



Gestione della privacy da parte degli enti locali in situazioni di emergenza (Covid-19)

A domanda risponde Avv. Michele IASELLI

30 marzo 2020 - dalle ore 11.30 alle 12.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione degli Enti Locali

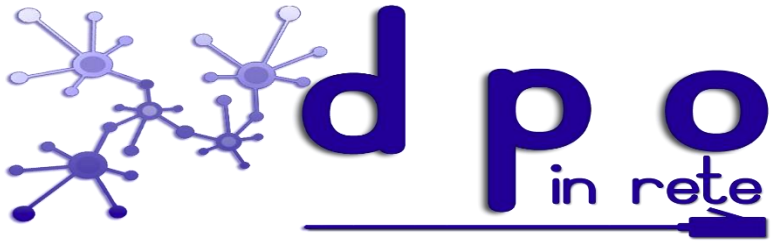
Email info@dpointrete.it

Numero Verde 800.16.56.54

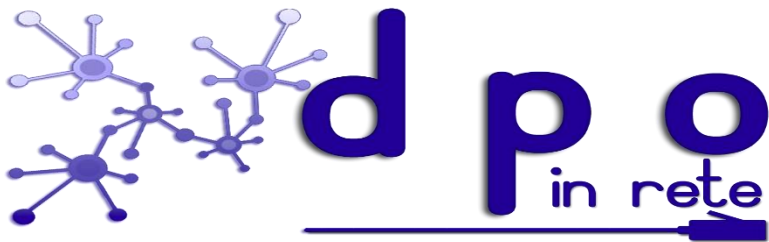
Web: www.dpointrete.it

www.asmel.eu





I dati sanitari



Il binomio Privacy - Sanità da sempre presenta non poche difficoltà, sia per la rilevanza dei principi da tutelare, tutti di rango costituzionale, sia per l'approccio non sempre agevole degli operatori sanitari alle tematiche proprie della protezione dei dati personali. L'avvento poi della sanità digitale, voluta innanzitutto dall'Europa, ha ulteriormente complicato la situazione.



La stessa applicazione della normativa in materia di trattamento dei dati personali e sensibili nel settore sanitario è sempre stata controversa: la giusta imposizione di norme e regole atte a tutelare la riservatezza della persona umana spesso appare in contrasto con le esigenze di celerità, di urgenza, di garanzia di salute del paziente e quasi una inutile aggiunta alle già numerose incombenze di carattere burocratico che toccano agli operatori sanitari.



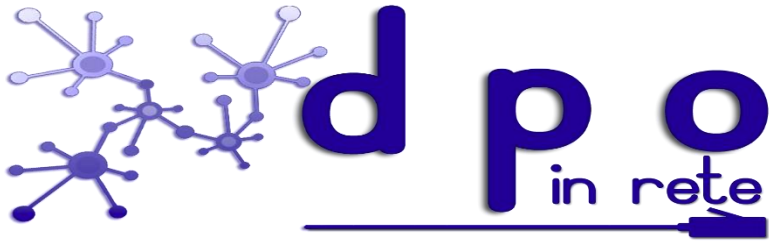
Gradualmente il senso della normativa sulla privacy è stato, tuttavia, compreso e importanti modifiche, soprattutto nei comportamenti hanno visto la luce nelle strutture sanitarie, che oggi mostrano una maggiore attenzione all'aspetto umano, alla dignità delle persone, alla riservatezza.



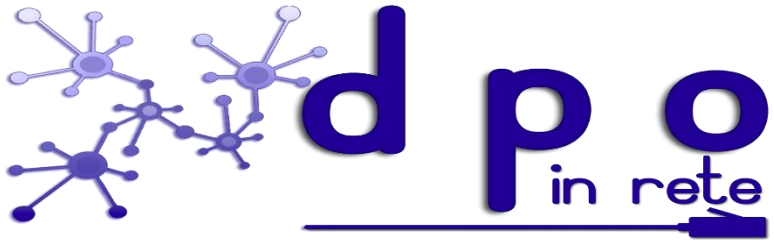
Naturalmente diverse sono le zone d'ombra negli aspetti applicativi, e sotto la vigenza della precedente direttiva 95/46/CE, il D.Lgs. n. 196/2003 agli artt. da 75 a 94, raccogliendo ed integrando nel titolo V, particolarmente dedicato ai dati sensibili, le varie disposizioni ha fornito alcune risposte alle perduranti incertezze del mondo sanitario.



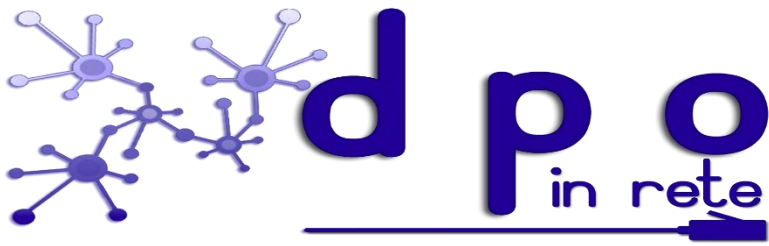
Il nostro codice in merito alla materia sanitaria (ma ciò vale anche per altre materie) ha quindi adottato un approccio di carattere settoriale e, partendo dal presupposto fondamentale rappresentato dall'art. 8, par. 3 della direttiva 95/46/CE che disciplinava i dati sanitari, ha dettato norme specifiche in materia.



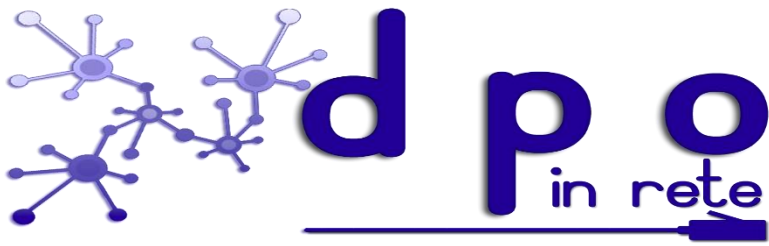
Come sappiamo, poi, è sopraggiunto il Regolamento UE n. 2016/679 (GDPR) ed il decreto di adeguamento n. 101/2018.



Definizione di dato sanitario



In realtà il Regolamento comunitario sulla protezione dei dati personali n. 2016/679 non prevede una disciplina specifica per il trattamento dei dati personali effettuato in ambito sanitario al di là di riferimenti specifici relativi all'applicazione di alcune norme o istituti.



Naturalmente la materia è oggetto di particolare attenzione da parte del legislatore comunitario e lo dimostra il considerando 35 dove si chiarisce che *“nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro”*.



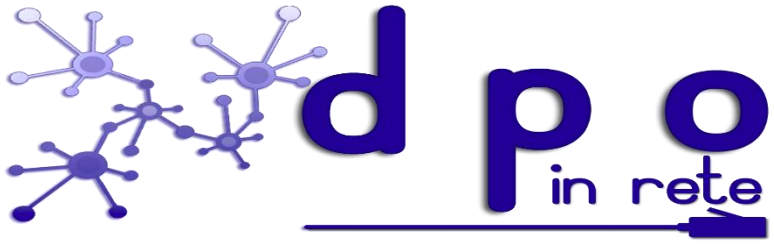
Una definizione estremamente completa e dettagliata sintetizzata in qualche modo dall'art. 4, n. 15 del GDPR che per dati relativi alla salute intende: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.



In ragione della loro natura, i dati sanitari sono qualificati dal GDPR, in linea con quanto già previsto dalla Direttiva madre, come una particolare categoria di dati e, quindi, come meritevoli di una specifica protezione sotto il profilo dei diritti e delle libertà fondamentali. Tuttavia, a differenza della Direttiva madre, il Regolamento ricomprende nella definizione di questi dati anche i dati genetici e quelli biometrici, il cui Trattamento, come quello dei dati sanitari, può esser soggetto a condizioni e/o limitazioni ulteriori, liberamente mantenute o introdotte dai singoli Stati membri.



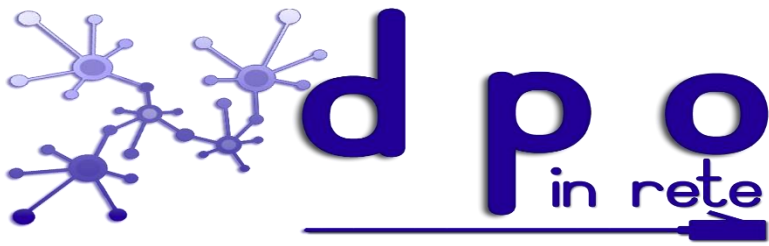
In verità secondo la nostra Cassazione, tutte le volte che si parla di dati riguardanti la salute ed il sesso degli interessati, detti dati sono “supersensibili” in quanto sono involgenti la parte più intima della persona nella sua corporeità e nelle sue convinzioni psicologiche più riservate. Pertanto, essi beneficiano di una protezione rafforzata (Cass. civ., sez. VI, sent. del 11 gennaio 2016, n. 222; sez. I, sent. del 7 ottobre 2014, n. 21107; sez. I, sent. 1 agosto 2013, n. 18443; sent. 8 luglio 2005, n. 14390).



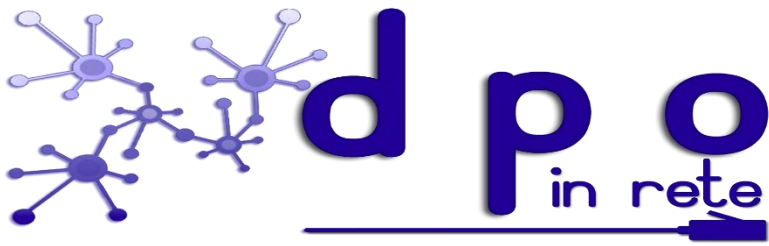
Il trattamento dei dati sanitari



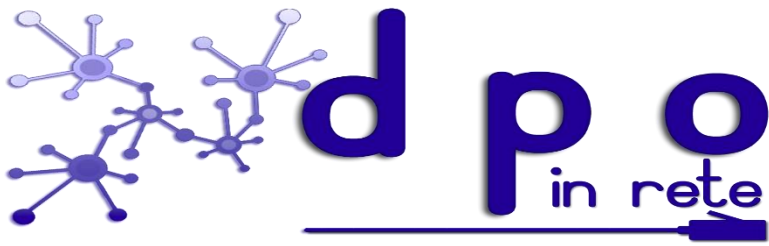
L'art. 9 del GDPR sancisce come principio di carattere generale il divieto di trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.



Il divieto non opera in una serie di circostanze che, per il settore sanitario, sono riconducibili all'erogazione della prestazione sanitaria complessivamente intesa. Tuttavia, il Regolamento è più flessibile ed amplia, rispetto alla Direttiva madre, il novero di ipotesi che legittimano il trattamento dei dati sanitari.



Si pensi all'ipotesi in cui il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri.

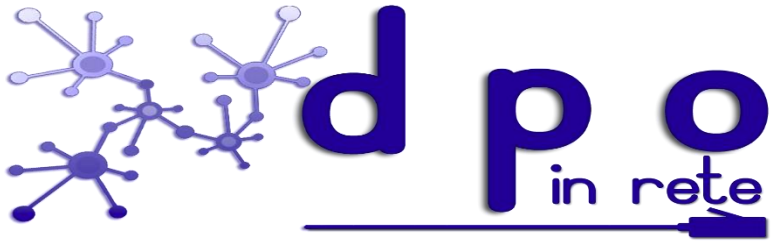


Oltre al caso più tradizionale in cui il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici.



Proprio in quest'ultimo caso si nota anche un approccio più ampio del GDPR rispetto alla materia sanitaria in quanto identifica esplicitamente il perseguimento dell'interesse pubblico nel settore della sanità pubblica quale giustificazione dell'inapplicabilità del divieto ex art. 9, par. 1, del GDPR.

Tale menzione esplicita va a vantaggio dei nuovi modelli di cura integrati e di gestione ospedaliera (ad esempio, ACO, i servizi di *medical* ed *health home*), nonché dei soggetti pubblici che, nell'ambito dell'erogazione dei servizi sanitari e dell'acquisto di prodotti medico-sanitari, assumono il ruolo di stazioni appaltanti.

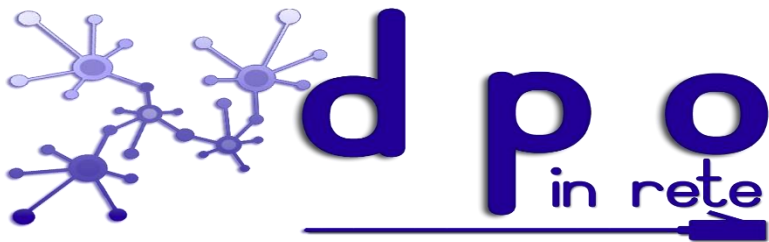


La situazione di emergenza (Covid-19)



Inevitabilmente il sorgere di una situazione particolarmente allarmante come quella attuale a seguito della pandemia da coronavirus cambia l'equilibro dei due valori di rilevanza costituzionale che vengono in conflitto e cioè il diritto alla riservatezza ed il diritto alla salute.

Ma ovviamente è necessaria una base normativa che giustifichi il trattamento dei dati sanitari in questo particolare periodo. E l'Italia in questo non è seconda a nessuno.

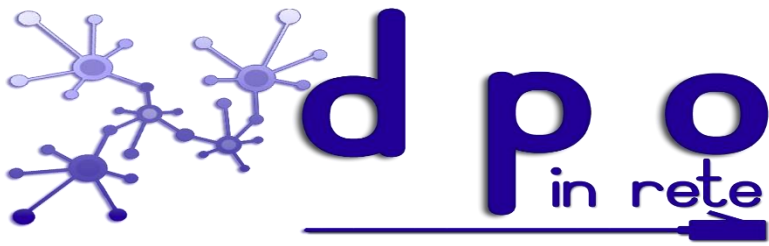


L'art. 14 del DL n. 14/2020 ha subito fornito le adeguate basi di liceità del trattamento richiamando le disposizioni del GDPR.

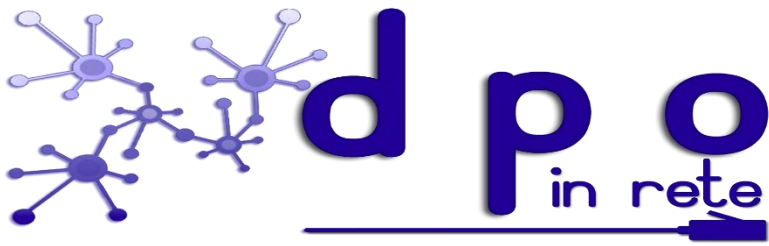
In particolare al 1° comma ha sancito che *«fino al termine dello stato di emergenza deliberato dal Consiglio dei ministri in data 31 gennaio 2020, per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del COVID-19 mediante adeguate misure di profilassi, nonché per assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Servizio sanitario nazionale, nel rispetto dell'articolo 9, paragrafo 2, lettere g) , h) e i) , e dell'articolo 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, nonché dell'articolo 2-sexies , comma 2, lettere t) e u), del decreto legislativo 30 giugno 2003, n. 196, i soggetti operanti nel Servizio nazionale di protezione civile, di cui agli articoli 4 e 13 del decreto legislativo 2 gennaio 2018, n. 1, e i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile 3 febbraio 2020, n. 630, nonché gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'articolo 3 del decreto-legge 23 febbraio 2020, n. 6, convertito, con modificazioni, dalla legge 5 marzo 2020, n. 13, 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 attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19».*



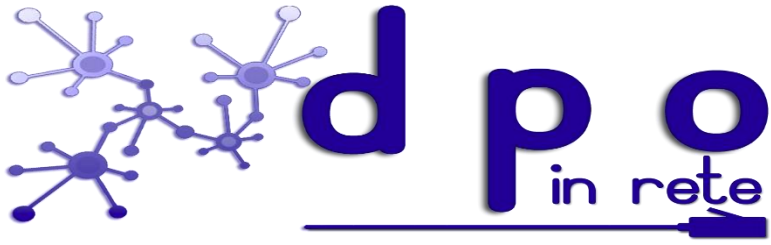
La medesima disposizione chiarisce che la comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli di cui al comma 1, nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del regolamento (UE) 2016/679, è effettuata, nei casi in cui risulti indispensabile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



L'art. 14 opera altri due richiami fondamentali all'art. 5 del GDPR come principi generali da rispettare ed all' 2-quaterdecies del d.lgs. n. 196/2003 per soddisfare la necessità di contemperare le esigenze di gestione dell'emergenza sanitaria in atto con quella afferente alla salvaguardia della riservatezza degli interessati, prevedendo un regime semplificato per le autorizzazioni di sorta.



Addirittura al comma 5 l'art. 14 prevede che nel contesto emergenziale in atto, ai sensi dell'articolo 23, paragrafo 1, lettera e) , del GDPR, fermo restando quanto disposto dall'articolo 82 del decreto legislativo 30 giugno 2003, n. 196, i soggetti di cui al comma 1 possono omettere l'informativa di cui all'articolo 13 del medesimo regolamento o fornire una informativa semplificata, previa comunicazione orale agli interessati della limitazione.



Il protocollo condiviso di regolazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro del 14 marzo 2020



Come noto il documento è stato realizzato per agevolare gli enti e le imprese nell'adozione di protocolli di sicurezza anti-contagio, ovvero sia Protocollo di regolamentazione per il contrasto e il contenimento della diffusione del virus COVID 19 negli ambienti di lavoro, ma contiene importanti disposizioni anche in materia di privacy.



Difatti la rilevazione in tempo reale della temperatura corporea costituisce un trattamento di dati personali e, pertanto, deve avvenire ai sensi della disciplina privacy vigente. Per questo motivo vengono suggerite tutta una serie di precauzioni da adottare.



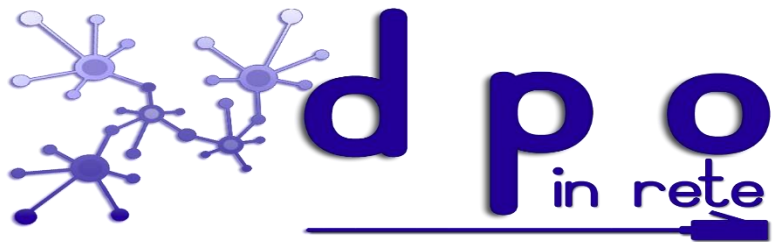
Prima precauzione

Rilevare la temperatura e non registrare il dato acquisito. 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.



Seconda precauzione

Fornire l'informativa sul trattamento dei dati personali. Si ricorda che l'informativa può omettere le informazioni di cui l'interessato è già in possesso e può essere fornita anche oralmente. 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. 1, n. 7, lett. d) del DPCM 11 marzo 2020 e con riferimento alla durata dell'eventuale conservazione dei dati si può far riferimento al termine dello stato d'emergenza.



Esempio di informativa



Ai sensi del Regolamento Ue n. 679/2016 (cd. GDPR), si forniscono di seguito le informazioni in merito al trattamento dei dati personali dei soggetti che, durante l'emergenza COVID-19, c.d. Coronavirus, accedono ai locali e agli uffici del comune..... o ad altri luoghi comunque a quest'ultimo riferibili.

Titolare del trattamento

Il Comune..... , con sede legale in....., e-mail:.....

Tipologia di dati personali trattati e di interessati

Nei limiti delle finalità e delle modalità definite nella presente informativa, sono oggetto di trattamento:

- a) i dati attinenti alla temperatura corporea;
- b) le informazioni in merito a contatti stretti ad alto rischio di esposizione, negli ultimi 14 giorni, con soggetti sospetti o risultati positivi al COVID-19;
- c) le informazioni in merito alla provenienza, negli ultimi 14 giorni, da zone a rischio secondo le indicazioni dell'OMS.

I dati personali oggetto di trattamenti si riferiscono a:

- a) il personale dipendente del Comune..... Rispetto a tali interessati, la presente informativa integra quella già fornita per il trattamento dei dati personali funzionale all'instaurazione e all'esecuzione del rapporto di lavoro;
- b) i fornitori, i trasportatori, gli appaltatori, visitatori e ogni altro soggetto terzo autorizzati ad accedere ai locali e agli uffici del Comune..... o ad altri luoghi comunque a quest'ultimo riferibili.

Finalità e base giuridica del trattamento

I dati personali saranno trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19, in esecuzione del Protocollo di sicurezza anti-contagio adottato ai sensi dell'art. 1, n. 7, lett. d) del DPCM 11 marzo 2020.

La base giuridica del trattamento è, pertanto, da rinvenirsi nell'implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. 1, n. 7, lett. d) del DPCM 11 marzo 2020 nonché nell' art. 6, par. 1 lett. d) ed e) del GDPR; art. 9, par. 1 lett. b) ed i) del GDPR);

Natura del conferimento dei dati personali

Il conferimento dei dati è necessario per accedere ai locali e agli uffici del Comune..... o ad altri luoghi comunque a quest'ultimo riferibili. Un eventuale rifiuto a conferirli impedisce di consentire l'ingresso.



Modalità, ambito e durata del trattamento

Il trattamento è effettuato dal personale dipendente del Comune..... che agisce sulla base di specifiche istruzioni fornite in ordine alle finalità e alle modalità del trattamento.

Con riferimento alla misurazione della temperatura corporea, il Comune non effettua alcuna registrazione del dato. L'identificazione dell'interessato e la registrazione del superamento della soglia di temperatura potrebbero avvenire solo qualora fosse necessario documentare le ragioni che hanno impedito l'accesso. In tal caso, l'interessato sarà informato della circostanza.

I dati personali non saranno oggetto di diffusione, né di comunicazione a terzi, se non in ragione 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).

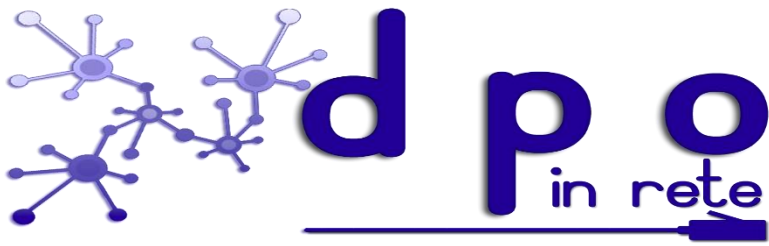
I dati saranno trattati per il tempo strettamente necessario a perseguire la citata finalità di prevenzione dal contagio da COVID-19 e conservati non oltre il termine dello stato d'emergenza, attualmente fissato al 31 luglio 2020 dalla Delibera del Consiglio dei Ministri 31 gennaio 2020.

Diritti degli interessati

In qualsiasi momento, gli interessati hanno il diritto di accedere ai propri dati personali, di chiederne la rettifica, l'aggiornamento e la relativa cancellazione. È, altresì, possibile opporsi al trattamento e richiederne la limitazione.

Queste richieste potranno essere rivolte al Comune..... via e-mail:

Inoltre, nel caso in cui si ritenga che il trattamento sia stato svolto in violazione della normativa sulla protezione dei dati personali, è riconosciuto il diritto di presentare reclamo all'Autorità Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 - Roma.



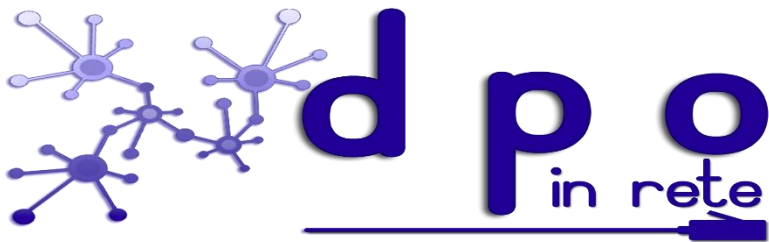
Terza precauzione

Definire le misure tecniche e organizzative adeguate a proteggere i dati. In particolare, sotto il profilo organizzativo, occorre individuare i soggetti preposti al trattamento e fornire loro le istruzioni necessarie. 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);



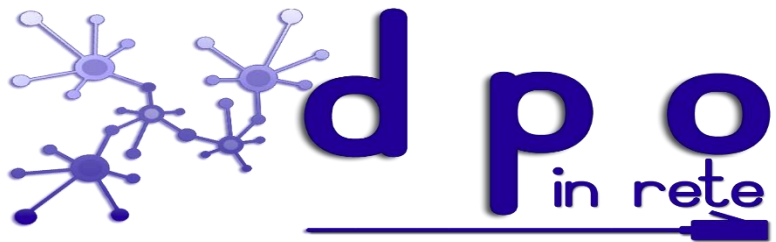
Quarta precauzione

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 lavorativo, 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.



Quinta precauzione

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 precedenti e, nello specifico, si 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.



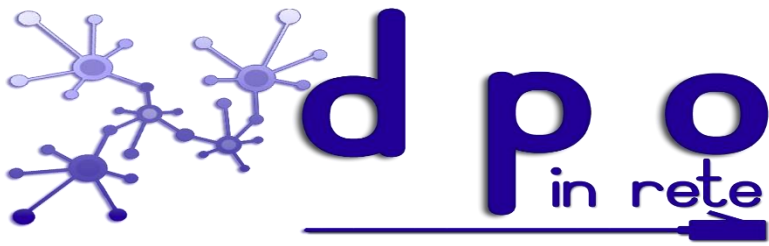
Ricorso alle nuove tecnologie



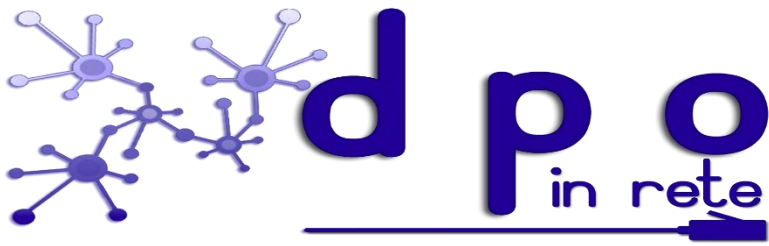
La telemedicina



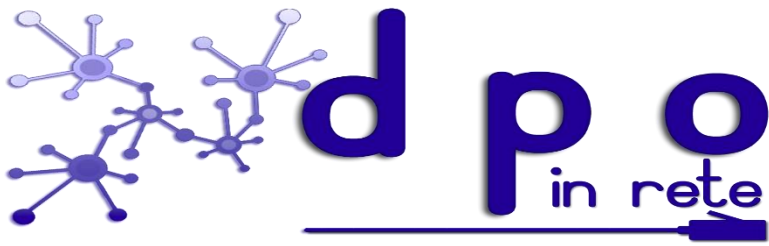
Nell'ambito dell'attuazione dei servizi di sanità in rete, assume grande rilevanza la definizione e creazione di modalità tecnico-organizzative finalizzate a consentire l'integrazione socio-sanitaria ed a sostenere forme di assistenza domiciliare del paziente.



La Commissione europea ha definito la telemedicina come *“la prestazione di servizi di assistenza sanitaria, tramite il ricorso alle TIC, in situazioni in cui il professionista della salute e il paziente (o due professionisti) non si trovano nella stessa località. Essa comporta la trasmissione sicura di informazioni e dati di carattere medico grazie a testi, suoni, immagini o altre forme necessarie per la prevenzione, la diagnosi, il trattamento e il successivo controllo dei pazienti”*



In particolare, quindi, la telemedicina può contribuire a migliorare la qualità dell'assistenza sanitaria e consentire la fruibilità di cure, servizi di diagnosi e consulenza medica a distanza, oltre al costante monitoraggio di parametri vitali, al fine di ridurre il rischio d'insorgenza di complicazioni in persone a rischio o affette da patologie croniche.



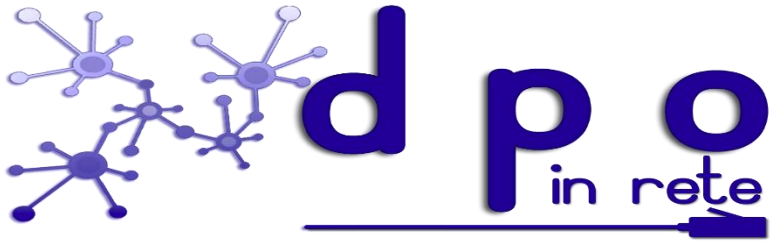
La Commissione Europea ha dato una particolare rilevanza al tema della Telemedicina. In particolare, attraverso la Comunicazione (COM-2008-689), del 4 novembre 2008, recante "*Telemedicina a beneficio dei pazienti, sistemi sanitari e società*", vengono individuate una serie di azioni che coinvolgono tutti i livelli di governo, sia in ambito comunitario che dei singoli Stati Membri, volte a favorire una maggiore integrazione dei servizi di Telemedicina nella pratica clinica, rimuovendo le principali barriere che ne ostacolano la piena ed efficace applicazione.



Infine presso il Consiglio Superiore di Sanità è stato istituito, in data 24 febbraio 2011, un apposito Tavolo tecnico sulla telemedicina con l'obiettivo di predisporre apposite Linee di indirizzo nazionali, finalizzate a delineare un quadro strategico nel quale collocare gli ambiti prioritari di applicazione delle telemedicina, analizzare modelli, processi e modalità di integrazione dei servizi di telemedicina nella pratica clinica, definire tassonomie e classificazioni comuni, oltre ad aspetti concernenti i profili normativi e regolamentari e la sostenibilità economica dei servizi e delle prestazioni di telemedicina. Tali Linee Guida sui cui è stata acquisita l'Intesa in sede di Conferenza Stato-Regioni in data 20 febbraio 2014 costituiscono oggi una base di lavoro per chi si appresta a creare servizi di telemedicina.



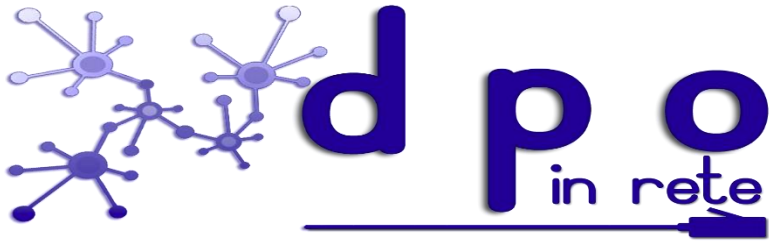
L'azione vincente della telemedicina è riscontrabile soprattutto in attività di prevenzione per particolare categorie della popolazione con patologie che pur conducendo una vita normale, devono sottoporsi ad un costante monitoraggio di alcuni parametri vitali, al fine di ridurre il rischio d'insorgenza di complicazioni.



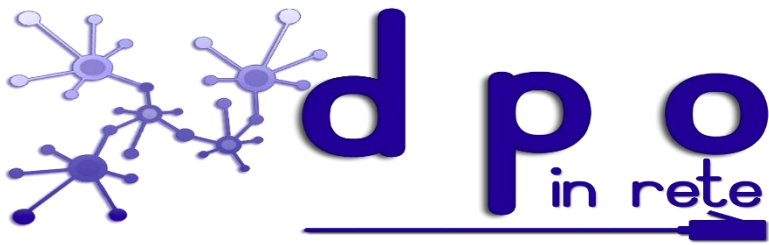
Sistemi di videosorveglianza in ambito sanitario



Il “controllo” fisico dei pazienti, ma anche il controllo dei campioni nelle analisi di laboratorio viene oggi realizzato spesso con tecnologie che se, da una parte, raggiungono efficacemente il risultato, dall'altra, spesso espongono a rischi legati al trattamento dati.



Le tecnologie, in particolare, oggi più utilizzate sono le tecnologie RFID (Radio Frequency IDentification) che in sanità da anni vengono utilizzate per svariate finalità. Le principali sono le seguenti:

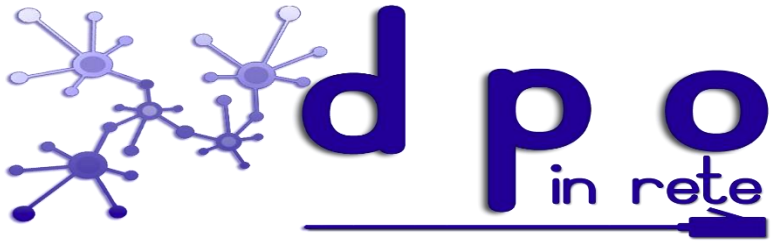


IDENTIFICAZIONE PAZIENTE: in tale ambito si trovano principalmente applicazioni per la sicurezza del paziente, dove l'RFID è funzionale all'identificazione della persona, riducendo i rischi legati ad errori (si pensi ad esempio ad omonimie o nomi "difficili" dovuti alle diverse nazionalità).

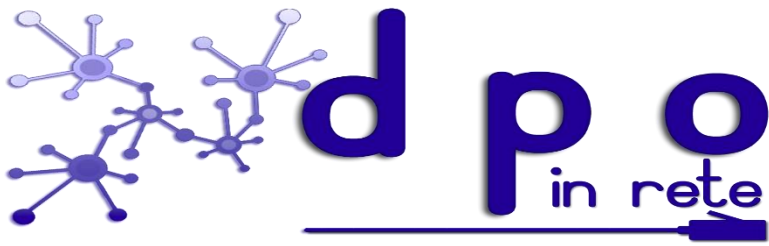
LOCALIZZAZIONE PAZIENTE: in tale ambito la tecnologia RFID è utilizzata per localizzare il paziente e monitorarne gli spostamenti all'interno della struttura in cui si trova, così da emettere alert automatici nel caso in cui il malato entri in una zona non consentita o esca da una determinata area (si pensi alla necessità di monitorare gli spostamenti di pazienti psichiatrici, potenzialmente pericolosi, o a malati di Alzheimer).

TRACCIABILITÀ E LOCALIZZAZIONE "ASSET": in tale ambito la tecnologia RFID viene implementata per evitare furti, smarrimenti e conseguenti perdite di tempo nella ricerca di attrezzature mobili (ad esempio sedie a rotelle, apparecchiature elettrobiomedicali portatili necessarie ai reparti).

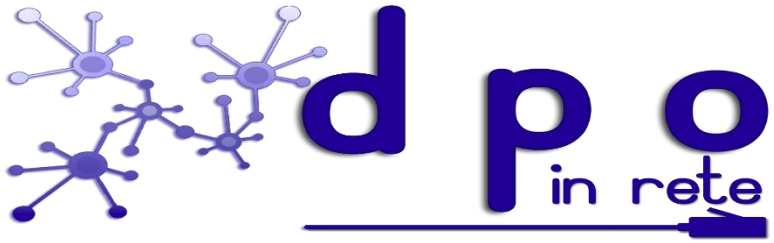
TRACCIABILITÀ "PRODOTTI" O CAMPIONI: ovvero tutto ciò che viene gestito all'interno dell'ospedale ad eccezione delle apparecchiature e dei pazienti: sacche di sangue, sostanze organiche, farmaci, strumenti chirurgici, etc.



Tecniche di tracciamento (contact tracing)



Seguendo il modello coreano anche il nostro paese sta cercando di utilizzare delle apps che possono mappare e tracciare i movimenti delle persone risultate positive al coronavirus allo scopo di avvertire chi è entrato in contatto con loro ed è quindi a rischio contagio.

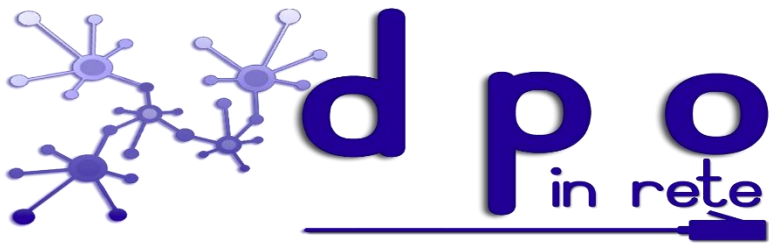


Le posizioni del nostro Garante e del Comitato europeo sulla protezione dei dati personali



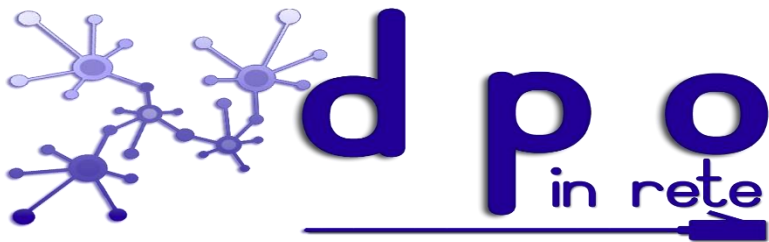
Il Comitato europeo con dichiarazione del 19 marzo 2020 ha sostenuto che le norme in materia di protezione dei dati (come il regolamento generale sulla protezione dei dati) non ostacolano l'adozione di misure per il contrasto della pandemia di coronavirus. La lotta contro le malattie trasmissibili è 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 sottolinea però 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.

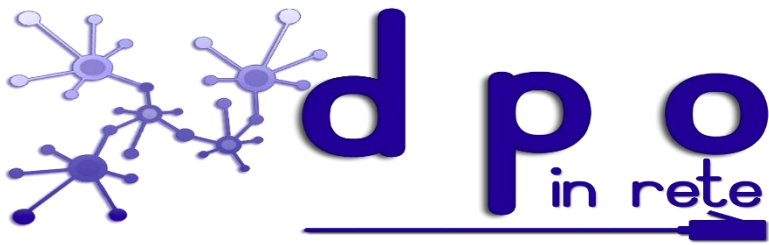


Sostiene il Comitato europeo che il GDPR è una normativa di ampia portata e contiene disposizioni che si applicano anche al trattamento dei dati personali in un contesto come quello relativo al COVID-19.

Il GDPR 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.

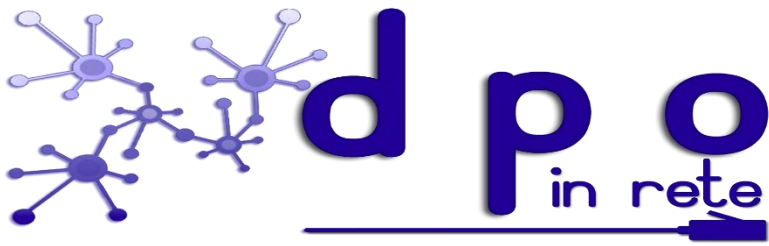


Riguardo il trattamento dei dati personali, comprese le categorie particolari di dati, da parte di autorità pubbliche competenti (ad es. autorità sanitarie pubbliche), il Comitato ritiene che gli articoli 6 e 9 del GDPR consentano tale trattamento, in particolare quando esso ricada nell'ambito delle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



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 GDPR 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.

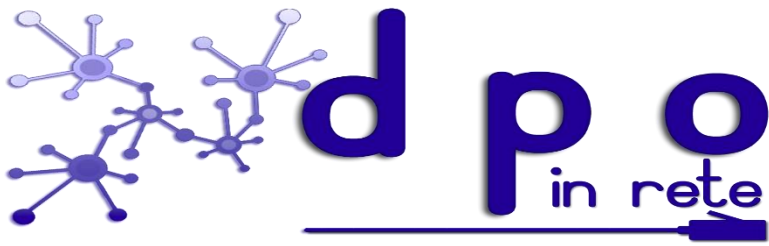


Riguardo il trattamento dei dati delle telecomunicazioni, come i dati relativi all'ubicazione, devono essere rispettate anche le leggi nazionali di attuazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva e-privacy).

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.



Con riferimento alle apps il Comitato sottolinea che 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).

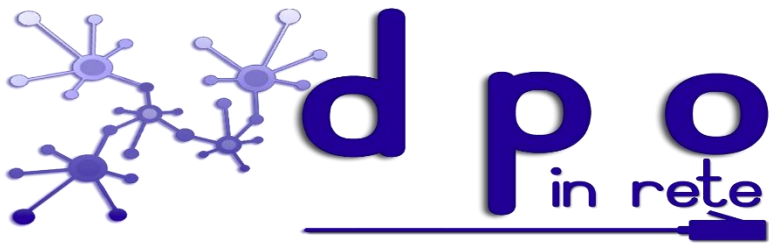
Qualora siano introdotte misure che consentono il trattamento dei dati di localizzazione in forma non anonimizzata, lo Stato membro ha l'obbligo di predisporre garanzie adeguate, ad esempio fornendo agli utenti di servizi di comunicazione elettronica il diritto a un ricorso giurisdizionale.

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).



Inoltre, più in generale, il Comitato ricorda il rispetto di altri principi fondamentali:

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



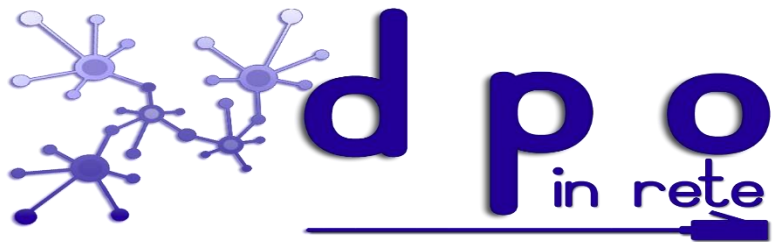
La posizione della nostra Autorità Garante è sostanzialmente allineata a quella del Comitato e con riferimento al contact tracing il nostro Garante sarebbe dell'idea di introdurre l'utilizzo di questa tecnica attraverso un provvedimento normativo urgente e temporaneo come il decreto legge.



Lo scambio e, prima ancora, la raccolta dei dati devono avvenire, secondo l’Autorità, nel modo meno invasivo possibile per gli interessati, privilegiando l'uso di dati pseudonimizzati (ove non addirittura anonimi), ricorrendo alla re-identificazione laddove vi sia tale necessità, ad esempio per contattare i soggetti potenzialmente contagiati.

Nella complessa filiera in cui si articolerebbe il contact tracing, soggetti privati - a partire dalle grandi piattaforme - dovrebbero porre il patrimonio informativo di cui dispongono a disposizione dell'autorità pubblica, alla quale dovrebbe invece essere riservata la fase dell'analisi dei dati, che necessita delle garanzie e della responsabilità degli organi dello Stato.

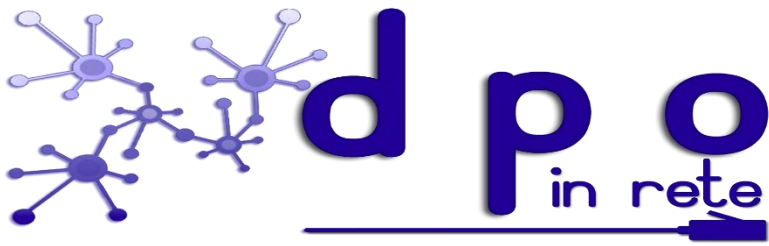
In ogni caso, le società coinvolte in questo progetto dovrebbero possedere requisiti di affidabilità e trasparenza di azione. Nella valutazione è fondamentale il vaglio di conformità ai requisiti di protezione dati, per la garanzia dei diritti degli interessati, per l'attendibilità dell'analisi dei dati e anche per la sicurezza nazionale.



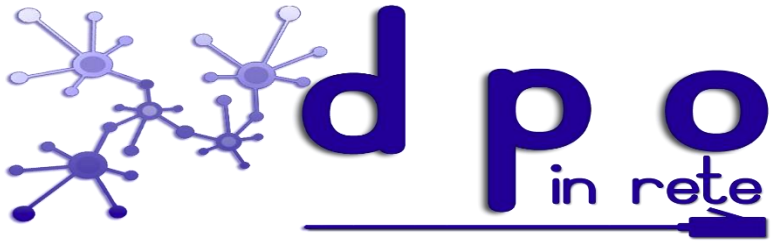
DOMANDE



**Registrare un atto (nascita o morte) da casa?
Come si può ovviare per le firme dei dichiaranti?**



In realtà gli strumenti ci sarebbero ma è necessario che i comuni attivino i relativi servizi telematici. Senza pensare a strumenti complessi come la firma digitale, si potrebbe consentire l'accesso riservato ad un'area web (tramite CIE, Spid o comunque delle credenziali di autenticazione) e prevedere la compilazione del modulo on line.



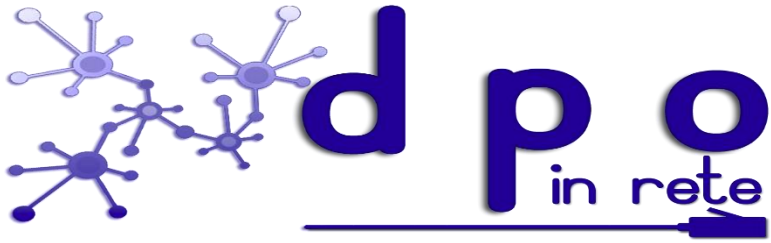
Come tutelare la privacy del personale posto in "lavoro agile"?



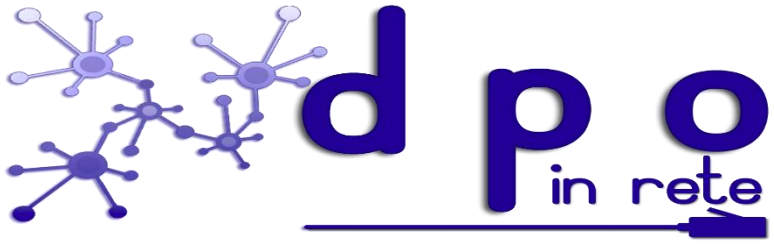
In genere quelle che vanno tutelate in smart working sono sicuramente esigenze di sicurezza più che altro a tutela dello stesso datore di lavoro che, difatti, prevede nello specifico un'informativa che richiama le norme del GDPR e principalmente tutti gli accorgimenti da utilizzare per evitare che soggetti estranei possano venire a conoscenza di informazioni e documenti d'ufficio.



Ritiro dei rifiuti urbani da abitazioni con positivi al virus. Elenco dei positivi domiciliati nel comune in possesso all'ASP e inviato al Comune. Procedure per la consegna all'impresa affidataria e modalità di gestione da parte di questa. Come si tutela la privacy?



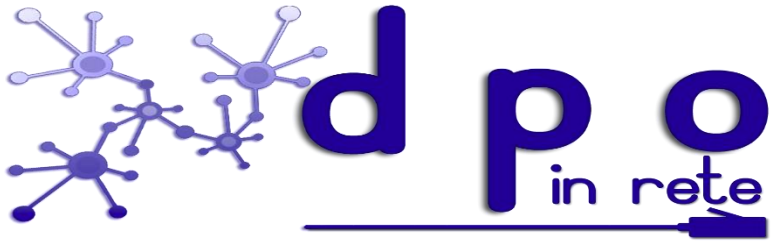
Tutte queste attività possono tranquillamente rientrare nell'ambito della previsione dell'art. 14 del D.L. n. 14/2020.



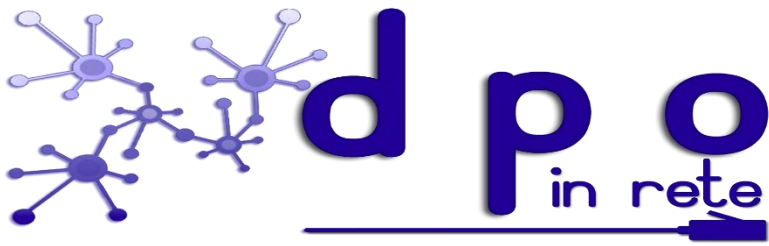
La gestione da remoto delle concessioni demaniali marittime



Si tratta di procedimenti piuttosto complessi e molto tecnici che sono sempre contraddistinti da una fase telematica ma anche da fasi più prettamente analogiche (si veda il rilascio di una concessione). Naturalmente anche in questo caso molto dipende da come sono organizzati gli enti locali e lo stesso Ministero delle infrastrutture e dei trasporti. Anche i pagamenti dei canoni di concessione possono essere gestiti on line. Inutile dire che qualsiasi procedura telematica deve rivestire quelle necessarie condizioni di sicurezza che possano consentire una gestione senza particolari rischi.

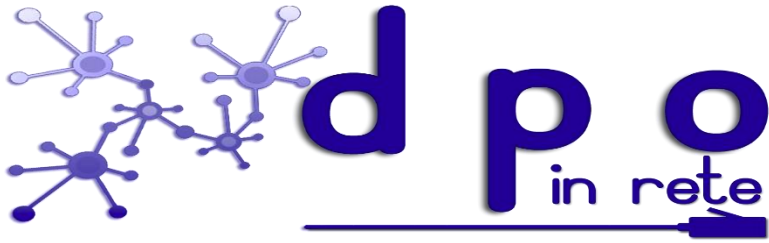


La privacy e la gestione delle concessioni cimiteriali da remoto



Molti comuni hanno informatizzato i servizi cimiteriali e quindi attraverso un programma informatico si è in grado di visualizzare, in tempo reale, i dati relativi ai posti occupati nei vari settori del cimitero, la scadenza delle concessioni e le anagrafiche dei concessionari, incrociati con i dati delle utenze di lampade votive.

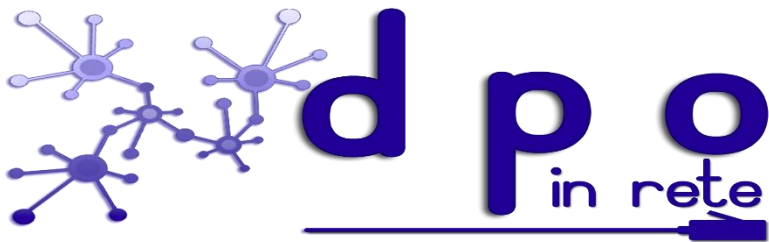
Anche in questo caso i problemi connessi ad una gestione telematica sono riconducibili principalmente ad esigenze di sicurezza.



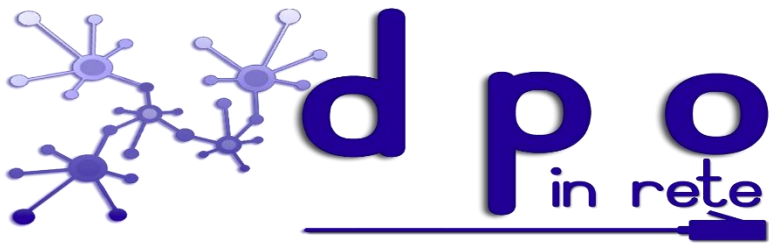
Un titolare del trattamento può chiedere ai visitatori o ai dipendenti di fornire informazioni sanitarie specifiche nel contesto del COVID-19?



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 nei casi previsti dalla normativa speciale.



Il titolare del trattamento può informare dipendenti o soggetti esterni del fatto che un dipendente è affetto dal COVID-19?



I titolari del trattamento devono informare il personale sui casi di COVID-19 e adottare misure di protezione, ma non devono 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), i dipendenti interessati ne sono informati in anticipo tutelando la loro dignità e integrità.