Il pediatra di libera scelta e la normativa di dati personali: dal D.lgs. 196/03 al Regolamento Europeo 2016/679

Aspetti sanzionatori e analisi di casi concreti

A cura di
Luigi Guerra
Avvocato e Data Protection Officer (DPO)
Bari 21.04.2018

ARGOMENTI

1. Glossario;
2. Principi fondamentali;
3. Informativa privacy;
4. Consenso privacy;
5. Le nomine obbligatorie;
6. Registro del trattamento;
7. Misure di sicurezza;
8. Data breach;
9. Ulteriori adempimenti del PDS;
10. Valutazione d'impatto privacy;
11. Dpo;
12. Responsabilità del PDS;

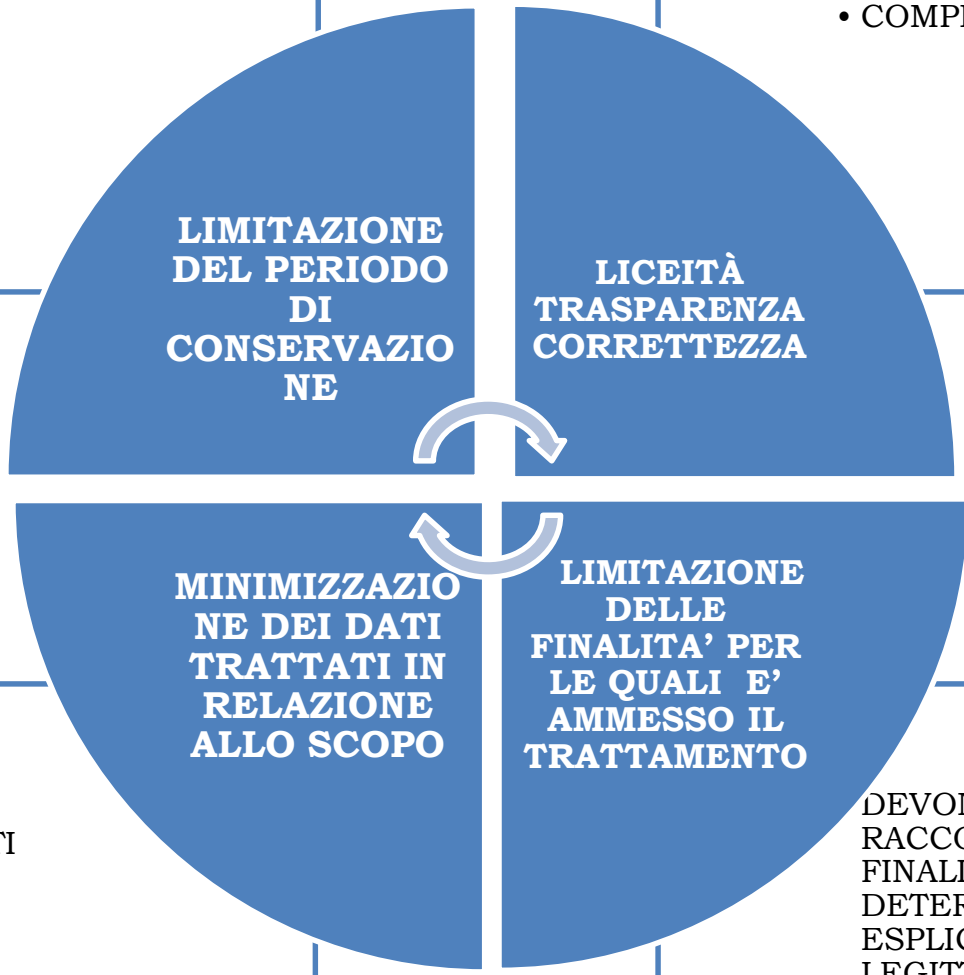
Regolamento UE 2016/679: Breve glossario

- **GDPR:** Regolamento generale sulla protezione dei dati (UE 2016/679)
- **Titolare del trattamento:** persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo (associazioni ed enti) che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
- **Responsabile del trattamento:** persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
- **Incaricato del trattamento (nuovo soggetto autorizzato):** persona fisica autorizzata a compiere operazioni di trattamento sulla base di istruzioni ricevute dal Titolare o Responsabile.
- **Interessato dal trattamento** persona fisica cui si riferiscono i dati.
- **Trattamento:** Un'operazione o un complesso di operazioni che hanno per oggetto dati personali. La raccolta, la registrazione, l'organizzazione, la conservazione, la modificazione, la selezione, l'estrazione, l'utilizzo, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

Principi applicabili al trattamento di dati personali Art. 5 GDPR

- UNO
- CINQUE
- DIECI

- ART. 6 GDPR;
- COMPRENSIBILITÀ



- ADEGUATI
- PERTINENTI
- LIMITATI

DEVONO ESSERE RACCOLTI PER FINALITÀ DETERMINATE, ESPLICITE E LEGITTIME

Gli adempimenti del PDS

INFORMATIVA ART. 13 GDPR

Cosa deve contenere:

- Identità e dati di contatto del Titolare del Trattamento;
- Dati di contatto DPO (ove obbligatorio);
- Finalità e modalità del trattamento;
- Obbligo o facoltà del conferimento dati e conseguenze del rifiuto;
- Soggetti o categorie a cui vengono comunicati (consultati);
- Periodo di conservazione;
- I diritti consentiti: Accesso, Rettifica, Cancellazione, Revoca, Limitazione, Opposizione, Portabilità, Reclamo.

Informativa Art. 78 (42) Codice Privacy

1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati nell'articolo 13, comma 1.

2. L'informativa può essere fornita per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal PEDIATRA a tutela della salute dell'interessato [...].

3. L'informativa può riguardare, altresì, dati personali eventualmente raccolti presso terzi, ed è fornita preferibilmente per iscritto, anche attraverso carte tascabili con eventuali allegati pieghevoli, includendo almeno gli elementi indicati dal Garante ai sensi dell'articolo 13, comma 3, eventualmente integrati anche oralmente in relazione a particolari caratteristiche del trattamento.

4. L'informativa, se non è diversamente specificato dal medico o dal pediatra, riguarda anche il trattamento di dati correlato a quello effettuato dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

a) sostituisce temporaneamente il medico o il pediatra;

b) fornisce una prestazione specialistica su richiesta del pediatra;

c) nell'ambito di un'attività professionale prestata in forma associata;

d) fornisce farmaci prescritti;

5. L'informativa evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, in particolare in caso di trattamenti effettuati:

a) per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, [...], ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;

b) nell'ambito della teleassistenza o telemedicina;

c) per fornire altri beni o servizi all'interessato [...].

d)Per Fascicolo sanitario elettronico

Informativa consigli utili

- Quando fornirla?
- Come fornirla?
- Dove esporla?
- Sostituto temporaneo?
- Faccio parte di associazione in rete o gruppo?
- Ricerca scientifica? Sperimentazione? Telemedicina?
- Segretaria ed infermiere?
- Informativa anche per trattamento correlato! (Specialista, Farmacista)
- Confronto e consulto con collega e/o specialista?

Consenso
Evoluzione legislativa

Consenso Evoluzione legislativa

L'art. 9 del GDPR relativo al trattamento dei dati relativi alla salute, prevede infatti che non sia necessario il consenso "per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale […]".

La norma lascia però agli Stati membri la possibilità di "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute" (comma 4).

Quindi in linea di principio il legislatore nazionale avrebbe ben potuto mantenere in vita il consenso "scritto" per i c.d. dati sensibili, come previsto oggi del Codice Privacy.

La scelta invece è stata più in linea con il Regolamento UE.

L'articolo 8 della bozza del decreto infatti, rubricato "Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute", prevede che il trattamento di queste particolari categorie di dati non sia subordinato al consenso scritto ma solo all'osservanza di misure di garanzia, stabilite dal Garante per la protezione dei dati personali con provvedimento adottato con cadenza almeno biennale, a seguito di consultazione pubblica.

Consenso ad oggi SI

Art. 76 Cod. Privacy: Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, [...], trattano i dati personali idonei a rivelare lo stato di salute:

a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;

Il **consenso,** in base al nuovo Regolamento Generale (art. 4 GDPR), è qualsiasi **manifestazione di volontà libera, specifica, informata e inequivocabile** dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Non è ammesso il consenso tacito o presunto

No a caselle pre-spuntate su un modulo

Consenso consigli utili

Minore, chi firma?

Il consenso dei minori è valido a partire dai 16 anni.

Il consenso di entrambi i genitori (che esercitano la responsabilità) è necessario solo per gli atti di straordinaria amministrazione che implicano modifiche nei diritti o nella sfera economica del soggetto minore.

Per gli atti di ordinaria amministrazione è sufficiente il consenso di un solo genitore, in applicazione del principio generale che gli atti di ordinaria amministrazione possono essere compiuti disgiuntamente da ciascun genitore (art. 320 Codice Civile). In questi casi il consenso dell'altro è considerato implicito.

Consiglio: RACCOGLIERE IL CONSENSO DI ENTRAMBI

Consenso consigli utili

Comunicazione stato di salute e consegna documentazione

Familiari, conoscenti e Baby sitter?

Formula: autorizzo e presto consenso affinché il Dott. Guerra comunichi la mia condizione clinica e consegni ogni tipo di documentazione, incluse ricette e referti, alle seguenti persone:

Predisporre modelli di delega per ritiro documentazione.

Nomina responsabile del trattamento Art. 28 GDPR

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico (…), che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Responsabili del Trattamento consigli utili

Chi nominare responsabile (esterno) del trattamento?

1. Medici sostituti e Associazione in rete o gruppo;

   Il medico titolare del trattamento nomina responsabili del trattamento tutti i componenti della rete o gruppo, per finalità di continuità assistenziale e cura.

   No cootitolare – No incaricato o soggetto autorizzato

2. Consulente fiscale e paghe;
3. Software gestionali (conformità al GDPR);
4. Tecnico informatico (*);

*lettera di riservatezza o ADS

Soggetto autorizzato al trattamento (incaricato del trattamento)

Art. 29 GDPR «Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali ***non può trattare tali dati se non è istruito in tal senso dal titolare*** *…».*

I soggetti autorizzati, corrispondono agli ex incaricati del codice privacy e sono, tutti coloro che trattano dati personali. Essi dovranno essere appositamente nominati mediante una lettera di designazione contenete dettagliate istruzioni sui trattamenti che dovranno svolgere.

Soggetto autorizzato consigli utili

Chi nominare?

Segretaria, Infermiere, Medici in formazione e Tirocinanti

Come nominare?

Per iscritto, controfirmata, specificando l'ambito del trattamento consentito e istruendo puntualmente su cosa gli è consentito e come deve svolgerlo

La segretaria può accogliere i pazienti in studio e fissare appuntamenti. Non può accedere ai dati sanitari e prescrivere farmaci.

Registro del trattamento Art. 30 GDPR

L'obbligo di redazione e adozione del registro non è generale: infatti l'art. 30 specifica che esso non compete "alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati."

Registro del trattamento Art. 30 GDPR

Cosa deve contenere il registro del trattamento dati

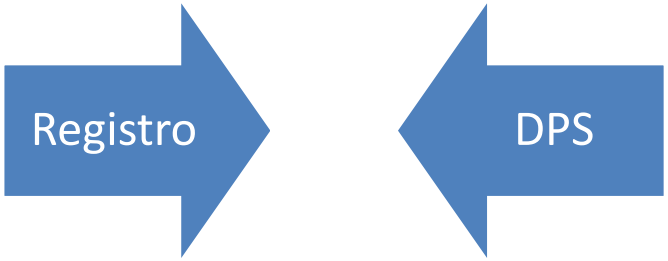
- **Il nome e i dati di contatto del titolare del trattamento** e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati (DPO);
- Le **finalità** del trattamento;
- La descrizione delle **categorie di interessati** e delle **categorie di dati personali**;
- Le **categorie di destinatari** a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- Se presenti, i **trasferimenti di dati personali verso paesi terzi** e la loro identificazione;
- I **termini ultimi** previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.

Questo registro rappresenta una delle novità e, al tempo stesso, uno degli adempimenti più importanti concernenti le attività di trattamento.

Registro del trattamento Art. 30 GDPR

Tenuto anche in formato elettronico dal Titolare del trattamento dei dati, tale registro **dovrà essere messo a disposizione dell'Autorità Garante** qualora lo richieda, così come è previsto dal par. 4 dell'art. 30.

Consigli: aggiornalo periodicamente



Sicurezza del trattamento Art. 32 GDPR (Misure di sicurezza)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **MISURE TECNICHE E ORGANIZZATIVE** adeguate per garantire un livello di sicurezza adeguato al rischio.

Sono considerate dal GDPR tecniche efficaci per garantire una reale protezione delle informazioni, soprattutto sensibili.

Consiglio: effettuare prima un'analisi del rischio!

Sicurezza del trattamento Art. 32 GDPR (Misure di sicurezza)

comprendono, **tra le altre, se del caso (lista aperta e non esaustiva)**:

a) la pseudonimizzazione e la cifratura dei dati personali;

La pseudonomizzazione è il trattamento eseguito in modo tale che i dati personali non possano più essere attribuiti all'interessato senza l'utilizzo di informazioni aggiuntive. Condizione essenziale: tali informazioni aggiuntive devono essere conservate separatamente.

La Cifratura si basa di solito su algoritmo di cifratura e su una password (molto complessa) che «apre» e «chiude» i dati al momento dell'autentificazione.

Consiglio: Creare delle policy per una corretta gestione del sistema di cifratura e pseudonomizzazione.

Sicurezza del trattamento Art. 32 GDPR (Misure di sicurezza)

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

riservatezza, ovvero la protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la lettura da parte di persone non autorizzate;

integrità, come conferma che i dati trasmessi, ricevuti o conservati siano completi e inalterati;

disponibilità, come conferma che i dati siano accessibili e i servizi funzionino anche in caso di interruzioni dovute a eventi eccezionali o ad attacchi di pirateria informatica.

Sicurezza del trattamento Art. 32 GDPR (Misure di sicurezza)

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

Esempio: policy su disaster recovery

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Dimostrare non solo la conformità, ma anche che le misure di sicurezza abbiamo effettivamente funzionato

Misure di sicurezza

Le misure MINIME di sicurezza (Allegato b Cod. Privacy):

1. Password Alfanumerica 8 caratteri pc;
2. Modificare password ogni tre mesi;
3. Aggiornare il sistema operativo;
4. Dotarsi di firewall;
5. Antivirus;
6. Back-up almeno settimanale;
7. Soggetto autorizzato credenziali e ambito di trattamento;
8. Custodia supporti removibili.

<u>Dopo il 25 maggio non esisterà più l'obbligo di adottare tali misure, poiché la valutazione su quale misura di sicurezza utilizzare, spetterà al titolare del trattamento.</u>

Misure di sicurezza consigli utili

- Il collega sostituto deve accedere all'archivio o al gestionale del titolare con proprie credenziali;
- Gli accessi devono essere configurati in modo tale che solo se un medico è chiamato a sostituire il titolare, possa vedere e modificare quei dati;
- E' buona prassi che il medico sostituto avvisi il paziente che si sta accedendo e modificando la propria cartella;
- Attivare il salva-schermo;
- Consegna ricette e documenti chiusi in busta;
- Mai mettere a disposizione degli assistiti i documenti da ritirare in uno scaffale nella sala d'attesa;(Garante Privacy dic. 2014).
- Distanze di cortesia (riservatezza colloqui);
- In sala d'attesa chiamare il proprio paziente per nome;
- Non affiggere in sala d'attesa liste di pazienti in attesa o prenotati;
- Inserire avvisi in calce alle e-mail;

Misure di sicurezza consigli utili

- Mai condividere sui social nomi e foto di pazienti;
- Mai chiedere al paziente in sede di accettazione informazioni su HIV, salvo tale dato non risulti indispensabile per la terapia. In ogni caso tale dato può raccoglierlo solo il dottore!
- Mai lasciare documentazione sanitaria (libretto pediatrico) incustodita (istruire la segretaria);
- Armadi e archivi con chiavi, idem per armadi rack contenenti server-nas;
- Mai dismettere supporti removibili (USB- Nas) senza procedura di cancellazione sicura (RAEE);
- Utilizzare sempre distruggi documenti per dati sanitari e non;
- Mai indicare la diagnosi nel certificato scolastico;
- Mai aprire e-mail di dubbia provenienza (Cryptolocker)

Violazione di dati personali (data breach) Art. 33 GDPR

Per **violazione dei dati personali (*data breach*)** si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati.

Violazione di dati personali (data breach) Art. 33 GDPR

- Un data breach, quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente).
- Il GDPR prescrive la NOTIFICA al Garante Privacy entro 72 ore dall'evento, salvo che sia improbabile che la violazione presenti rischi per i diritti delle persone fisiche.

Data Breach consigli utili

- Utilizzare le tecniche di cifratura e pseudonomizzazione (i dati «rubati» saranno incomprensibili);
- Contratto assicurativo per coprire i danni derivanti dalla violazione dei dati;

Ulteriori adempimenti del PDS

Predisporre moduli (chiari e facilmente accessibili) per diritti dell'interessato:

- Diritto di accesso Art. 15 GDPR;
- Diritto di rettifica Art. 16 GDPR;
- Diritto alla cancellazione – Oblio Art. 17 GDPR;
- Diritto alla limitazione del trattamento Art. 18 GDPR;

Risposta chiara, concisa e gratuita entro un mese.

Informativa dipendenti

Ulteriori adempimenti del PDS

LA FORMAZIONE

L'art. 29 del GDPR prevede: "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali* ***non può trattare tali dati se non è ISTRUITO in tal senso dal titolare*** *…*".

Corsi base e per settore sanitario, per segretarie e/o collaboratori.

Formazione ruolo centrale per dimostrare l'accountability.

Valutazione d'impatto protezione dati Art. 35 GDPR

SINGOLO PEDIATRA

- VIP: Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati. *Considerando 91 GDPR*

Data protection officer (DPO)

CHI È IL DPO

Il DPO è un soggetto che facilita l'osservanza delle disposizione GDPR.

Il GDPR riconosce nel DPO uno degli elementi chiave all'interno del nuovo sistema di governance dei dati.

COMPITI DEL DPO:

- Sorveglia l'osservanza del GDPR;
- Fungere da **punto di contatto per gli interessati** in merito alle problematiche connessa al trattamento dei loro dati;
- Cooperare con l'Autorità di controllo, fungere da **punto di contatto per l'Autorità di controllo**;
- Fornire, se richiesto, **pareri in merito alla valutazione d'impatto sulla protezione dei dati**;
- Verificare che le policy interne del titolare siano correttamente applicate e attuate;
- Formazione costante del personale e audit interni.

Data protection officer (DPO)

Art. 37GDPR -LA DESIGNAZIONE DEL DPO È OBBLIGATORIA IN TRE CASI:

Se le attività principali del titolare consistono nel trattamento su larga scala di categorie particolari di dati [sanitari] o di dati personali relativi a condanne penali e reati.

SINGOLO PEDIATRA

Alcuni esempi di trattamento **non** su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario; *Fonte: Linee guida WP-29 su DPO*

Il singolo pediatra non dovrebbe nominare il DPO

E L’ASSOCIAZIONE IN RETE O IL GRUPPO NOMINA IL DPO E EFFETTUA LA VALUTAZIONE D’IMPATTO PRIVACY?

Responsabilità del PDS

Chi può chiedere il risarcimento dei danni?

Chiunque subisca un danno materiale o immateriale causato da una violazione del regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Chi è responsabile del risarcimento del danno?

Innanzi tutto al risarcimento di danni causati da un trattamento che violi il regolamento è tenuto il titolare del trattamento. Il responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili del trattamento o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

A quali condizioni non scatta la responsabilità?

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Si applica la cosiddetta inversione dell'onere della prova.

Avv. Luigi Guerra

Master Data Protection Officer Roma Tre
Consulente Privacy certificato TUV Italia cdp_149
Delegato Barletta-Andria-Trani Federprivacy

Contatti:

Studio: Via Canne n. 21 Barletta
Cellulare: 328/9699210
Email: guerra_luigi@yahoo.it