




Tonucci & Partners



Il trattamento dei dati sanitari dei lavoratori nell'emergenza coronavirus: l'equilibrio tra applicazione del GDPR e norme emergenziali.



Il bilanciamento tra diritto alla riservatezza e tutela pubblica della salute collettiva.



PRIVACY vs. TUTELA DELLA SALUTE PUBBLICA

Come è noto, **l'introduzione di norme emergenziali** per il contenimento e il contrasto della grave epidemia in corso di COVID-19 **ha interessato anche la normativa *data protection***, che ovviamente viene primariamente in considerazione in un momento così grave (si pensi alla tracciatura dei dati sanitari tra tamponi e contagi, agli incroci delle informazioni a scopo di studio epidemiologico, alle comunicazioni tra enti pubblici e privati dei dati dei cittadini positivi al COVID-19 che necessitano di ospedalizzazione ai fini della gestione dei posti, anche di terapia intensiva, etc).

Tutti si fanno la stessa domanda: ha senso in questo momento la protezione dei dati personali in un contesto emergenziale, dove la “privacy” potrebbe essere sentita come – oppure potrebbe costituire oggettivamente – un ostacolo alla gestione dell'emergenza?



PRIVACY vs. TUTELA DELLA SALUTE PUBBLICA

La domanda in realtà reca in sé una **trappola “emotiva”**, possibile fonte di risposte e reazioni **istintive** che effettivamente sembrano spingere verso la direzione di considerare la “*privacy*”, in questo momento, un qualcosa di cui fare volentieri a meno: ad esempio in **Corea del Sud**, che era il secondo Paese al mondo per numero di contagi fino a qualche settimana fa, sono riusciti attualmente a fermare l’epidemia (oramai da tempo sotto controllo) anche **attraverso una app di geolocalizzazione degli spostamenti dei cittadini, in grado di ricostruire compiutamente la cosiddetta “catena dei contatti” in caso di positività al virus, con il pronto isolamento degli interessati**. Alcuni studi sostengono che questo controllo capillare via cellulare (in Europa **non pienamente** praticabile in base alle attuali regole *data protection*, anche emergenziali) abbia contribuito in maniera addirittura decisiva (unitamente ai tamponi effettuati su tutta la popolazione asintomatica) al controllo ormai in atto dell’epidemia in quale Paese.



PRIVACY vs. TUTELA DELLA SALUTE PUBBLICA: IL CASO DELLA COREA DEL SUD

Il modello della Corea del Sud ha puntato innanzitutto su **test a tappeto** e poi sull'uso della tecnologia con **applicazioni mobili e attingendo a Gps o carte di credito per creare una mappa del contagio**, utile anche per allertare le persone che potrebbero aver incrociato un infetto, di cui nessuno saprebbe nome e cognome (ma tutti saprebbero dove è stato e chi lo conosce potrebbe ricostruirlo). Questa è una misura **lesiva della privacy** e bisogna avere la certezza che il **dato venga usato a fini di sanità pubblica**, ma tracciare tutti i contatti dei positivi può aiutare a contenere il contagio, anche in questa condizione di semi reclusione in cui siamo. Si tratta di una misura eccezionale che dovrebbe essere svolta solo per un determinato periodo.



PRIVACY vs. TUTELA DELLA SALUTE PUBBLICA: ALCUNE PRIME CONCLUSIONI

In realtà non dobbiamo e possiamo correre il rischio (grave quanto quello epidemico in corso) di rinunciare alla privacy: la tenuta democratica delle istituzioni e la tenuta anche dell'insieme delle garanzie e tutele democratiche e normative in favore della cittadinanza passa anche attraverso il mantenimento (non la rinuncia) delle ordinarie prescrizioni sulla protezione dei dati personali, da gestire con freddezza che eviti scelte istintive e dannose anche nel medio termine.

D'altra parte, tanto il Regolamento Generale UE 679/2016 ("RGPD") sulla protezione dei dati personali quanto la stessa logica che da sempre permea la disciplina sulla protezione dei dati personali (e cioè quella del contemperamento di opposte esigenze come la libera circolazione delle informazioni e il diritto alla protezione dei dati personali), contengono in sé dei meccanismi atti a rendere applicabile – senza snaturarla – la protezione dei dati anche in contesti emergenziali come quello che stiamo vivendo. Senza che sia cioè necessario rinunciare *in toto* alle tutele (e alle corrispondenti prescrizioni obbligatorie in capo a chi tratta i dati) come molti vorrebbero fare (istintivamente) in questo momento.



**La legislazione emergenziale
data protection del Governo
italiano.**



PRIVACY vs. TUTELA DELLA SALUTE PUBBLICA: LE SCELTE DEL GOVERNO

Ordinanza 630 del 9 marzo 2020 con cui la Protezione civile ha ottenuto una deroga per acquisire e trattare i dati biometrici che identificano in modo univoco una persona o quelli sulla salute.

Decreto-Legge 9 marzo 2020, n. 14, recante “*Disposizioni urgenti per il potenziamento del Sistema Sanitario Nazionale in relazione all'emergenza COVID-19*” che all'articolo 14 fissa le condizioni per il trattamento dei dati sanitari dei cittadini nel contesto emergenziale;

Legge 24 Aprile 2020, n. 27 (in cui è di fatto confluito l'articolo 14 del decreto legge – non convertito n. 14/2020) di conversione del d.l. 17 Marzo 2020, n. 18 recante «*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*» che all'articolo 17-bis fissa le condizioni per il trattamento dei dati sanitari dei cittadini nel contesto emergenziale all'articolo 76 prevede la nomina di un "**contingente di esperti**" che si occupi "**di dare concreta attuazione alle misure adottate per il contrasto e il contenimento del diffondersi del virus con particolare riferimento alle soluzioni di innovazione tecnologica**".

Protocollo Confindustria/Sindacati siglato il 14 Marzo 2020 (e aggiornato il 24 aprile 2020) sulla “*Regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro*” che reca numerose disposizioni in materia di trattamento dei dati personali dei lavoratori da parte dei datori di lavoro.




PRIVACY vs. TUTELA DELLA SALUTE PUBBLICA: LE SCELTE DEL GOVERNO

Decreto-Legge 30 aprile 2020, n. 28, recante “*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*” che all’articolo 6 fissa le condizioni per il trattamento dei dati personali nell’ambito del sistema nazionale di tracciamento (**contact tracing**).

Decreto-legge 10 maggio 2020, n. 30 recante «*Misure urgenti in materia di studi epidemiologici e statistiche sul SARS-COV-2*».

[Raccolta delle principali disposizioni adottate in relazione allo stato di emergenza epidemiologica da Covid-19 aventi implicazioni in materia di protezione dei dati personali \(AGGIORNATO AL 7 MAGGIO 2020\)](#)



**L'articolo 17-bis del d.l. 17
Marzo 2020, n. 18
(«Disposizioni sul trattamento
dei dati personali nel contesto
emergenziale»).**



L'ARTICOLO 17-bis DEL D.L. 18/2020 SUL TRATTAMENTO DEI DATI PERSONALI NEL CONTESTO EMERGENZIALE

Secondo **l'articolo 17-bis** del Decreto Legge del 17 marzo 2020 n. 18 che introduce misure urgenti per il rafforzamento del Sistema Sanitario Nazionale in relazione all'emergenza COVID-19, fino al termine dell'attuale emergenza sanitaria deliberata fino al 31 Luglio 2020 dal decreto del Presidente del Consiglio e al fine di:

- 1) garantire la protezione contro la diffusione transfrontaliera del COVID-19;
- 2) garantire l'assistenza sanitaria e la diagnosi per le persone colpite;
- 3) garantire la gestione generale del Sistema Sanitario Nazionale.



L'ARTICOLO 17-bis DEL D.L. 18/2020 SUL TRATTAMENTO DEI DATI PERSONALI NEL CONTESTO EMERGENZIALE

Ai sensi dell'articolo 9, comma 2, lettere g), h) e i) e dell'articolo 10 del Regolamento UE 679/2016 e all'articolo 2-sexies del Codice della Privacy:

- **i soggetti pubblici autorizzati ad operare nell'ambito del Sistema Nazionale di Protezione Civile;**
- **i soggetti attuatori di cui all'articolo 1 dell'Ordinanza della Protezione Civile 630/2020 individuati tra gli enti pubblici economici e non economici e soggetti privati che agiscono sulla base di specifiche direttive;**
- **il Ministro della Salute;**
- **l'Istituto Superiore della Sanità;**
- **gli enti pubblici e privati operanti nell'ambito del Sistema Sanitario Nazionale e**
- **i soggetti preposti al controllo delle misure di emergenza già emanate**



L'ARTICOLO 17-bis DEL D.L. 18/2020 SUL TRATTAMENTO DEI DATI PERSONALI NEL CONTESTO EMERGENZIALE

anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni ad essi attribuite nell'ambito dell'emergenza determinata dal diffondersi del COVID-19.



L'ARTICOLO 17-bis DEL D.L. 18/2020 SUL TRATTAMENTO DEI DATI PERSONALI NEL CONTESTO EMERGENZIALE

La comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli autorizzati al comma 1, nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del citato regolamento (UE) 2016/679, sono effettuate nei casi in cui risultino indispensabili ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto.

Tutti i trattamenti di cui sopra saranno comunque effettuati nel pieno rispetto dei principi di cui all'art. **5 del Regolamento UE 679/2016**, adottando specifiche garanzie per i soggetti interessati.




LA'RTICOLO 17-bis DEL D.L. 18/2020 SUL TRATTAMENTO DEI DATI PERSONALI NEL CONTESTO EMERGENZIALE

I soggetti pubblici e privati autorizzati di cui al comma 1 sono autorizzati a:

- **omettere l'informativa** di cui all'articolo 13 del Regolamento UE 679/2016, comunicando oralmente all'interessato tale limitazione; o
- **rilasciare un'informativa semplificata** ai sensi dell'articolo 13 del Regolamento UE 679/2016, comunicando oralmente all'interessato tale limitazione;
- **dare istruzioni ai soggetti autorizzati** ai sensi dell'art. 29 del Regolamento UE 679/2016 e 2-quaterdecies del Codice in materia di protezione dei dati personali mediante modalità semplificate, **anche orali**.

Tutti i soggetti di cui sopra procederanno al trattamento dei dati personali secondo la disciplina ordinaria una volta superata l'attuale emergenza sanitaria in corso.



**Le norme data protection del
Protocollo 14 Marzo 2020
Confindustria/Sindacati sulla
“Regolamentazione delle misure
per il contrasto e il contenimento
della diffusione del virus Covid-
19 negli ambienti di lavoro»**



LE NORME DATA PROTECTION DEL PROTOCOLLO 14 MARZO 2020 CONFINDUSTRIA/SINDACATI

In primo luogo il personale, prima dell'accesso al luogo di lavoro **potrà essere sottoposto al controllo della temperatura corporea.**

Se tale temperatura risulterà superiore ai 37,5 non sarà consentito l'accesso ai luoghi di lavoro. Le persone in tale condizione saranno momentaneamente isolate e fornite di mascherine, non dovranno recarsi al Pronto Soccorso e/o nelle infermerie di sede, ma dovranno contattare nel più breve tempo possibile il proprio medico curante e seguire le sue indicazioni.

Il **controllo della temperatura** e **l'acquisizione dei relativi dati personali** del lavoratore sono tuttavia soggetti alle seguenti condizioni di conformità, sia pure in un contesto emergenziale, alla normativa sulla protezione dei dati personali:



LE NORME DATA PROTECTION DEL PROTOCOLLO 14 MARZO 2020 CONFINDUSTRIA/SINDACATI

A. la rilevazione in tempo reale della temperatura corporea costituisce un trattamento di dati personali e, pertanto, deve avvenire ai sensi della disciplina privacy vigente. A tal fine il Protocollo “**suggerisce**” (ma non obbliga) di:

1) rilevare a temperatura e **non registrare** il dato acquisto. È possibile identificare l'interessato e registrare il superamento della soglia di temperatura solo qualora sia necessario a documentare le ragioni che hanno impedito l'accesso ai locali aziendali;

2) di **fornire – anche oralmente - l'informativa** sul trattamento dei dati personali (che potrà eventualmente omettere le informazioni di cui l'interessato sia già in possesso). Quanto ai contenuti dell'informativa, con riferimento alla **finalità del trattamento** potrà essere indicata la prevenzione dal contagio da COVID-19 e con riferimento alla **base giuridica** può essere indicata l'implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020 (che impone a titolari di attività produttive o professionali di implementare protocolli di sicurezza anti-contagio e, laddove non fosse possibile rispettare la distanza interpersonale di un metro come principale misura di contenimento, di adottare strumenti di protezione individuale); con riferimento alla **durata dell'eventuale conservazione** dei dati si può far riferimento al termine dello stato d'emergenza;



LE NORME DATA PROTECTION DEL PROTOCOLLO 14 MARZO 2020 CONFINDUSTRIA/SINDACATI

3) di **definire le misure di sicurezza e organizzative adeguate a proteggere i dati**. In particolare, sotto il profilo organizzativo, occorrerà **individuare i soggetti preposti al trattamento e fornire loro le istruzioni necessarie** (si vedano gli articoli 2-quaterdecies del vigente Codice della privacy, d.lgs. 30 Giugno 2003 no. 196 e 29 e 32 del Regolamento UE 679/2016) . A tal fine, si ricorda che i dati possono essere trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19 e non **devono essere diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative** (es. in caso di richiesta da parte dell’Autorità sanitaria per la ricostruzione della filiera degli eventuali “contatti stretti di un lavoratore risultato positivo al COVID-19);

4) in caso di isolamento momentaneo dovuto al superamento della soglia di temperatura, **assicurare modalità tali da garantire la riservatezza e la dignità del lavoratore**. Tali garanzie devono essere assicurate anche nel caso in cui il lavoratore comunichi all’ufficio responsabile del personale di aver avuto, al di fuori del contesto aziendale, contatti con soggetti risultati positivi al COVID-19 e nel caso di allontanamento del lavoratore che durante l’attività lavorativa sviluppi febbre e sintomi di infezione respiratoria e dei suoi colleghi.




LE NORME DATA PROTECTION DEL PROTOCOLLO 14 MARZO 2020 CONFINDUSTRIA/SINDACATI

B. il datore di lavoro deve informare preventivamente il personale, e chi intende fare ingresso in azienda, della preclusione dell'accesso a chi, negli ultimi 14 giorni, abbia avuto contatti con soggetti risultati positivi al COVID-19 o provenga da zone a rischio secondo le indicazioni dell'OMS. Qualora **si richieda il rilascio di una dichiarazione attestante la non provenienza dalle zone a rischio epidemiologico e l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19**, si ricorda di prestare attenzione alla disciplina sul trattamento dei dati personali, poiché **l'acquisizione della dichiarazione costituisce un trattamento dati**. A tal fine, si applicano le indicazioni di cui alla precedente lettera A, nn.1) - 4) e, nello specifico, il Protocollo "suggerisce" di **raccogliere solo i dati necessari, adeguati e pertinenti rispetto alla prevenzione del contagio da COVID-19**. Ad esempio, se si richiede una dichiarazione sui contatti con persone risultate positive al COVID-19, occorre astenersi dal richiedere informazioni aggiuntive in merito alla persona risultata positiva. Oppure, se si richiede una dichiarazione sulla provenienza da zone a rischio epidemiologico, è necessario astenersi dal richiedere informazioni aggiuntive in merito alle specificità dei luoghi.



LE NORME DATA PROTECTION DEL PROTOCOLLO 14 MARZO 2020 CONFINDUSTRIA/SINDACATI

C. il medico competente segnala all'azienda situazioni di particolare fragilità e patologie attuali o pregresse dei dipendenti e l'azienda provvede alla loro tutela nel rispetto della privacy il medico competente applicherà le indicazioni delle Autorità Sanitarie.



Le indicazioni sul trattamento dei dati personali nel contesto emergenziale COVID-19 emanate dal Comitato Europeo per la protezione dei dati personali.



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Nel primo **Statement 1/2020** rilasciato il 16 Marzo 2020 dal presidente del Comitato Europeo per la Protezione dei dati personali (CEPD), cioè di quell'organismo previsto dall'articolo 68 del RGPD che riunisce i rappresentanti nazionali delle Autorità per la protezione dei dati personali degli Stati membri, il Garante Europeo per la protezione dei dati Personali (EDPS) e i rappresentanti della Commissione UE (dunque il vertice europeo massimo delle istituzioni *data protection*) il CEPD ricorda che le **norme poste a protezione dei dati personali non impediscono od ostacolano le misure emergenziali che gli Stati stanno attuando per combattere il diffondersi dell'epidemia di COVID-19.**

Tuttavia, anche in tempi eccezionali come questi – ricorda il CEPD – i titolari del trattamento devono assicurare la protezione dei dati personali degli interessati.



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Ciò può tuttavia avvenire in un contesto – come quello ad ampio spettro del RGPD – **che reca in sé le regole per gestire i dati anche nella presente emergenza**, fornendo la base di legittimità del trattamento che – ad esempio – **autorizza i datori di lavoro e le autorità pubbliche competenti a trattare dati personali nel contesto dell’epidemia senza la necessità di dover ottenere il consenso dei soggetti interessati**.

Ciò ad esempio si applica – ricorda sempre il CEPD nel suo comunicato – quando i datori di lavoro devono procedere al trattamento dei dati dei lavoratori necessario per **ragioni di pubblico interesse nel settore della sanità pubblica o devono proteggere un interesse vitale o devono conformarsi a prescrizioni contenute nelle leggi**.



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

In maniera più articolata, in un secondo **Statement 2/2020** rilasciato il 20 Marzo 2020, il CEPD dettaglia come segue la posizione già evidenziata nel primo Comunicato:

1. Liceità del trattamento

Il regolamento generale sulla protezione dei dati (RGPD) è una normativa di ampia portata e contiene disposizioni che si applicano anche al trattamento dei dati personali in un contesto come quello relativo al COVID-19. **Il RGPD consente alle competenti autorità sanitarie pubbliche e ai datori di lavoro di trattare dati personali** nel contesto di un'epidemia, conformemente al diritto nazionale e alle condizioni ivi stabilite. Ad esempio, se il trattamento è necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica. In tali circostanze, non è necessario basarsi sul consenso dei singoli.



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Per quanto riguarda il trattamento dei dati personali, comprese le categorie particolari di dati, da parte di autorità pubbliche competenti (ad es. autorità sanitarie pubbliche), il Comitato ritiene che **gli articoli 6 e 9 del RGPD consentano tale trattamento**, in particolare quando esso ricada nell'ambito delle competenze che il diritto nazionale attribuisce a tale autorità pubblica e nel rispetto delle condizioni sancite dal RGPD.

Nel contesto lavorativo, il trattamento dei dati personali può essere necessario per **adempiere un obbligo legale** al quale è soggetto il datore di lavoro, per esempio in materia di salute e sicurezza sul luogo di lavoro o per il perseguimento di un interesse pubblico come il controllo delle malattie e altre minacce di natura sanitaria. Il RGPD prevede anche deroghe al divieto di trattamento di talune categorie particolari di dati personali, come i dati sanitari, se ciò è necessario **per motivi di interesse pubblico rilevante nel settore della sanità pubblica** (articolo 9.2, lettera i), sulla base del diritto dell'Unione o nazionale, o laddove vi sia la necessità di **proteggere gli interessi vitali dell'interessato** (articolo 9.2.c), poiché il considerando 46 fa esplicito riferimento al controllo di un'epidemia.



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Per quanto riguarda il trattamento dei dati delle telecomunicazioni, come i dati relativi all'ubicazione, devono essere rispettate anche le leggi nazionali di attuazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva e-privacy). **In linea di principio, i dati relativi all'ubicazione possono essere utilizzati dall'operatore solo se resi anonimi o con il consenso dei singoli.** Tuttavia, **l'articolo 15 della direttiva e-privacy** consente agli Stati membri di introdurre misure legislative per salvaguardare la sicurezza pubblica. Tale legislazione eccezionale è possibile solo se costituisce una misura necessaria, adeguata e proporzionata all'interno di una società democratica. Tali misure devono essere conformi alla Carta dei diritti fondamentali e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Inoltre, esse sono soggette al controllo giurisdizionale della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo. **In presenza di situazioni di emergenza, le misure in questione devono essere rigorosamente limitate alla durata dell'emergenza.**



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Principi fondamentali relativi al trattamento dei dati personali

I dati personali necessari per conseguire gli obiettivi perseguiti dovrebbero essere trattati per finalità specifiche ed esplicite.

Inoltre, gli **interessati dovrebbero ricevere informazioni trasparenti sulle attività di trattamento svolte e sulle loro caratteristiche principali, compreso il periodo di conservazione dei dati raccolti e le finalità del trattamento**. Le informazioni dovrebbero essere facilmente accessibili e formulate in un linguaggio semplice e chiaro.

È importante adottare **adeguate misure di sicurezza** e riservatezza che garantiscano che i dati personali non siano divulgati a soggetti non autorizzati. **Si dovrebbero documentare in misura adeguata le misure messe in campo per gestire l'attuale emergenza e il relativo processo decisionale.**



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Uso dei dati di localizzazione da dispositivi mobili

- *I governi degli Stati membri possono utilizzare i dati personali relativi ai telefoni cellulari dei singoli nell'intento di monitorare, contenere o attenuare la diffusione del COVID-19?*

In alcuni Stati membri i governi prevedono di utilizzare i dati di localizzazione da dispositivi mobili per monitorare, contenere o attenuare la diffusione del COVID-19. Ciò implicherebbe, ad esempio, la possibilità di geolocalizzare le persone o di inviare messaggi di sanità pubblica ai soggetti che si trovano in una determinata area, via telefono o SMS. Le autorità pubbliche dovrebbero innanzitutto cercare di trattare i dati relativi all'ubicazione **in modo anonimo** (ossia, trattare dati in forma aggregata e tale da non consentire la successiva re-identificazione delle persone), il che potrebbe permettere di generare analisi sulla concentrazione di dispositivi mobili in un determinato luogo ("**cartografia**").



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Le norme in materia di protezione dei dati personali **non si applicano** ai dati che sono stati adeguatamente **anonimizzati**.

Quando non è possibile elaborare solo dati anonimi, la direttiva e-privacy consente agli Stati membri di introdurre misure legislative per salvaguardare la sicurezza pubblica (articolo 15).

Qualora siano introdotte misure che consentono il trattamento dei dati di localizzazione in forma non anonimizzata, **lo Stato membro ha l'obbligo di predisporre garanzie adeguate, ad esempio fornendo agli utenti di servizi di comunicazione elettronica il diritto a un ricorso giurisdizionale.**



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Si applica anche il principio di proporzionalità. Si dovrebbero sempre privilegiare le soluzioni meno intrusive, tenuto conto dell'obiettivo specifico da raggiungere.

Misure invasive come il "tracciamento" (ossia il trattamento di dati storici di localizzazione in forma non anonimizzata) **possono essere considerate proporzionate in circostanze eccezionali e in funzione delle modalità concrete del trattamento.**

Tuttavia, tali misure dovrebbero essere soggette a un **controllo rafforzato e a garanzie più stringenti** per assicurare il rispetto dei principi in materia di protezione dei dati (proporzionalità della misura in termini di durata e portata, ridotta conservazione dei dati, rispetto del principio di limitazione della finalità).



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Contesto lavorativo

- ***Un datore di lavoro può chiedere ai visitatori o ai dipendenti di fornire informazioni sanitarie specifiche nel contesto del COVID-19?***

Nel caso di specie, è particolarmente pertinente l'applicazione dei principi di proporzionalità e di minimizzazione dei dati. Il datore di lavoro dovrebbe chiedere informazioni sanitarie soltanto nella misura consentita dal diritto nazionale.

- ***Il datore di lavoro è autorizzato a effettuare controlli medici sui dipendenti?***

La risposta dipende dalle leggi nazionali in materia di lavoro o di salute e sicurezza. I datori di lavoro dovrebbero accedere ai dati sanitari e trattarli solo se ciò sia previsto dalle rispettive norme nazionali.



LE INDICAZIONI SU DATA PROTECTION E COVID-19 DEL CEPD/EDPB

Il datore di lavoro può informare colleghi o soggetti esterni del fatto che un dipendente è affetto dal COVID-19?

I datori di lavoro dovrebbero informare il personale sui casi di COVID-19 e adottare misure di protezione, ma non dovrebbero comunicare più informazioni del necessario. Qualora occorra indicare il nome del dipendente o dei dipendenti che hanno contratto il virus (ad esempio, in un contesto di prevenzione) e il diritto nazionale lo consenta, **i dipendenti interessati ne sono informati in anticipo tutelando la loro dignità e integrità.**

Quali informazioni trattate nel contesto del COVID-19 possono essere ottenute dai datori di lavoro?

I datori di lavoro possono ottenere informazioni personali nella misura necessaria ad adempiere ai loro obblighi e a organizzare le attività lavorative, conformemente alla legislazione nazionale.



**Le FAQ del Garante privacy sul
trattamento dei dati sanitari dei
lavoratori**



LE FAQ DEL GARANTE PRIVACY SUL TRATTAMENTO DEI DATI DEI LAVORATORI

Il datore di lavoro può comunicare al Rappresentante dei lavoratori per la sicurezza l'identità dei dipendenti contagiati?

I datori di lavoro, nell'ambito dell'adozione delle misure di protezione e dei propri doveri in materia di sicurezza dei luoghi di lavoro, non possono comunicare il nome del dipendente o dei dipendenti che hanno contratto il virus a meno che il diritto nazionale lo consenta.

In base al quadro normativo nazionale il datore di lavoro deve comunicare i nominativi del personale contagiato alle autorità sanitarie competenti e collaborare con esse per l'individuazione dei "contatti stretti" al fine di consentire la tempestiva attivazione delle misure di profilassi.

Tale obbligo di comunicazione non è, invece, previsto in favore del Rappresentante dei lavoratori per la sicurezza, né i compiti sopra descritti rientrano, in base alle norme di settore, tra le specifiche attribuzioni di quest'ultimo.

Il Rappresentante dei lavoratori per la sicurezza, proprio nella fase dell'attuale emergenza epidemiologica, dovrà continuare a svolgere i propri compiti consultivi, di verifica e di coordinamento, offrendo la propria collaborazione al medico competente e al datore di lavoro (ad esempio, promuovendo l'individuazione delle misure di prevenzione più idonee a tutelare la salute dei lavoratori nello specifico contesto lavorativo; aggiornando il documento di valutazione dei rischi; verificando l'osservanza dei protocolli interni).

Il Rappresentante dei lavoratori per la sicurezza quando nell'esercizio delle proprie funzioni venga a conoscenza di informazioni - che di regola tratta in forma aggregata ad es. quelle riportate nel documento di valutazione dei rischi - rispetta le disposizioni in materia di protezione dei dati nei casi in cui sia possibile, anche indirettamente, l'identificazione di taluni interessati



LE FAQ DEL GARANTE PRIVACY SUL TRATTAMENTO DEI DATI DEI LAVORATORI


Può essere resa nota l'identità del dipendente affetto da Covid-19 agli altri lavoratori da parte del datore di lavoro?

No. In relazione al fine di tutelare la salute degli altri lavoratori, in base a quanto stabilito dalle misure emergenziali, spetta alle autorità sanitarie competenti informare i “contatti stretti” del contagiato, al fine di attivare le previste misure di profilassi.

Il datore di lavoro è, invece, tenuto a fornire alle istituzioni competenti e alle autorità sanitarie le informazioni necessarie, affinché le stesse possano assolvere ai compiti e alle funzioni previste anche dalla normativa d'urgenza adottata in relazione alla predetta situazione emergenziale (cfr. paragrafo 12 del predetto Protocollo).

La comunicazione di informazioni relative alla salute, sia all'esterno che all'interno della struttura organizzativa di appartenenza del dipendente o collaboratore, può avvenire esclusivamente qualora ciò sia previsto da disposizioni normative o disposto dalle autorità competenti in base a poteri normativamente attribuiti (es. esclusivamente per finalità di prevenzione dal contagio da Covid-19 e in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali “contatti stretti di un lavoratore risultato positivo”).

Restano ferme le misure che il datore di lavoro deve adottare in caso di presenza di persona affetta da Covid-19, all'interno dei locali dell'azienda o dell'amministrazione, relative alla pulizia e alla sanificazione dei locali stessi, da effettuarsi secondo le indicazioni impartite dal Ministero della salute.



Un caso pratico: se il dipendente di un'azienda risulta positivo al COVID-19, si può effettuare una comunicazione a tutti i dipendenti dell'azienda mettendoli a conoscenza della circostanza (e identificando il collega positivo)?



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Approfondiamo un caso pratico per rispondere alla domanda e indicare ai datori di lavoro-titolari del trattamento quali scelte intraprendere e su quali basi normative nel contesto delle norme emergenziali sopra indicate (e nel contesto “ordinario” della normale applicabilità del RGPD) per affrontare una situazione del genere.

Inviare a dipendenti con i quali il lavoratore positivo al COVID-19 è entrato in contatto una comunicazione contenente i dati identificativi di quest'ultimo è tecnicamente una **“comunicazione”** di dati personali ai sensi dell'art. **2-ter** del Codice della privacy (cfr. articolo 2-ter, comma 4, che dispone che per “comunicazione” si intende il “dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione”).



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Come ogni trattamento, anche questa comunicazione - indipendentemente dalle modalità (es: email, ricordando che nel **contesto lavorativo** devono comunque essere **privilegiate comunicazioni individuali** quando aventi ad oggetto dati di particolare natura) – deve fondarsi su **una idonea base di legittimità**, che nel contesto emergenziale che stiamo vivendo deve ovviamente coordinarsi, appunto, con le norme emergenziali emanate applicabili alla vostra situazione particolare. **Trattasi inoltre di comunicazione avente ad oggetto dati di particolare natura sub specie dati sanitari** (cfr. art. 4, n. 15 del Regolamento 679/2016, *«dati relativi alla salute»*): i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute”.


Quando parliamo di **“dati di particolare natura”**, viene in considerazione – come regola generale – il divieto di trattamento di cui all’articolo 9, comma 1 del Regolamento 679/2016:



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona”.

Solo ove siano applicabili una o più deroghe a tale divieto tra quelle elencate al successivo comma 2 dell'articolo 9, il trattamento dei dati di particolare natura potrà risultare lecito.



La comunicazione ai colleghi dei dati sanitari (afezione da COVID-19) del lavoratore in stato di incoscienza (terapia intensiva).



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Nel caso pratico in esame una circostanza di fatto che può costituire una discriminante nell'ottica del fondamento di legittimità del trattamento è **l'eventuale stato fisico del lavoratore positivo al COVID-19.**

Difatti, ove **fosse accertata la sua impossibilità fisica** a prestare il consenso, sarebbe applicabile come deroga al divieto di trattamento la ipotesi elencata all'articolo 9, comma 2, lettera c) del Regolamento 679/2016:

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO


Tale ipotesi vedrebbe il datore di lavoro e titolare del trattamento valutare come “vitali” gli interessi sanitari dei dipendenti entrati in contatto con il lavoratore (le “altre persone fisiche”). “Vitali” in quanto non avvertirli o attendere le procedure di comunicazione del datore alle competenti autorità sanitarie che sono le uniche deputate a trattare i dati e ad intervenire presso tali lavoratori a rischio, ricostruendone la “catena dei contatti”, rischierebbe di far perdere tempo prezioso o potrebbe in teoria anche fondare responsabilità ex art. 438 c.p.

Dunque, nel caso il lavoratore positivo al COVID-19 non possa prestare il consenso per impossibilità fisica, il datore di lavoro potrebbe legittimamente procedere come sopra indicato. Ciò è d'altra parte coerente sia con il dettato normativo richiamato, sia con le indicazioni del CEPD sopra riportate.



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

In questo caso, ovviamente, la comunicazione dovrebbe altresì essere conforme a tutti gli altri **principi di cui all'articolo 5 del Regolamento 679/2016** (ad esempio, il principio di proporzionalità imporrebbe una **precomunicazione mirata ai soli colleghi che siano realmente a rischio** gressi contatti, essendo eccedente una comunicazione indifferenziata a tutti i lavoratori, anche a quelli che a seguito di una valutazione oggettiva non siano entrati in contatto con il dipendente positivo o non corrano rischi reali di infezione).



**La comunicazione ai colleghi dei
dati sanitari (afezione da COVID-19)
del lavoratore cosciente.**



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Nella diversa ipotesi in cui il lavoratore positivo al COVID-19 sia cosciente, va valutato il quadro delle regole emergenziali in materia di trattamento dei dati sanitari per poter dare una risposta in base al quadro fattuale diverso, ora oggetto di valutazione.

Una prima considerazione attiene all'articolo 14 del decreto legge 9 Marzo 2020, alla cui illustrazione sopra effettuata si rinvia. Secondo tale norma – come si è visto - i soggetti pubblici autorizzati ad operare nell'ambito del Sistema Nazionale di Protezione Civile, il Ministro della Salute, l'Istituto Superiore della Sanità, gli enti pubblici e privati operanti nell'ambito del Sistema Sanitario Nazionale e i soggetti preposti al controllo delle misure di emergenza già emanate **possono trattare i dati personali, anche mediante interscambio e comunicazione reciproca di dati (sia sanitari che relativi a reati per eventuali violazioni delle misure di emergenza).**



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Invece tutti gli altri soggetti privati diversi da quelli sopra individuati possono procedere alla comunicazione e alla diffusione dei soli dati personali comuni (esclusi quindi i dati sanitari e i dati relativi ai reati) a soggetti **pubblici e privati diversi dai soggetti pubblici autorizzati** ad operare nell'ambito del Sistema Nazionale di Protezione Civile, il Ministro della Salute, l'Istituto Superiore della Sanità, gli enti pubblici e privati che operano nell'ambito del Sistema Sanitario Nazionale è autorizzata, **ove indispensabile, nell'ambito della gestione dell'emergenza sanitaria in corso.**

In base a questa **disciplina speciale emergenziale** emergerebbe che un soggetto quale una società privata datrice di lavoro non sia autorizzato alla comunicazione o alla diffusione di dati personali di particolare natura, essendo autorizzato a comunicare e diffondere - eventualmente – solo dati personali comuni.



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Interviene però questione interpretativa, che potrebbe portare ad una conclusione di segno opposto a quella appena proposta dalla mera lettura dell'articolo 17-bis, comma 2 del d.l. 18/2020 (e cioè che i privati possono in via di emergenza procedere a comunicare e diffondere a soggetti pubblici e privati diversi da quelli sanitari i soli dai personali comuni, adottando tale emergenza e l'articolo 14 del decreto legge quale base di legittimità del trattamento).

E' una lettura orientata dell'articolo 17-bis, comma 2, del decreto legge:

*“2. La comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli di cui al comma 1, **nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del regolamento (UE) 2016/679**, è effettuata, nei casi in cui risulti indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto”.*



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Se esaminiamo **l'inciso tra le due virgole sopra evidenziato**, una non irragionevole lettura interpretativa potrebbe portare alla conclusione che:

- **la comunicazione dei “dati personali”** (dunque anche di quelli di particolare natura, sanitari inclusi) a soggetti privati (es: i dipendenti del nostro datore di lavoro) e pubblici diversi da quelli autorizzati dal comma 1 dell'art. 17-bis è consentita nei casi in cui risulti indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto; mentre
- **la diffusione dei dati** (che è in se stessa operazione più delicata della comunicazione, in quanto – sempre ai sensi dell'articolo 2-ter del Codice della privacy – consiste nel “dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione”), sarebbe consentita solo con riferimento dati comuni.



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Con la conseguenza che una tale lettura interpretativa consentirebbe al datore di lavoro privato di procedere alla detta comunicazione emergenziale ove appunto come datore di lavoro gli *“risultati indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto”*. **Ovviamente, anche in questo caso, sarebbe comunque applicabile – anche nel contesto emergenziale – il comma 3 dell'articolo 17-bis decreto legge 17 marzo 2020 n. 18:** *“I trattamenti di dati personali di cui ai commi 1 e 2 sono effettuati nel rispetto dei principi di cui all'articolo 5 del citato regolamento (UE) 2016/679, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati”*.

L'adozione di **adeguate misure di tutela dell'interessato è comunque e sempre una preconditione di liceità del trattamento** anche ove consentito in via eccezionale come nel contesto sopra delineato. Anche il contesto emergenziale – in altri termini – in assenza delle adeguate misure organizzative di gestione della comunicazione **non sarebbe da solo sufficiente a fondare la legittimità del trattamento.**




CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

La lettura interpretativa sopra proposta, tra l'altro, e l'apertura possibilista alla comunicazione dei dati nella cornice di garanzie **appare costituzionalmente orientata nel senso lavoristico**. Difatti, il fondamento giuridico di tipo non data protection ma di tipo lavoristico sarebbe altresì rinvenibile nell'art. 2087 c.c. : *“l'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro”*.



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

L'articolo 2087 c.c. ha un elevato dinamismo applicativo, poiché tutela la salute dei lavoratori. A ciò si aggiunga che ogni norma ordinaria deve essere applicata secondo una lettura costituzionalmente orientata. Nel caso di specie, l'imprenditore, nello scegliere le misure necessarie a tutelare la salute dei lavoratori, deve anche valutare un altro **diritto costituzionale e cioè la salute dei cittadini.** Ora, volendo operare una gradazione dei diritti ed interessi in gioco, la privacy del dipendente positivo al COVID 2019 non può avere valore costituzionale primario rispetto alla salute dei lavoratori e dei familiari e, di conseguenza, della comunità. Con la conseguenza che in casi come questo **i datori di lavoro possono adottare la misura ritenuta più necessaria, secondo le valutazioni rese anche dal Medico Competente e dal Responsabile della Sicurezza e Prevenzione RSPP, per applicare l'art. 2087 e tutelare la salute dei lavoratori e di conseguenza la salute pubblica.**



La comunicazione ai colleghi dei dati sanitari (afezione da COVID-19) del lavoratore nella prospettiva dei “*motivi di interesse pubblico rilevante*”.



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

L'articolo **9, comma 2, lettera (g) del Regolamento 679/2016** come integrato in sede nazionale dall'articolo **2-sexies, comma 1, del vigente d.lgs. 30 Giugno 2003, n. 196 coordinato al RGPD** prevede che il trattamento dei dati di particolare natura (ivi inclusi quelli sanitari) è consentito in deroga al divieto generale di trattamento di cui all'articolo 9, comma 1, RGPD se è *“necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato”*. L'articolo 2-sexies, comma 1, del Codice della privacy (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante) prevede poi che:



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato”.



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Ora, certamente tali norme sono per lo più destinate a soggetti pubblici che perseguono nello svolgimento delle loro attività istituzionali interessi pubblici rilevanti o svolgono compiti di interesse pubblico o sono destinatari di poteri di natura pubblicistica, ma un “*interesse pubblico rilevante*”- soprattutto in un contesto emergenziale - può ben essere perseguito anche da un soggetto privato come una azienda. Se non è irragionevole una tale conclusione, allora se ne deve trarre la **conseguenza che comunicare dati personali sanitari a terzi è legittimo se previsto dall’ordinamento nazionale con norme che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato: tutte condizioni che a ben vedere l’articolo 17-bis, commi 2 e comma 3 del decreto legge 18/2020 appunto prevede nello specifico**



CASO PRATICO: COMUNICAZIONE AI COLLEGHI DEI DATI DI UN DIPENDENTE COVID-19 POSITIVO

Infine, una lettura non approfondita del Protocollo Sindacati/Confindustria potrebbe portare alla conclusione che la comunicazione dei dati che il datore di lavoro si trovi nella necessità di dover fare sia vietata dagli accordi.

In realtà, a ben leggere, gli accordi di cui al Protocollo:

1. richiamano la legittimità di tutte le misure aziendali volte alla implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. 1, n. 7, lett. d) del DPCM 11 marzo 2020 (e dunque avvertire i lavoratori che sono stati a contatto con il dipendente positivo potrebbe essere una comunicazione nella cornice dei protocolli – non solo sanitari - anti-contagio cui ogni datore di lavoro è in questo periodo tenuto);
2. specificano che i dati possono essere trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19 (che sarebbe finalità comune alla comunicazione che il datore di lavoro intenderebbe effettuare) e non devono essere diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (ma le “specifiche previsioni normative” possono ben essere rappresentate dalla lettura interpretativa dell'articolo 14, comma 2 del decreto legge 14/2020 che vieta solo la “diffusione” dei dati sanitari, ma non anche la comunicazione a terzi soggetti privati quali sarebbero i dipendenti da avvertire).



Tonucci & Partners

Per approfondimenti:

Prof. Avv. Alessandro del Ninno

Email: adelninno@tonucci.com

WWW: www.alessandrodelninno.it