgenti già adottate dal Ministero della Salute.

In particolare:

- ✓ **L'Articolo 5 dell'Ordinanza – Trattamento dati personali – prevede**:
    - una prima estensione del potere di effettuare attività di trattamento dei dati personali stabilendo come, nell'attuale circostanza emergenziale, "i soggetti operanti nel Servizio nazionale di protezione civile di cui agli articoli 4 e 13 del decreto legislativo 2 gennaio 2018, Nr. 1, nonché quelli individuati ai sensi dell'Art. 1 della presente ordinanza, dalle Forze dell'Ordine ai Comuni, compresi i soggetti privati autorizzati che agiscono sulla base di specifiche direttive. Il focus è che questi soggetti possono realizzare trattamenti ivi compresa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del Regolamento del Parlamento Europeo 27 aprile 2016, Nr. 2016/679/UE, necessari per l'espletamento della funzione di protezione civile al ricorrere dei casi di cui agli articoli 23, comma 1 e 24, comma 1, del Decreto Legislativo 2 gennaio 2018, Nr. 1, fino al 30 luglio 2020.

Successivamente sono stati emessi:

- ✓ **Il decreto-legge Nr. 6 del 23 febbraio 2020** convertito con modificazioni, dalla legge 5 marzo 2020, Nr. 13, ed i **DPCM del 1marzo 2020, 8 marzo 2020 e successivi** che hanno previsto per l'intero territorio nazionale la possibilità per i datori di lavoro e per tutta la durata dello stato di emergenza di ricorrere immediatamente al remote-working pur in assenza di accordo individuale con il lavoratore;
- ✓ **Il decreto-legge n. 9 del 02 marzo 2020 e il recente DPCM 11 marzo 2020**.

Tuttavia, il diffondersi di prassi troppo artigianali e non omologate nella richiesta e nel monitoraggio di dati ha spinto il Garante per la Privacy a sottolineare gli aspetti di protezione e tutela dei lavoratori. Infatti, le misure preventive e di contrasto, anche emergenziali, devono sempre essere applicate entro i limiti stabiliti dalla normativa in materia di protezione dei dati personali e – in ambito lavorativo – delle norme dello Statuto dei lavoratori.

Si riportano i seguenti comunicati quali linee guida da applicare:

- ✓ **Garante Privacy - Comunicato stampa del 2 marzo 2020 - Coronavirus e protezione dati:**
  - "Il Garante invita tutti i titolari del trattamento ad attenersi scrupolosamente alle indicazioni fornite dal Ministero della salute e dalle istituzioni competenti per la prevenzione della diffusione del Coronavirus, senza effettuare iniziative autonome che prevedano la raccolta di dati anche sulla salute di utenti e lavoratori che non siano normativamente previste o disposte dagli organi competenti".
- ✓ **EDPB (European Data protection Board) - Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19 - adottata il 19 marzo 2020 - condivide raccomandazioni sulle aree relative a:**
  - *Liceità del trattamento dei dati;*
  - *Principi fondamentali relativi al trattamento dei dati personali;*
  - *Uso dei dati di localizzazione da dispositivi mobili;*
  - *Contesto lavorativo.*

L'obiettivo, sia del Garante che del Board Europeo per la protezione dei dati, è principalmente quello di tutelare la corretta gestione della Privacy andando a valutare correttamente gli aspetti più critici delle aree di lavoro coinvolte.

Dal mese di aprile 2020, a tal fine, il Garante della Privacy ha attivato una sezione informativa aggiornata in tempo reale – https://www.garanteprivacy.it/temi/coronavirus – dove si trovano tutti gli aggiornamenti e la raccolta delle principali disposizioni adottate in relazione allo stato di emergenza epidemiologica da Covid-19, aventi implicazioni in materia di protezione dei dati personali.

In questo articolo abbiamo pensato di analizzare in maniera più approfondita due delle aree maggiormente sensibili, ovvero: la gestione del controllo degli accessi agli ambienti di lavoro e la modalità di lavoro in "remote-working".

GESTIONE DEL CONTROLLO DEGLI ACCESSI

Il principale riferimento risulta essere il **"**Protocollo per contrasto e contenimento diffusione Covid-19 negli ambienti di lavoro**"** del 14 marzo 2020**, aggiornato in data 24 aprile 2020**.
Il maggiore impatto in materia di privacy, nella corretta applicazione di quanto previsto dai suddetti protocolli, si indentifica nella fase dell'accesso negli ambienti di lavoro.
La questione inerente alle modalità di accesso in azienda – lavoratori o personale esterno – è stata infatti oggetto delle valutazioni da parte della Task Force guidata da Colao, con particolare riferimento alla rilevazione della temperatura corporea da effettuare all'ingresso degli ambienti di lavoro mediante termometri ad infrarosso o Termoscanner. Tale misura, pur non risultando obbligatoria, risulta confermata nel DPCM del 26 aprile 2020 che ha fornito le indicazioni relative alle misure per il contenimento dell'emergenza Covid-19 nella cosiddetta "fase due".
Non si può evitare di porre attenzione sul fatto che tutte queste informazioni:

- la rilevazione in tempo reale della temperatura corporea;
- l'acquisizione di autocertificazioni attestanti che la temperatura corpora dei lavoratori/soggetti terzo sia inferiore ai 37,5 °C;
- l'acquisizione di dichiarazioni attestanti la non provenienza da zone a rischio epidemiologico;
- l'assenza di contatti con soggetti positivi al Covid-19;
- la ricezione di comunicazioni aventi ad oggetto certificazioni sanitarie;

sono qualificabili come attività di trattamento di dati personali, come confermato dalle note al punto 2 del DPCM del 26 aprile 2020 – MODALITÀ DI INGRESSO IN AZIENDA.

In particolare, ogni attenzione è comprensibilmente rivolta alle modalità operative dei controlli all'ingresso e, nel complesso, all'approccio che dovrà essere adottato per garantire il rispetto della normativa vigente in tema di privacy – in primis il Regolamento Europeo 2016/679 – detto GDPR.

In particolare, sottolineiamo le seguenti fasi e le relative criticità da gestire per ottemperare alle disposizioni in merito alla corretta gestione dei dati rilevati sul campo.

Dovranno essere definite le misure di sicurezza e organizzative, attivando sinergie tra Datore di Lavoro, RSPP, Medico Competente, RDP/DPO, tra le quali:

1. Aggiornare il Registro dei Trattamenti ai sensi dell'Art.30 Reg. Ue 2016/679, per il trattamento straordinario dei dati personali nel periodo di emergenza epidemiologica da COVID-19;
2. Autorizzare al trattamento dei dati personali i lavoratori incaricati alla rilevazione della temperatura corporea o alla raccolta delle autocertificazioni all'entrata in azienda – Incarico al Trattamento – Art. 2-quaterdecies Codice Privacy D.lgs. 196/2003 aggiornato al D.lgs. 101/2018 e Regolamento Europeo 2016/679;
3. Fornire ai lavoratori ed affiggere in azienda l'informativa sul trattamento dei dati ai sensi degli Artt. 13 e 14 Reg. UE n. 2016/679 e del D.lgs. 196/03 aggiornato dal D.lgs. 101/2018;

4. Gestire i flussi informativi limitandoli esclusivamente tra soggetti autorizzati al trattamento dei dati personali e vertici aziendali;
5. Far rilevare la temperatura corporea di chi accede agli spazi aziendali ai soggetti autorizzati al trattamento dei dati personali senza registrare la temperatura rilevata nel caso in cui la stessa non superi i 37,5 °C;
6. Nel caso in cui la temperatura corporea sia superiore ai 37,5 °C, impedire l'accesso al lavoratore/soggetto terzo ai luoghi di lavoro. Registrare – esclusivamente per i lavoratori dell'azienda – che al soggetto non è stato consentito l'accesso agli spazi aziendali in quanto la temperatura rilevata eccedeva i 37,5 °C – senza però registrare il dato effettivo della temperatura rilevata;
7. Far raccogliere esclusivamente ai lavoratori autorizzati al trattamento dei dati personali eventuali dichiarazioni su assenza di contatti con soggetti terzi contagiati o zone a rischio;
8. Attenersi sempre esclusivamente ad una raccolta limitata di dati pertinenti e strettamente necessari.

GESTIONE DELLA MODALITÀ "REMOTE-WORKING"

La seguente tabella riporta una serie di raccomandazioni e norme di buone prassi che devono essere messe in atto dai datori di lavoro e dai lavoratori durante questo periodo di remote-working.

	RACCOMANDAZIONI PER IL LAVORO IN REMOTE WORKING	
	LAVORATORI	**DATORI DI LAVORO**
DISPOSITIVI E RETI	**Utilizzare computer aziendali – quando in dotazione – non svolgendo sullo stesso computer attività personali**	**Fornire apparati informatici aziendali ai dipendenti in remote-working**
	Collegarsi via Internet utilizzando una rete sicura evitando reti aperte o gratuite	**Accertarsi che le caratteristiche tecniche e le protezioni della rete VPN aziendale siano in grado di sostenere un elevato numero di collegamenti simultanei**
	Accertarsi di avere sempre attivato gli applicativi di crittografia, mantenendoli debitamente aggiornati	**Mettere a disposizione un sistema di videoconferenze per i dipendenti e partner aziendali con capacità audio e video**
	Evitare lo scambio di informazioni critiche aziendali attraverso posta elettronica smistata su reti non sicure	**Accertarsi che il software di sicurezza sia aggiornato e che tutti i dipendenti effettuino regolari e tempestivi aggiornamenti**
	Usare solo risorse intranet aziendali per scambiare file di lavoro	**Garantire, attraverso procedure ad hoc, la sicurezza di apparati personali se utilizzati come laptop e smartphone aziendali**

	LAVORATORI	DATORI DI LAVORO
SICUREZZA DATI E PROCEDURE	Fare particolare attenzione a qualsiasi messaggio di posta elettronica che fa riferimento al coronavirus per evitare phishing o altre truffe informatiche	Accertarsi che vi sia sufficiente supporto tecnico per offrire assistenza ai dipendenti in remote-working
	I dati che vengono scaricati su archivi di memoria locali devono essere sempre bloccati con password per proteggerli da furto o perdita dell'apparato	Accertarsi che ogni trattamento di dati effettuato nel contesto di remote working sia conforme alle vigenti disposizioni afferenti alla protezione dei dati personali
	Mantenere sempre aggiornato ogni applicativo antivirus ed anti-malware	Accertarsi di aver aggiornato le procedure per fronteggiare incidenti afferenti alla sicurezza e violazione dei dati prendendo spunto dalla ISO27001
	Mantenere sempre aggiornati i sistemi operativi e le applicazioni utilizzate	Accertarsi che le procedure di remote working siano state comprese e sottoscritte dai dipendenti interessati
	Non condividere gli URL di incontri virtuali sui social media e su altri canali pubblici	Gestire i riscontri dei dipendenti sul processo di remote working per implementare azioni correttive o piani di continuità

Articolo realizzato da Ing. Federica Ferrario

La Segreteria di RAAM, sempre raggiungibile all'indirizzo mail **assistenza@raam.it** è a disposizione per ogni eventuale necessità o chiarimento.

VI INVITIAMO A SEGUIRE LA PAGINA LINKEDIN DI RAAM PER RIMANERE SEMPRE AGGIORNATI ATTRAVERSO I POST PREDISPOSTI DAI NOSTRI TECNICI

RAAM srl
Ricerca Applicata per l'Ambiente

20136 Milano – Via Ascanio Sforza, 29 – Tel. 02.67100436 – Fax 02.66703897
21040 Vedano Olona (VA) – P.zza San Rocco, 8/b – Tel. 0332.401477 – Fax 0332.401778
info@raam.it – https://www.raam.it – https://www.raamcloud.it
Operatore Accreditato da Regione Lombardia per i Servizi di Istruzione e Formazione Professionale – Sez. B
Albo Regionale N° 1024