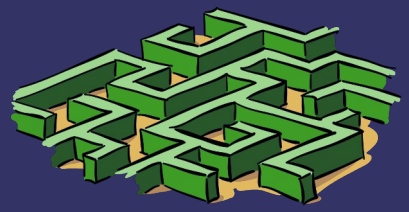
ASSOCIAZIONE NAZIONALE DENTISTI ITALIANI
SEZIONE PROVINCIALE DI MILANO LODI MONZA E BRIANZA

IL TRATTAMENTO DEI DATI PERSONALI IN AMBITO SANITARIO

con particolare riguardo al trattamento dei dati sensibili

Dr.ssa Silvia Coronelli
ANDI Sezione di Milano Lodi Monza Brianza



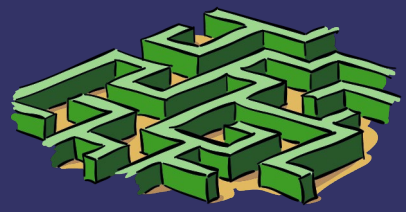
General Data Protection Regulation
Regolamento UE 2016/679

1995
- Direttiva 95/46/CE
- Decreto Privacy

2016
- 24 maggio
- Entra in vigore

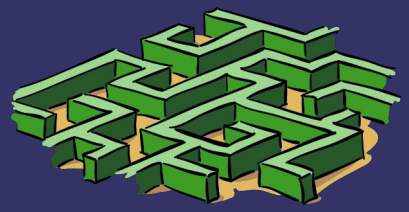
2018
- 25 maggio
- **Diventa pienamente efficace…**

…anche in attesa del decreto di adeguamento!!!



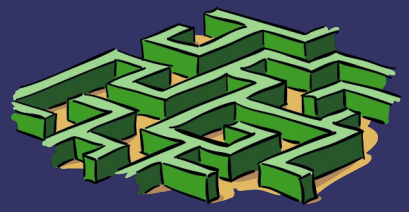
D.Lgs. 101/2018

Codifica l'adeguamento del vecchio Codice della Privacy al nuovo Regolamento per la Protezione dei Dati Personali modificandone e/o precisandone alcuni aspetti, come le sanzioni penali e l'età minima per esprimere consenso autonomo al trattamento dei propri dati personali



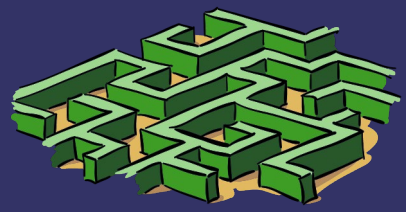
Art. 2-bis (D.Lgs. 101/2018)
Autorità di controllo

L'Autorità di controllo di cui all'*articolo 51 del regolamento* è individuata nel Garante per la protezione dei dati personali.



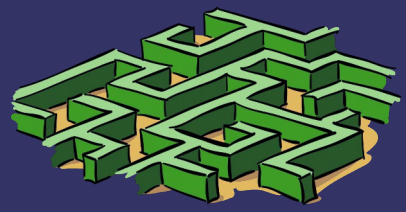
Articolo 1
Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.



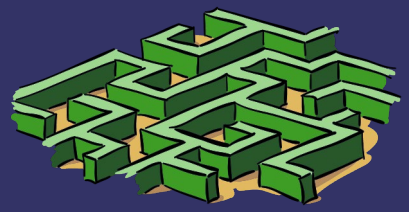
Articolo 2
Ambito di applicazione materiale

…..Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.



Art.3 «Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare/responsabile del trattamento nell'Unione e/o al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano offerta beni/servizi o monitoraggio.»

Foto di Michael Wolf



http://www.federprivacy.it/documentazione/Regolamento_UE_2016_679.pdf

DIRITTI degli interessati

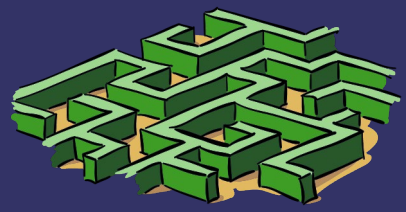
DOVERI del titolare/responsabile/incaricato

Dati Personali

DI CHI?

OBBLIGHI generali sulla sicurezza

SANZIONI



PRIVACY BY DESIGN – PRIVACY BY DEFAULT Art. 25

La necessità di tutelare il dato va rispettata sin dalla progettazione del sistema che ne prevedono l'utilizzo (DESIGN)

Tale sistema deve assicurare la tutela del dato per impostazione predefinita (DEFAULT)

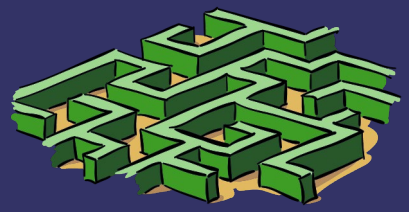
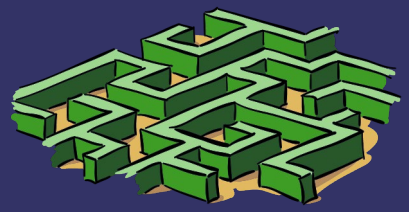


FIGURE COINVOLTE
Art.4

- **Titolare**: chi determina le finalità e le modalità di trattamento dei dati

- **Responsabile**: chi riceve dati dal titolare e gli assicura il rispetto delle finalità della procedura di trattamento

- **Incaricato**: chi è autorizzato dal titolare a trattare i dati secondo le direttive stabilite dal titolare

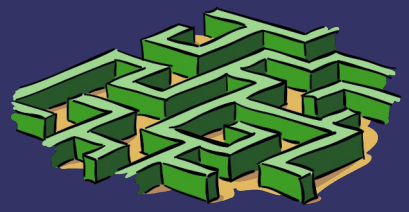


ACCOUNTABILITY

=

RESPONSABILIZZAZIONE

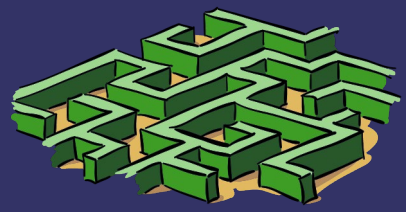
Il titolare del trattamento determina le modalità di trattamento purché rispetti l'art. 5 e sia in grado di comprovarlo (responsabilizzazione)



ACCOUNTABILITY
Art.5

Principi applicabili al trattamento dei dati personali:

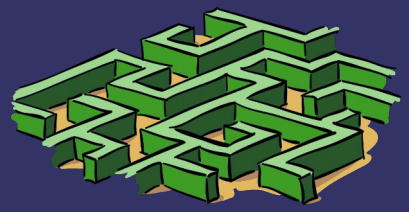
- Liceità, minimizzazione
- Correttezza
- Trasparenza
- Limitazione delle finalità
- Limitazione della conservazione
- Riservatezza (*misure tecniche ed organizzative* adeguate)



DIRITTI DELL'INTERESSATO

Sezioni 2, 3 e 4: Articoli dal 15 al 22

- Informativa
- Accesso, rettifica, cancellazione, oblio
- Limitazione
- Opposizione
- Portabilità



INFORMATIVA

- Identità del titolare (ed ev. Responsabile o DPO)
- Quali dati sono raccolti
- A quale scopo vengono raccolti
- La base giuridica su cui si fonda il trattamento
- Come sono conservati e protetti
- Chi vi ha accesso
- Quanto vengono conservati
- Come cancellarli/modificarli

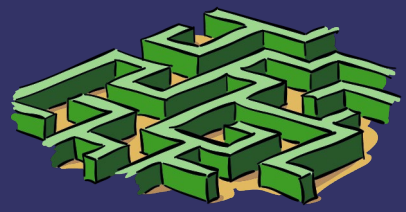
…..tutto questo in termini **SEMPLICI e COMPRENSIBILI**!

CONSENSO

Qualsiasi manifestazione di volontà

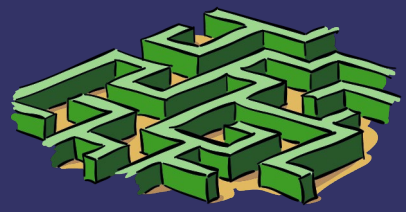
libera, specifica, informata e inequivocabile

dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; i consensi acquisiti fin qui restano validi se in linea col GDPR



Art. 2-quinquies (D.Lgs. 101/2018) Consenso del minore in relazione ai servizi della società dell'informazione

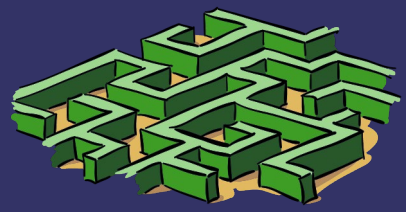
In attuazione dell'*articolo 8, paragrafo 1, del Regolamento*, il minore che ha compiuto i **quattordici anni** può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'*articolo 6, paragrafo 1, lettera a), del Regolamento*, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale.



Corte UE: pronuncia sul consenso per installare i cookie

sentenza CGUE 1/10/2019 (causa C673/17)

- Il consenso all'uso dei cookie con caselle preselezionate rende impossibile determinare l'attiva volontà dell'interessato di acconsentire alla loro installazione
- L'utente dovrebbe, inoltre, essere informato sulla durata dei cookie e sul fatto che taluni terzi abbiano o meno accesso ai cookie stessi

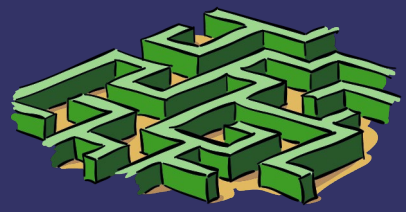


Odontoiatria33 10 ottobre 2019

I cyber attacchi al sistema informativo pubblico sono cresciuti del 41% rispetto all'anno scorso, mentre in quello sanitario del 99%. Gli accessi indebiti in ambito sanitario sono quindi i più rilevanti in assoluto".

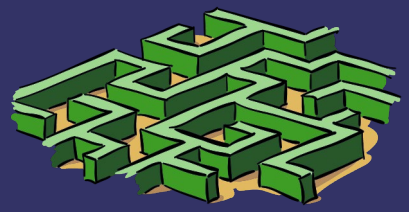
Le società che forniscono apparecchiature per l'alta diagnostica non possono utilizzare per i propri scopi i dati dei pazienti sottoposti agli accertamenti medici

Il chiarimento del Garante conferma la necessità di trattare con attenzione e cautela materiale informatico sensibile come quelli provenienti da scanner intraorali, Cone Beam etc. ad uso odontoiatrico.



REGISTRO DELLE ATTIVITA'
Art. 30

- Nome e dati contatto del titolare ed eventuale DPO
- Finalità del trattamento
- Categorie interessati e dati oggetto di trattamento
- Categorie di destinatari a cui i dati verranno comunicati
- Termini ultimi previsti per la cancellazione
- Descrizione generale delle misure di sicurezza tecniche e organizzative



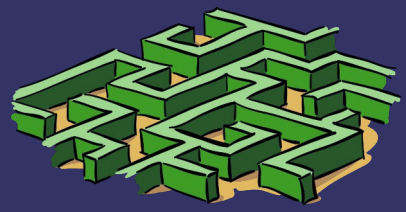
REGISTRO DELLE ATTIVITA'
Art. 30

TITOLARE

- Nome e dati contatto del titolare ed eventuale DPO
- Finalità del trattamento
- Categorie interessati e dati oggetto di trattamento
- Categorie di destinatari a cui i dati verranno comunicati
- Termini ultimi previsti per la cancellazione
- Descrizione generale delle misure di sicurezza tecniche e organizzative

RESPONSABILE

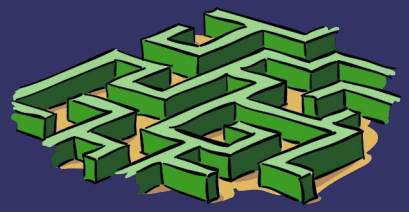
- Nome e dati contatto del responsabile e di ogni titolare ed eventuale DPO
- Categorie dei trattamenti effettuati
- Descrizione generale delle misure di sicurezza tecniche e organizzative



NOTIFICA DELLE VIOLAZIONI
Data Breach
Art. 33 e 34

- *All'autorità* senza ingiustificato ritardo, e comunque entro 72 ore dal momento in cui se ne viene a conoscenza, a meno che sia improbabile che la violazione rappresenti un rischio per diritti e la libertà delle persone fisiche

- Agli *interessati*, senza ingiustificato ritardo, qualora la violazione rappresenti un grave rischio per i diritti e la libertà degli interessati

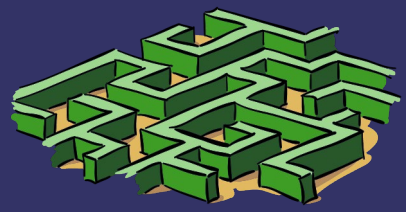


REGIME SANZIONATORIO
Art. 58, 82-84

Le sanzioni amministrative pecuniarie devono essere «effettive, proporzionate e dissuasive»

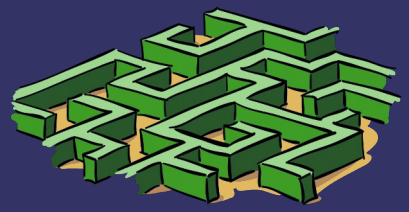
L'ammontare è stabilito sulla base dei seguenti elementi:

- La categoria di dati; natura, la gravità e la durata della violazione, la finalità del trattamento, il numero di interessati lesi e il livello del danno da essi subito;
- Il carattere doloso o colposo della violazione;
- Le misure adottate dal titolare o dal responsabile del trattamento per prevenire e/o attenuare il danno subito dagli interessati;
- Se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- Eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso(es. benefici economici)



TIPI DI RESPONSABILITA'

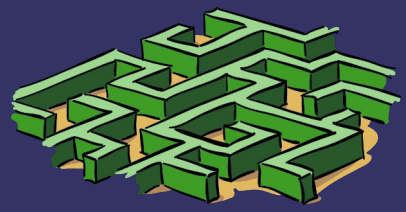
- Civile: procuro un danno ad una persona, devo risarcirla
- Amministrativa: sono le multe. È una responsabilità verso lo stato, come la penale.
- Penale: introdotta dal D.Lgs 101/2018



RESPONSABILITA' CIVILE

Art. 82

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del ..regolamento ha diritto ad ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento
2. Un titolare risponde per le violazioni alle disposizioni del trattamento, un responsabile solo per violazioni delle direttive impartite dal titolare
3. Entrambi sono esonerati dal risarcimento se dimostrano che la violazione non gli è in alcun modo imputabile
4. Qualora ci siano più soggetti debitori, sono tutti responsabili in solido: cioè ciascuno può essere costretto a risarcire in toto il danno, salvo poi rivalersi sugli altri per la parte che compete loro



SANZIONI PECUNIARIE

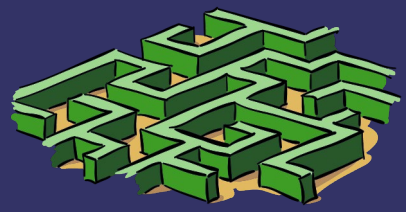
Art. 83 Par.2

Sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- Informativa
- Consenso
- Violazione dei principi applicabili al trattamento dei dati
- Violazione dei diritti dell'interessato
- Trasferimento dati all'estero

Sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- Obblighi del titolare
  - Violazione dei principi by design e by default
  - Registro delle attività
  - Sicurezza del trattamento

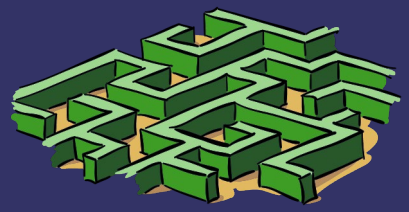


RESPONSABILITÀ PENALE

(Art 15 D.Lgs 101/2018)

Definita in base al tipo di illecito commesso, ma per lo più punita con la **reclusione.**

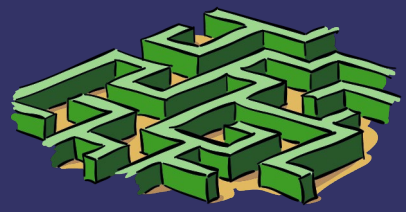
- Trattamento illecito per profitto, proprio o altrui, o per danneggiare l'interessato:
  - Di **dati** personali
    - dati comuni da 6 a 18 mesi
    - dati sanitari (GDPR art.9) o giudiziari (GDPR art. 10) o trasferimento all'estero degli stessi al di fuori dei casi consentiti (GDPR art. 45, 46 o 49) da 1 a 3 anni



RESPONSABILITÀ PENALE

(Art 15 D.Lgs 101/2018)

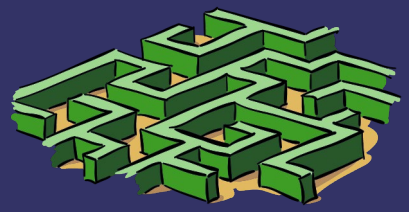
- **Trattamento illecito** per profitto, proprio o altrui, o per danneggiare l'interessato:
  - Di dati **oggetto di trattamento su larga scala**, quindi di archivio automatizzato o parte di esso
    - Comunicazione e diffusione illecita reclusione da 1 a 6 anni
    - Acquisizione fraudolenta di dati su larga reclusione 1-4 anni



RESPONSABILITÀ PENALE

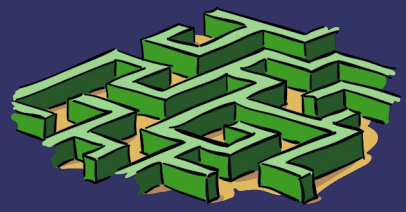
(Art 15 D.Lgs 101/2018)

- Illeciti verso il Garante:
  - Falsità di dichiarazioni o atti in un procedimento dinanzi al Garante da 6 mesi a 3 anni
  - Inosservanza provvedimenti del Garante: da 3 mesi a 2 anni



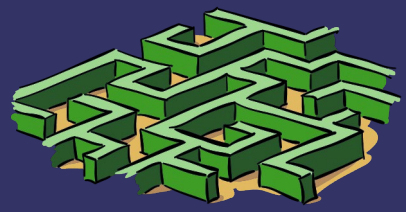
GESTIONE ARCHIVI

Sulla base del principio della privacy by design, della privacy by default e dell'accountability, ogni titolare deve adeguare le misure di sicurezza alla propria realtà, considerando che gli potrebbe essere chiesto di dimostrarne l'efficacia



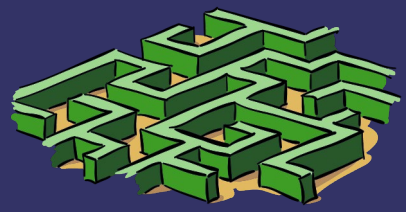
GESTIONE CARTACEA

- Conservazione documentazione sensibile (cartelle, radiografie, modelli studio..) in luogo sicuro
- Sotto chiave e accessibile solo agli incaricati
- Ove possibile pseudonimizzazione (es.negli invii al laboratorio) (codici numerici, prime 6 lettere C.F.)
- Non lasciare cartelle, agenda, lastre incustodite
- Cartelli di divieto d'accesso alle zone in cui vengono conservati dati sensibili
- Ordini di servizio su come comportarsi es. con esperto qualificato, tecnico autoclave…



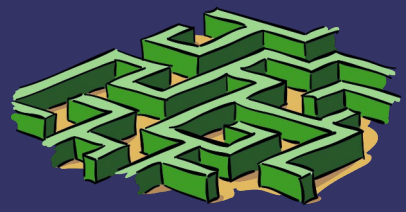
GESTIONE INFORMATIZZATA
Policy strumenti IT

È una sorta di vademecum in cui vengono descritte le modalità con le quali si gestiscono i dati informatizzati all'interno dello studio.
A partire dai problemi e dalle attenzioni che il trattamento di dati sensibili pone, il titolare esplicita le soluzioni adottate o da adottare allo scopo di rispettare il principio base della "responsabilizzazione" (accountability).



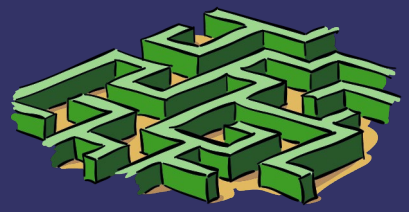
GESTIONE INFORMATIZZATA
Misure generali -1

- Password di accesso al database
  - individuale per incaricato e per tipologia di dati trattati
  - 8 caratteri
  - Rinnovata ogni 3-6 mesi
- Protezione (aggiornata!!!)
  - Firewall
  - Antivirus
  - Aggiornamenti del sistema operativo (patch di sicurezza) ogni 6 mesi
- Backup dei dati (ripristino max 7gg)
- Installazione Software su autorizzazione dello studio e con licenze o free

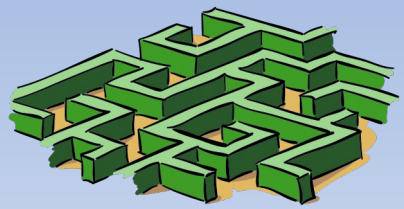


GESTIONE INFORMATIZZATA
Misure generali -2

- Posta elettronica SOLO dedicata ad attività
- Massima attenzione nell'aprire gli allegati
- Controllo accesso ad internet
- Screensaver con password e procedure di logout
- Criptazione messaggi (es. programma che cripta messaggio, lo invia, poi con chiave personalizzata, il paziente può decriptarla)
- Distruzione dei supporti rimovibili in disuso contenenti dati (HD, Pen Drive, Dischi esterni)

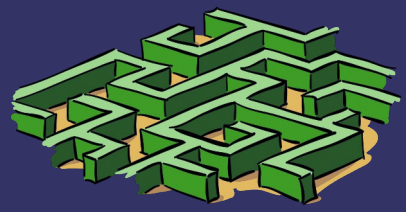


Concludendo…



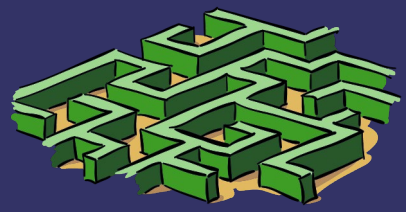
DOCUMENTI	GESTIONE CARTACEA	GESTIONE DIGITALE[2]
Informativa Persone Fisiche[1]	X	X
Consenso Persone Fisiche	X	X
Contratto per il trattamento dei dati (Responsabili)	X	X
Autorizzazione al trattamento dei dati personali in qualità di Amministratore di Sistema	-	N/O
Registro delle attività di trattamento (anche in formato elettronico) (art. 30)	X	X
Istruzioni per il Registro delle attività	In realtà N/O se impiega meno di 250 persone	
Elenco dei responsabili	X	X

1) Dipendenti, ditte individuali, collaboratori, pazienti
2) Anche solo la radiografia digitale colloca in questa gestione



DOCUMENTI	GESTIONE CARTACEA	GESTIONE DIGITALE(2)
Registri attività Responsabili	X	X
Policy strumenti IT + allegato 1		X
Policy Gestione Data Breach	X	X
Privacy Policy Sito	X	X
Policy base legale per il trattamento	X	X
Procedura per l'esercizio dei diritti dell'interessato	X	X
Policy sulla conservazione	X	X
• Formazione incaricati (art.5 com2)	X	X
Nomina DPO	N/O	N/O
DPIA	N/O	N/O

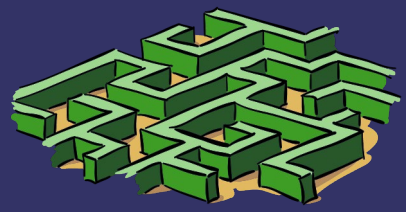
1) Dipendenti, ditte individuali, collaboratori, pazienti
2) Anche solo la radiografia digitale colloca in questa gestione



L'onere di dimostrare l'avvenuta formazione dei dipendenti è a carico del datore di lavoro

http://bit.ly/2mV6HZH

La protezione dei dati personali nello studio dentistico - Il GDPR e i dipendenti dello studio



Ma se non è obbligatorio…..

Rho 20 maggio 2018

Si istruiscono i suddetti incaricati al trattamento dei dati presso lo Studio Dentistico Associato Coronelli, circa le modalità di raccolta e trattamento degli stessi

Dati raccolti:
nome, cognome, indirizzo, telefono, email, cod. Fisc.(digitale)
Condizioni di salute generale (digitale e cartaceo)
dati sui trattamenti odontoiatrici effettuati e in corso (digitale e cartaceo)
radiografie odontoiatriche (digitale)
consenso al trattamento dei dati stessi (cartaceo)

Modalità:

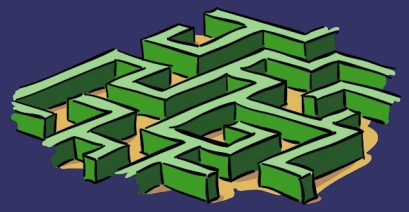
su pc, crittografati e protetti da password
su copia backup
su supporto cartaceo conservato in armadio in stanza non accessibile al pubblico se non sotto diretto controllo dei titolari o degli incaricati stessi, e, a fine giornata in armadio chiuso a chiave.

Trattamento:

ogni incaricato è tenuto alla riservatezza, al divieto assoluto di modifica se non sotto il diretto controllo dei titolari.
Il pc si trova in stanza con divieto di accesso diretto al pubblico e con screen saver automatico
Solo i titolari si occupano dell'aggiornamento delle cartelle, dei preventivi di cura e della fatturazione. Unica eccezione, la cartella ortodontica, aggiornata direttamente dal collaboratore dr.ssa Addamiano
L'incaricato si limita alla raccolta dei dati anagrafici, e alla gestione dell'agenda.

Per presa visione …..

i titolari del trattamento dati.



Gentile Sig.ra XXXXXX,

come intercorso questa mattina per le vie brevi, La informiamo che il Regolamento (UE) n. 2016/679, direttamente applicabile a partire dal 25 maggio scorso, prevede che gli interessati hanno il diritto di ottenere dal titolare del trattamento, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza va presentata al titolare del trattamento, che fornisce le informazioni richieste senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta. Al riguardo, può eventualmente essere utilizzato il **modello** predisposto dal Garante:

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1089924&zx=m2ia3q266lgt

Le rappresentiamo inoltre, che se ritiene che il trattamento dei dati che la riguardano non sia conforme alla disposizioni vigenti ovvero se la risposta ad un'istanza con cui esercita uno o più dei diritti previsti dagli articoli 15-22 del Regolamento (UE) 2016/679 non pervenga nei tempi indicati o non sia soddisfacente, l'interessato potrà rivolgersi all'autorità giudiziaria o al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'articolo art. 77 del Regolamento (UE) 2016/679.

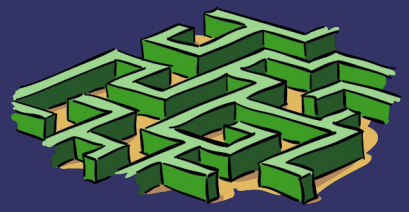
Può trovare ulteriori chiarimenti su tali aspetti nella Scheda informativa “Che cos'è il reclamo e come si presenta al Garante” reperibile al seguente link:

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/4535524&zx=mod9el8xtdlt

Nel ringraziare per l’attenzione prestata all’attività istituzionale del Garante, l'Ufficio Relazioni con il Pubblico resta a disposizione per eventuali ulteriori informazioni ai numeri indicati di seguito (lun-ven; ore 10-12,30).

Cordiali saluti.

Garante per la protezione dei dati personali
Ufficio Relazioni con il Pubblico
Piazza Venezia 11
00187 Roma
tel. 06.69677.2917 - fax 06.69677.3785
e-mail: urp@gpdp.it
posta certificata: protocollo@pec.gpdp.it



Di Dio conosciamo solo i primi 7 giorni perché, dopo, ha settato le impostazioni sulla privacy (da Twitter)

Grazie