PRIVACY

applicazione dei nuovi adempimenti per medici e odontoiatri a seguito dell'emanazione del D.lvo 101/2018

Sabato 20 ottobre 2018

PRIVACY

applicazione dei nuovi adempimenti per medici e odontoiatri a seguito dell'emanazione del D.lvo 101/2018

Il PUNTO sulla Privacy: l'EVOLUZIONE del quadro normativo.

Dott. Antonino Addamo

a che punto siamo

IL 25.5.18 È ENTRATO IN VIGORE IL REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

GDPR

(General Data Protection Regulation - Regolamento generale sulla protezione dei dati)

Dal 25 maggio 2018 il GDPR deve essere pienamente e integralmente attuato

Le sanzioni e i controlli sono in vigore dal 25 maggio

- **A TUTTI GLI EFFETTI DAL 25.05.18 E' IN VIGORE IL GDPR**

- **Dal 25 maggio IL CODICE PRIVACY DLgs 196/2003** è stato disapplicato negli articoli che confliggono con le indicazioni del GDPR rimando in vigore solo nelle parti che restano riservate allo stato italiano, con una sovrapposizione tra le disposizioni europee e il codice della privacy.

Dal D.Lgs 196/2003 al GDPR: le novità e le differenze

la norma europea non impone, “indica”

Il Regolamento Europeo infatti prescrive di adottare “misure adeguate” sul principio della **responsabilizzazione** “accountability”, ma non entra nel merito della fattibilità.

GDPR

- Il principio di "*Accountability*", ovvero della responsabilità "*verificabile*". E' obbligatorio documentare tutti i trattamenti effettuati.
- Riferimento oggettivo alla finalità e modalità del trattamento
- "*Privacy by Design*" e "*Privacy by Default*"
- Diritto alla portabilità dei dati
- Diritto alla cancellazione («diritto all'oblio»)
- Diritto di accesso
- Misure di sicurezza, con il GPDR le uniche misure di sicurezza ammesse sono quelle "adeguate".
- Responsabilità solidale tra il titolare e il responsabile
- Notifica delle violazioni di dati personali: data breach

GDPR

- ***Informativa scritta***

  preferibilmente in formato elettronico

- **concisa, trasparente, intelligibile per l´interessato e facilmente accessibile**; linguaggio **chiaro e semplice**
- **idonee informative per i minori**
- il titolare deve specificare **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all´autorità di controllo.

- ***Consenso scritto o orale esplicito inequivocabile***
- Il **consenso dei minori** è valido **a partire dai 16 anni** (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

GDPR

- Valutazione di Impatto sulla protezione dei dati
- Contratto per il Trattamento dei Dati Personali X RESPONSABILI
- Formazione Autorizzazione al Trattamento di Dati Personali X INCARICATI
- Informativa x dipendenti
- Registro delle attività di trattamento

e le figure interessate

- Titolare del trattamento
- Contitolare del trattamento
- Responsabile del trattamento
- Incaricato
- Destinatario
- **D**ata **P**rotection **O**fficer (DPO) /**R**esponsabile della **P**rotezione dei **D**ati (RDP)

- **DECRETO LEGISLATIVO 10 agosto 2018, n. 101**
- **Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).**
- **Gazzetta Ufficiale del 4 settembre 2018**
- ***Entrata in vigore del provvedimento: 19/09/2018***

Capo I **Modifiche al titolo e alle premesse del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196**
Capo II Modifiche alla parte I del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196
Capo III Modifiche alla parte II del codice in materia di protezione dei dati personali di cui decreto legislativo 30 giugno 2003, n. 196

L'art. 1 del decreto legislativo 30 giugno 2003, n. 196 è così modificato

- Art. 1 (Oggetto) Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito «Regolamento», e del presente codice, nel rispetto della dignita' umana, dei diritti e delle liberta' fondamentali della persona.»;

LE NOVITÀ INTRODOTTE di interesse per i sanitari dal *Dlgs 10 agosto 2018 n. 101*

Il Sole 24 ORE *19-9.18*

PRIVACY, PROFESSIONISTI ESONERATI DAL DPO E REGISTRO TRATTAMENTI

chi si è fermato a leggere soltanto il titolo di un autorevole quotidiano, il sole 24 ore, si è creato solo un allettante illusione, leggendo l'articolo si capisce che non è così.

LE NOVITÀ INTRODOTTE di interesse per i sanitari dal *Dlgs 10 agosto 2018 n. 101*

- In ordine generale il decreto 101/2018 di adeguamento al Gdpr, prevede un particolare regime di favore per le micro, piccole e medie imprese (inclusi professionisti e artigiani) attribuendo al Garante il compito di prevedere con apposite linee guida, modalità semplificate di adempimento degli obblighi di questi titolari, tra cui i professionisti

LE NOVITÀ INTRODOTTE di interesse per i sanitari dal *Dlgs 10 agosto 2018 n. 101*

- **Consenso al trattamento dei dati x finalità di cura**
- **Registro delle attività di trattamento semplificato**
- **Consenso dei minori**
- **Curriculum**
- **Persone decedute**
- **Apparato sanzionatorio**

Consenso al trattamento dei dati x finalità di cura

Il professionista sanitario che utilizza dati personali dei pazienti per finalità di cura ed assistenza sanitaria non sarà più tenuto a richiedere il consenso dell'interessato, restano comunque in essere tutti gli altri obblighi come l'informativa, chiare e semplici informazioni sul'utilizzo dei dati, sulla loro conservazione e sui diritti esercitabili.

- tale deroga già prevista dall'art. 9.3 GDPR, dispone che è possibile utilizzare la base giuridica di cui all'Art. 9.2 h)solo *se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale […] o da altra persona anch'essa soggetta all'obbligo di segretezza […].*

trattamento dei dati x finalità di cura

anche se non è più previsto il consenso, l'utilizzo e il trattamento dei dati sanitari deve essere svolto in conformità a misure di garanzia disposte dal Garante con cadenza biennale. Tali garanzie, adottate su parere del Ministero della salute e del Consiglio superiore di Sanità, devono tenere conto dell'evoluzione scientifica e tecnologica e includono tra l'altro la cifratura, la pseudonimizzazione e l'accesso selettivo dei dati misure che riguardano anche i gestionali in ambito sanitario, le modalità di comunicazione ai pazienti dei dati di diagnosi e di salute e le prescrizioni di farmaci.

ECCEZIONI:

- Il consenso resta necessario per l'utilizzo ed il trattamento dei dati genetici, trattamento consentito se svolto nell'ambito di attività sanitarie in conformità alle misure di garanzia disposte dal Garante con cadenza biennale
- In caso di trattamenti ad alto rischio può essere previsto il ripristino della richiesta di consenso.

Dlgs 10 agosto 2018 n. 101

- Il decreto specifica anche la differenza tra “comunicazione”, rivolta a terzi determinati diversi dall’interessato, e “diffusione” di dati a terzi generici di dati, quest’ultima in sanità è vietata.

- "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

registro delle attività di trattamento

- GARANTE
- L'art. 30 del Regolamento (EU) n. 679/2016 ("RGPD") prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento
- In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

  qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, *[…]*

L'art 9 ricomprende tra l'altro i dati sanitari

registro delle attività di trattamento

- Alla luce di quanto detto sopra, sono tenuti all'obbligo di redazione del registro, ad esempio:
- - liberi professionisti con almeno un dipendente e/o che trattino dati sanitari .. *[...]*(es. osteopati, fisioterapisti, farmacisti, medici in generale);
- Infine, si precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento

registro delle attività di trattamento

- **registro delle attività di trattamento semplificato**
  x le imprese e organizzazioni con meno di 250 dipendenti
- …… potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

consenso dei minori

- il consenso potrà essere espresso al compimento dei 14 anni di età. Al di sotto di tale soglia, il consenso andrà prestato da chi esercita la responsabilità genitoriale.

Curriculum

- **Obblighi del titolare del trattamento** nei casi di **ricezione di curriculum** finalizzati all'instaurazione di un rapporto di lavoro.

Le informazioni previste dall'articolo 13 del GDPR (tra cui le finalità del trattamento e i dati del DPO) dovranno essere fornite al momento del primo contatto utile successivo all'invio.

- **Articolo 13 EU GDPR**
  Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

Persone decedute

- **Privacy dei deceduti** – I dati di pazienti deceduti (articolo 2 terdecies) possono essere attinti da chi ha un interesse proprio o a tutela dell'interessato, o per ragioni familiari da proteggere, ma **non** se l'interessato lo ha vietato con dichiarazione scritta al titolare o lo ha comunicato allo stesso.

Apparato sanzionatorio

- Dal 25 maggio sono in vigore le sanzioni ma per i primi otto mesi dalla data di entrata in vigore del decreto, maggio 2018, il Garante della privacy dovrà tener conto, nell'applicare le sanzioni amministrative e compatibilmente con le disposizioni del GDPR, della fase di prima applicazione delle disposizioni sanzionatorie.
- l'avvio del provvedimento sanzionatorio sarà subordinato alla presentazione di apposito reclamo o ad automa iniziativa del Garante nonché a seguito di accessi o ispezioni della Guardia di Finanza

SANZIONI

- Le **sanzioni amministrative e penali** previste in caso di violazione degli obblighi introdotti dal GDPR, è stabilita la possibilità - per i provvedimenti non ancora definiti con l'adozione dell'ordinanza di ingiunzione - di pagare la sanzione in misura ridotta (pari a due quinti del minimo) entro il termine di 90 giorni dalla data di entrata in vigore del decreto attuativo.
- Inoltre, per le **violazioni commesse anteriormente** alla data di entrata in vigore del decreto, potranno essere applicate le sanzioni amministrative sostitutive delle sanzioni penali previste dall'*ex* Codice Privacy qualora il procedimento penale non sia ancora stato definito con sentenza o decreto irrevocabili.

RESPONSABILI OBBLIGHI

- Gli obblighi ed adempimenti relativi rapporti con i **RESPONSABILI** non cambiano alla luce del DLGS 101/18
- il DGPR specifica, Art.28, che i rapporti tra titolare e responsabile siano stabiliti con un contratto
- *I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico*

RESPONSABILE

- «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che tratta dati personali** per conto del titolare del trattamento;

Nella nostra realtà lavorativa possiamo identificarli ad es.

- ***Commercialista***
- ***Compagnia Assicurativa***
- ***Consulente del lavoro***
- ***Fornitore di servizi di hosting Hosting provider***
- ***Operatore di piattaforma di marketin***
- ***Laboratori di analisi mediche***
- ***Laboratorio odontotecnico***
- ***Medico competente***

- È necessario che il Responsabile del trattamento presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

- Il regolamento Europeo prevede la

Responsabilità solidale tra il titolare e il responsabile

- 1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o **identificabile**; si considera identificabile la persona fisica che può essere identificata, direttamente o **indirettamente**, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (**C26, C27, C30**,)
- ***Identificabile*** *è la persona che può essere identificata anche mediante il riferimento ad ulteriori elementi.*

- **2) «trattamento»:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Dati soggetti a trattamento speciale (ex dati sensibili)

- - **genetici**

  - **biometrici** intesi a identificare in modo univoco una persona fisica

  - relativi alla **salute**

- **Dati anonimizzati** sono quei dati che sono stati privati di tutti gli elementi identificativi. I dati anonimizzati non sono ritenuti dati personali, e quindi non sono soggetti alle norme a tutela dei dati personali.

- **Dati pseudonimi**
- **Pseudonimizzazione** è una tecnica che consiste nel conservare i dati in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive, **La pseudonimizzazione, o cifratura, consiste nel modificare e mascherare i dati** personali e sensibili di una persona fisica al fine di non renderli direttamente e facilmente attribuibili allo stesso senza l'utilizzo di informazioni aggiuntive.

  I dati pseudonimi, a differenza di quelli anonimizzati, sono comunque dati personali in quanto consentono l'identificazione della persona, anche se indirettamente, tramite incrocio con altre informazioni.
  Sono soggetti ad una tutela ridotta rispetto ai dati personali veri e propri.

PRIVACY

applicazione dei nuovi adempimenti per medici e odontoiatri a seguito dell'emanazione del D.lvo 101/2018

Il PUNTO sulla Privacy: l'EVOLUZIONE del quadro normativo.

Grazie per l'attenzione

LE FIGURE INTERESSATE

*D.Lgs.*196/2003	GDPR
Titolare del trattamento	Data Controller – Titolare del trattamento
Responsabile del trattamento	Data Processor – Responsabile del trattamento
Incaricato	Non previsto, ma non esclusa la sua presenza: “persone autorizzate al trattamento dei dati personali sotto l’autorità diretta del titolare o del responsabile”
	Joint Controller – Contitolare del trattamento Introduzione della contitolarità nel trattamento dei dati
	Data **P**rotection **O**fficer (DPO) / **R**esponsabile della **P**rotezione dei **D**ati (RDP)
	Destinatario

LE FIGURE CHI SONO

Titolare

«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74)

- **STUDIO CON SINGOLO PROFESSIONISTA:**
  Medico/odontoiatra titolare dello studio
- **STUDIO ASSOCIATO, AMBULATORIO:**
  Persona giuridica, cioè la ragione sociale dello studio associato, della Società tra professionisti.

RESPONSABILE DEL TRATTAMENTO **la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;**	•Commercialista •Compagnia Assicurativa •Consulente del lavoro •Fornitore di servizi di hosting Hosting provider •Operatore di piattaforma di marketin •Laboratori di analisi mediche •Laboratorio odontotecnico •Medico competente

Persone autorizzate **(INCARICATI)** **persone autorizzate al trattamento dei dati personali sotto l´autorità diretta del titolare o del responsabile**	**dipendenti, collaboratori, tirocinanti:** **Infermiere** **Aso** **Segretaria**

«DESTINATARIO»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (C31) **OVVERO** **Soggetti che trattino Dati Personali di titolarità dello Studio per finalità autonome**	**•Agenzia delle entrate** **•INAIL** **•INPS** **•Sistema Tessera Sanitaria**
DPO	figura professionale con requisiti di indipendenza, autorevolezza e competenza manageriale