Regolamento UE 679/2016
analisi delle principali novità

MILANO 20121 • Via del Lauro 9
tel +39 0289836800 fax + 39 0289836899
milano@crealaw.com

PIACENZA 29100 • Via S. Eufemia 28
tel +39 0523 334670 fax +39 0523 331780
piacenza@crealaw.com

crealaw.com

Regolamento europeo 2016/679

«*Regolamento europeo concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati*»

- approvato dal Parlamento europeo il 14 aprile 2016
- direttamente applicabile dal 25 maggio 2018

Principi

La protezione dei dati personali è un diritto fondamentale (art. 8 par. 1 Carta dei diritti fondamentali dell'Unione Europea)

Il diritto alla protezione dei dati non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e contemperato con altri diritti fondamentali (Considerando 4)

Al fine di assicurare un livello coerente e elevato di protezione delle persone e rimuovere gli ostacoli alla circolazione dei dati personali, il livello di protezione dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali deve essere equivalente in tutti gli Stati membri (Considerando 10)

Ove il regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, **gli Stati membri possono nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone integrare elementi del regolamento nel proprio diritto nazionale** (Considerando 8)

Adeguamento normativa naziona

Per quanto riguarda il trattamento dei dati personali … per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del regolamento (Considerando 10)

Decreto Legislativo 10 agosto 2018, n. 101 «*recante disposizioni per l'adeguamento della normativa nazionale ………………*»
(in vigore dal 19 settembre 2018)
Non sono abrogati i provvedimenti del Garante

Elementi essenziali 4

Ambito di applicazione materiale e territoriale

Si applica:

- solo al trattamento di dati personali di persone fisiche
- ai trattamenti interamente o parzialmente automatizzati o non automatizzati se i dati personali sono contenuti in un archivio o sono destinati a confluirvi

Si applica ai trattamenti effettuati:

- da un Titolare o Responsabile stabilito nell'UE, anche se il trattamento è effettuato fuori dall'UE
- effettuati da un Titolare o Responsabile non stabilito nell'UE se il trattamento ha ad oggetto dati personali di interessati che si trovano nell'UE
- effettuati da un Titolare stabilito in uno Stato extra UE soggetto al diritto di uno Stato UE in virtù del diritto internazionale

Elementi essenziali 5

Ambito di applicazione materiale e territoriale

NON SI APPLICA ai trattamenti:

- **effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico**
- **di informazioni anonime o dati personali anonimizzati**
- per attività che non rientrano nel diritto dell'Unione (es. sicurezza nazionale)
- per attività di speciale rilevanza pubblica (es. politica estera e di difesa comune)
- effettuati da autorità ai fini di prevenzione, accertamento e repressione reati e ai fini di sicurezza pubblica

Principi

- **Liceità**
- **Correttezza**
- **Trasparenza – sensibilizzazione dei cittadini**
- **Finalità determinate esplicite legittime**
- **Minimizzazione – pertinenza e non eccedenza**
- **(Privacy by design – privacy by default)**
- **Esattezza**
- **Limitazione delle conservazione**
- **Integrità e sicurezza**
- **Responsabilizzazione**
- **Neutralità degli strumenti**

Principi

Privacy by Design e Privacy by Default

Art. 25 (“Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

N.B Tale adempimento va effettuato sia al momento di determinare i mezzi del trattamento (es: progettazione di device) sia all'atto del trattamento stesso (PRIMA DI EFFETTUARE IL TRATTAMENTO)

Principi

Approccio GDPR centrato sulla **<u>valutazione del rischio</u>** (*risk based approach*), con il quale si determina la misura di **<u>responsabilità</u>** (accountability) del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.

<u>Il GDPR comprende anche la definizione di rischio</u>:

Considerando 75

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Considerando 76

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Fondamenti di liceità del trattamento

Articolo 6 - Liceità del trattamento (Dati personali anagrafico-identificativi e contabili)

«Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;

Fondamenti di liceità del trattamento (segue)

d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.»

Fondamenti di liceità del trattamento (segue)

Articolo 9 - Liceità del trattamento (Categorie particolari di dati personali)

Non vi e’ la definizione di DATI SENSIBILI E GIUDIZIARI

CATEGORIE PARTICOLARI DI DATI

Dati sensibili

Dati relativi alla salute = dati sanitari (Considerando 35)

Dati genetici

Dati biometrici

Trattamento di categorie particolari di dati personali

9.1. **È vietato 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. (C51)

Basi giuridiche

Trattamento di categorie particolari di dati personali
Liceità

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (C51, C52)

a) l'interessato ha prestato il proprio **consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario **per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per **tutelare un interesse vitale dell'interessato** o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, **da una fondazione, associazione o altro organismo senza scopo di lucro** che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) e) il trattamento riguarda dati personali **resi manifestamente pubblici dall'interessato**;

f) il trattamento è necessario **per accertare, esercitare o difendere un diritto in sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario **per motivi di interesse pubblico** rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (C55, C56)

h) 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 o conformemente al contratto con un professionista della sanità**, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53)

i) 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, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54)

j) il trattamento è **necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici** in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Soggetti

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 (art. 4 GDPR)

Soggetti

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 (art. 4 GDPR)

Incaricato del trattamento

La persona fisica **autorizzata** a compiere le operazioni di trattamento dal titolare o dal responsabile del trattamento stesso (figura definita nel vecchio Codice Privacy, oggi prevista nei provvedimenti dell’Autorità Garante).

Data Proection Officer (DPO)

Figura **specializzata** e altamente **qualificata**, nominata dal titolare del trattamento quale responsabile per la protezione dei dati.

Obbligatorio solo in caso di:

- trattamento effettuato da parte della Pubblica Amministrazione;
- core business del titolare consiste nel monitoraggio regolare e sistematico su larga scala delle persone interessate;
- core business del titolare consiste nell'elaborazione di dati personali particolari su larga scala.

Adeguamento

FASI

1. MAPPATURA DEI TRATTAMENTI;
2. INDIVIDUAZIONE I RUOLI, LE RESPONSABILITA' E I COMPITI;
3. DEFINIZIONE MISURE DI SICUREZZA ADEGUATE;
5. DEFINIZIONE POLICY E PROCEDURE ORGANIZZATIVE;
6. DEFINIZIONE DI UNA PROCEDURA DI DATA BREACH;
7. DOCUMENTAZIONE DELLA CONFORMITA

Informativa

Obblighi di informativa rafforzati rispetto a quelli di cui all'art. 13 del Codice della privacy, con numerose informazioni aggiuntive da fornire agli interessati (Va resa per iscritto o con altri mezzi, anche elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente):

- ***in forma concisa**,*
- ***trasparente**,*
- ***intelligibile***
- ***facilmente accessibile**,*
- ***con un linguaggio semplice e chiaro**.*

<u>L'Informativa (due tipologie)</u>:

- ***Dati raccolti presso l'interessato** (art. 13)*
- ***Dati NON raccolti presso l'interessato** (art. 14)*

Informativa – i contenuti (art. 13)

- I dati del Titolare del trattamento
- Responsabile della Protezione dei Dati, se nominato
- Finalità e base giuridica del trattamento
- Interesse legittimo del Titolare se esistente
- Destinatari dei dati personali
- Intenzione di trasferire i dati all’estero (extra-U.E), se esistente
- Periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo

Informativa (segue)

- La specifica esistenza del diritto alla portabilità dei dati;
- L'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità basata sul consenso prestato prima della revoca;
- Il diritto di proporre reclamo al Garante privacy
- La eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;

Informativa art. 14

- Stesso contenuto di quella ex art. 13

IN AGGIUNTA

- L'indicazione delle categorie di dati oggetto del trattamento
- La fonte di origine dei dati personali

Consenso

<u>**CONSENSO**</u>:
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 (non vale il silenzio assenso)

<u>Se non ricorre una delle altre condizioni di liceità</u>:
Per le categorie particolari di dati:

- deve essere "esplicito"
- non è necessariamente "documentato per iscritto", né è richiesta la "forma scritta", ma il titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento
- il consenso dei minori è valido a partire dai 14 anni solo per i servizi della società dell'informazione, per il consenso al trattamento osteopatico il paziente deve avere compiuto i 18 anni di età → prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci

N.B. **MEGLIO CHIEDERLO SEMPRE E SEMPRE IN FORMA SCRITTA!**

REGISTRO DEI TRATTAMENTI

Se l'azienda (o l'ente) ha più di 250 dipendenti o svolge trattamenti che riguardano dati particolari, giudiziari o che comportano un rischio per i diritti e le libertà degli interessati

DEVE

- PREDISPORRE E MANTENERE AGGIORNATO UN REGISTRO DEI TRATTAMENTI E ASSICURARSI
- CHE RISPETTINO I PRINCIPI PREVISTI DAL REGOLAMENTO

- Se l'azienda ha meno di 250 dipendenti e il trattamento svolto non riguarda dati particolari, giudiziari o non comporta mai un rischio per i diritti e le libertà degli interessati

DEVE

VALUTARE LA PREDISPOSIZIONE DI UN REGISTRO DELLE ATTIVITÀ ANCHE SE NON OBBLIGATORIO.

REGISTRO DEI TRATTAMENTI

Per il Garante Privacy:

Si tratta di uno strumento fondamentale per disporre di un quadro aggiornato dei trattamenti in essere. I contenuti minimi sono indicati all'art. 30 del Regolamento. Deve avere forma scritta, anche elettronica, e va esibito su richiesta al Garante.

DI FATTO E' UN ADEMPIMENTO OBBLIGATORIO

REGISTRO DEI TRATTAMENTI

L'art. 30 - il Registro contiene per ogni trattamento le seguenti informazioni:

• I differenti trattamenti di Dati personali;
• Le categorie di Interessati e di dati personali trattati;
• Le finalità del Trattamento;
• I soggetti interni ed esterni coinvolti nel Trattamento di dati, tra cui l'elenco degli incaricati;
• Il flusso di Dati, in caso di trasferimento di Dati extra UE;
• Il luogo in cui i Dati sono conservati;
• Per ciascuna categoria di dati il tempo di conservazione;
• Le misure di sicurezza adottate per minimizzare i rischi.

REGISTRO DEI TRATTAMENTI

SCHEDA REGISTRO DEI TRATTAMENTI – MODELLO DELLA AUTORITA' GARANTE							
TITOLARE (inserire la denominazione e i dati di contatto del titolare							
RESPONSABILE DELLA PROTEZIONE DEI DATI [inserire la denominazione e i dati di contatto], se nominato							
TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI	TRASFERIMENTO DATI VERSO PAESI TERZI O ORG. INT.	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
Gestione attività di trattamento osteopatico	Erogazione prestazioni di osteopatia	Pazienti	Dati relativi alla salute	Pazienti	N/A	i dati, raccolti nella relativa scheda , verranno conservati a tempo indeterminato, perdurando il rapporto contrattuale di cura. Al termine del rapporto contrattuale di cura, saranno conservati un periodo non superiore al termine prescrizionale di legge per la tutela dei propri diritti legali e di difesa.	Vedi scheda

Misure di sicurezza

Misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio 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

Misure di sicurezza art. 32

Misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio 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 tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

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

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

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

Data breach

Obbligo di notifica all’Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche

Obbligo di documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio

Obbligo di comunicare la violazione all'interessato senza ingiustificato ritardo quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche

In sintesi

CHE FARE?

- Nominare il Titolare e il Responsabile e gli eventuali Responsabili esterni con relative lettere di incarico
- Dichiarare gli incaricati e dar loro lettere di incarico, mansionari e policy privacy
- Redigere un registro dei trattamenti con tutte le indicazioni di legge
- Eventualmente redigere un Privacy Impact Assessments con tutte le indicazioni di legge
- Predisporre i registri per il data breach e la modifica dei trattamenti.
- Predisporre tutta la documentazione per la videosorveglianza
- Stampare idonee informative e raccolta consensi
- Valutare quanto il proprio sito web sia a norma

Grazie per l'attenzione
Avv. Marco Chiesara
m.chiesara@crealaw.com

MILANO 20121 • Via del Lauro 9
tel +39 0289836800 fax + 39 0289836899
milano@crealaw.com

PIACENZA 29100 • Via S. Eufemia 28
tel +39 0523 334670 fax +39 0523 331780
piacenza@crealaw.com

crealaw.com