ENGLISH VERSION (https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en)

Comitato europeo per la protezione dei dati - EDPB

Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19

Adottata il 19 marzo 2020

Il comitato europeo per la protezione dei dati ha adottato la seguente dichiarazione:

Governi e organismi pubblici e privati di tutta Europa stanno adottando misure per contenere e attenuare il COVID-19. Ciò può comportare il trattamento di diverse tipologie di dati personali.

Le norme in materia di protezione dei dati (come il regolamento generale sulla protezione dei dati) non ostacolano l'adozione di misure per il contrasto della pandemia di coronavirus. La lotta contro le malattie trasmissibili è un importante obiettivo condiviso da tutte le nazioni e, pertanto, dovrebbe essere sostenuta nel miglior modo possibile. È nell'interesse dell'umanità arginare la diffusione delle malattie e utilizzare tecniche moderne nella lotta contro i flagelli che colpiscono gran parte del mondo. Il Comitato europeo per la protezione dei dati desidera comunque sottolineare che, anche in questi momenti eccezionali, titolari e responsabili del trattamento devono garantire la protezione dei dati personali degli interessati. Occorre pertanto tenere conto di una serie di considerazioni per garantire la liceità del trattamento di dati personali e, in ogni caso, si deve ricordare che qualsiasi misura adottata in questo contesto deve rispettare i principi generali del diritto e non può essere irrevocabile. L'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza.

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.

1.1 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.

1.2 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.

1.3 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.

2. 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.

3. 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 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**.

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).

4. 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.

• 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.

Per il Comitato europeo per la protezione dei dati
La presidente
(Andrea Jelinek)