PROTOCOLLI ANTI-COVID E TRATTAMENTO DATI

GUIDA PER AZIENDE

NETPATROL

DATA PROTECTION & CYBER SECURITY

NET PATROL ITALIA

Net Patrol Italia è una società di consulenza specializzata in **privacy** e **cybersecurity**.

Net Patrol raccoglie il **know-how** di professionisti operanti da anni nel settore della privacy, cybersecurity e ICT.

La nostra squadra, formata da **esperti di data protection, avvocati e tecnici specializzati**, affianca da vicino il cliente per sviluppare o migliorare i sistemi di gestione aziendali per privacy e cybersecurity.

Il nostro obiettivo è quello di dare al cliente un **interlocutore unico,** in grado di affrontare la protezione dei dati con approccio multidisciplinare e **business oriented**.

Crediamo fermamente che privacy e cybersecurity siano due pilastri importanti dell'economia **data-driven**, oltre che un mezzo per valorizzare il proprio business.

- Privacy compliance & governance
- Data Protection Officer
- Cybersecurity & Cyber law advisory

AFFILIAZIONI E PARTNERSHIP

intercom SOLUTIONS

ATMAN

karmasec

PREMESSA

Ogni azienda è impegnata nella definizione di nuovi processi e protocolli interni, al fine di gestire al meglio la nuova normalità del COVID-19.

Molti di questi processi e protocolli interni potrebbero comportare il **trattamento di dati personali** dei dipendenti, che deve essere fatto nel rispetto della normativa per evitare pericolose sanzioni.

Per dare il nostro contributo alla gestione dell'emergenza da COVID-19 abbiamo voluto creare questa **guida** destinata alle aziende, dove rispondiamo ad alcune delle più diffuse domande sul trattamento dei dati personali dei dipendenti.

IL PROTOCOLLO DI REGOLAMENTAZIONE

Il principale riferimento normativo per l'attuazione e gestione delle misure anti-covid in azienda è il Protocollo di regolamentazione, del 24 aprile 2020, ancora in vigore. Il protocollo prevede che la prosecuzione delle attività lavorative possa avvenire solo in presenza di condizioni che assicurino alle persone che lavorano **adeguati livelli di protezione**.

La mancata attuazione dei protocolli di sicurezza determina la **sospensione delle attività** fino al ripristino delle condizioni adeguate.

Considerati gli interessi in gioco, è importante che le aziende siano in grado di assicurare la tutela dei dipendenti, anche attraverso il trattamento lecito, corretto e trasparente dei loro **dati personali**.

FONTI RILEVANTI

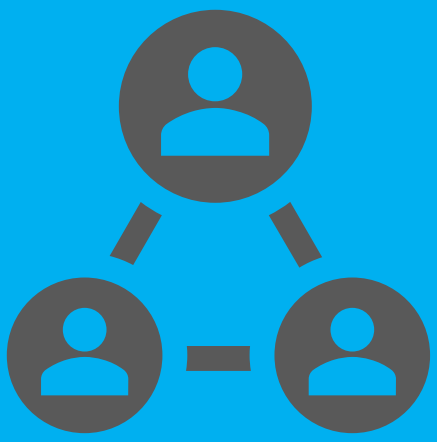
- Reg. UE 2016/679 (GDPR)
- Dichiarazione dell'Autorità Garante per la protezione dei dati, 2 marzo 2020
- Dichiarazione del Comitato Europeo per la protezione dei dati, 19 marzo 2020
- Protocollo di regolamentazione delle misure per il contenimento covid19, 24 aprile 2020
- DPCM 24 ottobre 2020
- D.L. 28/2020
- FAQ Garante Protezione Dati Personali

ULTIMO AGGIORNAMENTO

Febbraio 2021

PROTOCOLLI ANTI-COVID19 E TRATTAMENTO DI DATI

LIBERTÀ E DIVIETI PER IL DATORE DI LAVORO



Posso misurare la temperatura corporea a dipendenti o visitatori?

Il Protocollo prevede, come misura di sicurezza, la rilevazione della temperatura al personale dipendente, visitatori o clienti, prima dell'accesso ai locali aziendali.

✓	Il datore può **rilevare** la temperatura corporea prima dell'ingresso in azienda
⊘	Il datore non può **registrare** la temperatura corporea identificando il dipendente

La **rilevazione in tempo reale** della temperatura, quando effettuata con mezzi manuali (es. termometro elettronico) non è un trattamento di dati soggetto alla normativa privacy.

Si consiglia quindi di evitare in ogni caso di registrare la temperatura corporea, sia per evitare inutili trattamenti di dati, che per rispettare il principio di minimizzazione di cui all'articolo 5 del GDPR.

✓	Invece di registrare la temperatura, sostituisci il dato con un **giudizio di idoneità** o non idoneità all'ingresso!

Termoscanner

I termoscanner sono ormai molto utilizzati, perché velocizzano le operazioni di ingresso e non c'è bisogno di supervisione umana. Ci sono però alcune questioni di cui bisogna tenere conto.

I termoscanner acquisiscono e archiviano diverse tipologie di dati. Alcuni modelli, ad esempio, acquisiscono dati come il battito cardiaco della persona o immagini del viso per consentire il riconoscimento facciale (spesso abbinato a logiche di accesso ai locali aziendali).

Questo trattamento di dati ulteriore dovrà quindi rispettare tutti i requisiti normativi, oltre che essere identificato e descritto nel **Registro delle attività di trattamento** (articolo 30 GDPR).

In alcuni casi potrebbe essere illecito trattare alcune tipologie di dati senza una corretta base giuridica e senza l'adozione di particolari misure di tutela per le persone.

	Il divieto di associare l'identità del dipendente con uno storico della temperatura corporea sussiste anche con l'uso di termoscanner.
	Molti termoscanner utilizzano tecnologie di face detection o facial recognition. Questi sono trattamenti di dati ulteriori che necessitano di specifiche accortezze. Il **facial recognition** è un trattamento di dati biometrici che gode di tutele rafforzate a fronte dei maggiori rischi legati alla tipologia di dato. È **vietato** trattare dati biometrici del dipendente senza un suo **consenso espresso** o senza autorizzazione di legge.

Posso inviare ai dipendenti questionari per sapere se hanno frequentato persone o zone a rischio negli ultimi 14 giorni?

Tra le misure di prevenzione previste anche dal Protocollo c'è la preclusione dell'accesso alla sede di lavoro per coloro che provengano da zone a rischio. In questo contesto, è possibile chiedere ai dipendenti una dichiarazione che attesti queste circostanze.

✓	Il datore può ottenere una **dichiarazione** da parte del dipendente di non aver frequentato zone a rischio.
⊘	Evita di acquisire dati personali ulteriori **non necessari**, come le specifiche località visitate,

Eventualmente, questa dichiarazione può essere rivolta anche a terzi (visitatori, clienti, fornitori, ecc.).

Come sempre, è bene evitare di acquisire informazioni **inutili**, il cui unico scopo è quello di de-responsabilizzare il datore, ottenendo in realtà l'effetto contrario.

Posso chiedere ai dipendenti informazioni sul loro stato di salute o sulla presenza di sintomi influenzali?

La sorveglianza sanitaria in azienda rimane **competenza** esclusiva del **medico** del lavoro, che deve comunque rispettare il **divieto** di informare il datore di lavoro delle specifiche patologie dei lavoratori.

In ogni caso, il medico deve segnalare al datore situazioni di particolare fragilità, per adottare le misure anti-covid19.

⊘	Il datore deve astenersi dal raccogliere informazioni sulla presenza di **sintomi influenzali** o che comunque riguardano lo stato di salute del dipendente.
✓	In alcuni casi il datore può venire a conoscenza dello **stato di positività o negatività** del lavoratore, ad esempio quando è lo stesso lavoratore a comunicarlo.
✓	Il datore può venire a conoscenza dello **stato di negativizzazione** del tampone, per riammettere i dipendenti guariti presso la sede di lavoro. Le visite e gli accertamenti, anche per la riammissione al lavoro, devono essere però fatti dal medico, perché la legge **vieta** al datore di lavoro di effettuare direttamente esami diagnostici sui dipendenti.

Se non posso trattare questi dati, come faccio a sapere se i miei dipendenti sono a rischio?

I rischi possono essere mitigati e gestiti attraverso adeguate **procedure interne**, che, come obiettivo, devono avere quello di **responsabilizzare** i soggetti che frequentano l'azienda e ridurre al minimo l'uso di dichiarazioni, auto-certificazioni e acquisizioni di dati in generale.

L'articolo 20 del D.Lgs. 81/2008 prevede che il dipendente abbia lo specifico **obbligo di segnalare** al datore di lavoro **qualsiasi situazione di pericolo** per la salute e sicurezza sul lavoro.

Un dipendente che dovesse sospettare di essere a rischio (o positivo) deve **segnalarlo** al datore di lavoro e astenersi da fare ingresso in azienda, comunicando le circostanze al proprio medico, che deciderà nel merito.

È possibile chiedere dichiarazioni scritte ai dipendenti che entrano in azienda (nel rispetto dei criteri menzionati nella precedente sezione). È anche possibile prevedere dei canali privilegiati e riservati per la comunicazione di queste situazioni di rischio.

Posso comunicare l'identità di dipendenti positivi al COVID-19 a RLS o altri dipendenti?

Il **RLS** svolge una funzione di verifica, coordinamento e collaborazione con medico e datore, per la promozione delle misure di sicurezza.

È possibile che il Rappresentante dei lavoratori per la sicurezza abbia accesso a dati che riguardano dipendenti positivi (es. nel documento di valutazione dei rischi), ma che dovrebbero comunque essere **anonimizzati** e in forma aggregata.

In nessun caso il datore di lavoro può **comunicare** l'identità di dipendenti positivi al COVID a RLS o ad altri dipendenti.

La tutela della salute pubblica e dei lavoratori spetta alle autorità sanitarie competenti.

Posso richiedere che i dipendenti facciano tamponi o test sierologici?

Attraverso il medico competente l'azienda può richiedere di effettuare tamponi o test sierologici. Solo il medico competente può stabilire la necessità di particolari esami clinici e biologici e suggerire l'adozione di mezzi diagnostici.

Il datore non può acquisire **referti** o esiti degli esami, che dovranno essere trattati dal medico competente.

Il datore può trattare dati relativi al **giudizio di idoneità** predisposto dal medico competente, anche nel caso di riammissione al lavoro dopo aver effettuato un test.

Posso chiedere ai dipendenti se hanno fatto il vaccino?

In linea generale, il datore di lavoro non può mai trattare dati relativi alla salute dei dipendenti. Anche le informazioni sullo stato vaccinale sono dati relativi alla salute.

	Come per altri casi, il datore di lavoro non può indagare sullo stato di salute dei dipendenti. Non è quindi possibile trattare **dati che riguardano lo stato vaccinale** dei dipendenti, **neanche col loro consenso** (che sul luogo di lavoro si considera sempre invalido).
	Solo il **medico competente** può trattare i dati sanitari dei lavoratori e le relative informazioni vaccinali.

I miei dipendenti sono esposti a situazioni a rischio. Cosa posso fare?

Alcuni contesti lavorativi potrebbero esporre i dipendenti a situazioni di rischio, come nel contesto sanitario.

In questi casi si applicano regole precise, che però non permettono comunque al datore di lavoro di trattare direttamente le informazioni vaccinali dei dipendenti.

	Nei casi di esposizione diretta ad agenti biologici durante il lavoro trovano applicazione le **misure speciali di protezione** previste per alcuni ambienti lavorativi (art. 279, Titolo X del d.lgs. n. 81/2008). In questi casi, è comunque sempre il **medico competente** che ha la funzione di raccordo tra il sistema sanitario e il contesto lavorativo. Sarà quindi sempre il medico a poter trattare i dati vaccinali dei dipendenti e valutare la loro idoneità alla mansione specifica.

I PRINCIPALI REQUISITI DELLA NORMATIVA PRIVACY

Informazioni sul trattamento e trasparenza (artt. 12 – 14 GDPR)

Uno dei principali requisiti della normativa privacy è la trasparenza.

I dipendenti, così come qualsiasi altro soggetto interessato, hanno **diritto di conoscere** tutte le informazioni in merito al trattamento dei loro dati personali, anche nell'ambito del contrasto al coronavirus.

Aggiorna le **informative privacy** destinate ai dipendenti e comunica tutte le informazioni sul trattamento di dati insieme ai protocolli anti-covid.

Le modalità di comunicazione di queste informazioni sono libere, ma è opportuno che sia fatto con modalità che possono tenere traccia di chi ha ricevuto la comunicazione, anche ai fini probatori.

Registro delle attività di trattamento (art. 30 GDPR)

Ogni nuova attività di trattamento deve essere identificata e descritta nel Registro delle attività di trattamento, ai sensi dell'articolo 30 GDPR.

Aggiorna il **Registro delle attività di trattamento** con ogni nuovo trattamento di dati personali.

Alcune tipiche attività di trattamento relative ai protocolli anti-covid sono: l'uso di termoscanner, l'acquisizione e conservazione di dichiarazioni e autocertificazioni, l'introduzione di nuovi software gestionali, o il monitoraggio degli strumenti aziendali in caso di **remote working**.

Diritto di accesso ai dati (art. 15 GDPR)

La normativa prevede il diritto di accedere ai dati personali trattati dal datore, ed eventualmente ottenerne copia. Ogni dipendente può richiedere al datore di accedere ai propri dati personali, sia in generale che per uno specifico trattamento (es. protocolli anti-covid).

Adotta specifiche **procedure** per ricevere e gestire queste richieste entro i tempi di legge (30 giorni). Le procedure dovrebbero essere gestite dall'ufficio Risorse Umane.

Per coadiuvare l'attività di recupero e consegna di copia dei dati, i sistemi informativi dovrebbero essere configurati per consentire estrazioni di dati in formato elettronico standard.

Limitazione della conservazione (art. 5 GDPR)

In generale, ogni azienda deve essere in grado di gestire il ciclo vita dei dati personali trattati. Questo vale in particolar modo per i dati relativi ai protocolli anti-covid, che dovrebbero essere cancellati periodicamente entro breve termine.

Verifica che le **politiche di conservazione** di dati siano aggiornate per includere anche i dati acquisiti per l'attuazione dei protocolli anti-covid, e garantisci l'introduzione di misure tecniche o organizzative adeguate a consentire la loro cancellazione periodica.

Responsabili del trattamento (art. 28 GDPR)

L'introduzione dei protocolli anti-covid può comportare anche l'ingresso di nuovi **soggetti esterni** che trattano dati personali per conto dell'azienda. È il caso, ad esempio, dei termoscanner, che potrebbero essere dotati di *software as a service*, gestito dal fornitore.

I fornitori che trattano dati personali per conto dell'azienda sono qualificati responsabili del trattamento, e devono essere soggetti a particolari **clausole contrattuali** previste dall'articolo 28 GDPR.

Identifica quali **soggetti esterni** sono incaricati di trattare dati personali e verifica di aver concluso tutte le clausole contrattuali obbligatorie per legge.

C'è altro da tenere in considerazione?

Le indicazioni qui riportate sono **solo una parte** di ciò che compone un sistema di gestione privacy, e riguardano più che altro le principali obbligazioni a cui tutte le aziende sono soggette, a prescindere dal contesto e dalle attività di trattamento concretamente realizzate.

L'azienda è però chiamata a rispettare ogni prescrizione e principio previsti dalla normativa privacy. Se sei in dubbio su quali siano gli **ulteriori adempimenti** di legge a cui è soggetta la tua azienda, chiedi al tuo consulente privacy o Data Protection Officer.

Sono previste sanzioni in caso di violazione della normativa privacy?

Il Reg. UE 2016/679 ("GDPR") prevede specifiche sanzioni amministrative in caso di violazione della normativa privacy.

La violazione dei principi fondamentali prevede due diversi massimali sanzionatori:

20 milioni di euro **/** **4% del fatturato globale** **(il valore più alto)**	In caso di violazione dei **principi fondamentali** (articoli 5, 6, 7, 9) o di violazione dei diritti dei soggetti interessati (articoli da 12 a 22).
10 milioni di euro **/** **2% del fatturato globale** **(il valore più alto)**	In caso di violazione degli **altri obblighi** previsti dalla normativa, come gli obblighi che riguardano i responsabili del trattamento (articolo 28) o in caso di mancata adozione di misure adeguate a garantire la sicurezza dei dati (articolo 32).

Oltre ai rischi sanzionatori, bisogna fare i conti con rischi collaterali, come eventuali **richieste di risarcimento** danni in caso di violazione dei dati dei dipendenti (come nel caso di diffusione non autorizzata dell'identità di dipendenti positivi al COVID).

È bene poi sottolineare che, in generale, un sistema di gestione privacy organico e adeguatamente maturo, è anche in grado di mitigare rischi relativi a **incidenti di sicurezza**, che possono mettere a dura prova la resilienza e continuità operativa di un'azienda, già provata dalle misure emergenziali.

Net Patrol Italia

www.netpatrol.it - info@netpatrol.it - 02 87165913

Sede di Milano
Via Napo Torriani, 31 | 20124 Milano

Sede di Udine
Via Giovanni Paolo II, 3 | 33100 Udine

PROTOCOLLI ANTI-COVID E TRATTAMENTO DATI

GUIDA PER LE AZIENDE

Febbraio 2021

Disclaimer:

Questa pubblicazione non intende sostituire le fonti legali e riflette unicamente le opinioni degli autori.

Le azioni intraprese dalle organizzazioni non possono basarsi esclusivamente sulla lettura di questa pubblicazione.

In nessun modo la lettura di questa pubblicazione può sostituire il lavoro prestato da persone specializzate e competenti nella materia della protezione dei dati personali. Net Patrol Italia s.r.l. non può essere ritenuta responsabile per i danni o le violazioni del Regolamento UE 2016/679 realizzate dalle organizzazioni che fondino le proprie decisioni esclusivamente sulla base di questa pubblicazione.