INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

Istituto di Teoria e Tecniche dell'Informazione Giuridica
Consiglio Nazionale delle Ricerche

FONDAZIONE per la FORMAZIONE FORENSE dell'ORDINE degli AVVOCATI di FIRENZE
SCUOLA FORENSE

INFORM DAY

Regolamento europeo sulla protezione dei dati e settore giudiziario

Avv. Prof. Giorgio Giannone Codiglione

Firenze, Nuovo Palazzo di Giustizia
26 novembre 2018

Il nuovo Regolamento Generale sulla protezione dei dati personali - GDPR (679/2016/UE)
Novità e profili applicativi

Il nuovo Regolamento Generale sulla protezione dei dati personali - GDPR (679/2016/UE)
Le novità (1)

- L'ambito di applicazione materiale del GDPR riguarda principalmente il settore del mercato interno, con l'esclusione di attività quali ad esempio la cooperazione di polizia e giudiziaria in materia penale (regolate dalla direttiva 680/2016) e le comunicazioni elettroniche (oggetto di un autonomo Regolamento, ancora al vaglio del legislatore comunitario).

- Il GDPR non si applica al trattamento di dati effettuato da persone fisiche esclusivamente per finalità di carattere personale o domestico (v. *infra*)

- <u>Accesso semplificato ai propri dati</u>: obbligo di fornire maggiori informazioni sul trattamento dei propri dati, in un linguaggio semplice e chiaro.

- <u>Diritto alla portabilità dei dati</u>: interoperabilità e trasferimento dei propri datipersonali tra prestatori di servizi.

- <u>Diritto all'oblio e alla cancellazione</u>: quando l'interessato si oppone al trattamento dei propri dati – e ammesso che non sussistano ragioni legittime per la sua effettuazione – i dati devono essere cancellati o rimossi dagli indici di ricerca.

Il nuovo Regolamento Generale sulla protezione dei dati personali - GDPR (679/2016/UE)
Le novità (2)

- **Consenso : qualora il trattamento dei dati personali sia basato sul consenso dell'individuo interessato, il consenso deve essere prestato in modo chiaro e intellegibile.**

- **Responsabilizzazione dei titolari del trattamento (*accountability*): valutazioni del rischio derivante dal trattamento dei dati e individuazione di responsabili della protezione dei dati (DPO).**

- **Norme europee sul suolo europeo: alle imprese stabilite fuori dal territorio dell'Unione europea si applicano le medesime norme qualora offrano servizi nell'ambito dell'Unione.**

- **Un continente, una legislazione: il GDPR stabilisce un unico insieme di norme che rende più**

- **Protezione dei dati "by design" e "by default": Garanzie per la protezione dei dati dovranno essere incorporate in prodotti e servizi già a partire dalle prime fasi del loro sviluppo e impostazioni di sicurezza predefinite saranno la norma, ad es.,sui social network o nelle applicazioni per la telefonia mobile.**

- **Rimedi giudiziari e amministrativi più incisivi: sanzioni amministrative per un importo fino al 4% del fatturato globale annuo.**

Le Autorità di controllo: compiti e novità

- Il GDPR stabilisce che ogni Stato membro deve garantire che le autorità di controllo monitorino l'applicazione del regolamento.
- **Funzione di controllo *ex post***: abolizione della notifica preventiva dei trattamenti all'autorità di controllo e del *prior checking* (c.d. verifica preliminare).
- ***Data Breach***: Tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.
- Le persone interessate i cui dati sono trattati in modo incompatibile con il regolamento hanno il diritto specifico di **proporre reclamo** a un'autorità di controllo (articolo 77) e le autorità di controllo devono informare il reclamante dello stato o dell'esito del reclamo.
- **Codici di condotta**: forniscono linee guida per i titolari del trattamento o responsabili del trattamento circa la precisa applicazione del GDPR e sono indicatori dell'ottemperanza di un'organizzazione alle disposizioni del regolamento; i codici di condotta devono essere approvati dalla competente autorità di controllo.
- **C.d. Autorità di controllo capofila (*one stop shop*)**: autorità di controllo dello stabilimento principale o unico nell'Ue del titolare o responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre autorità di controllo (definite, in questo caso, "autorità interessate") per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile.

Il d.lgs. n. 101/2018 di armonizzazione del Codice (d.lgs. 196/2003) al GDPR (1)

<u>Il decreto, in vigore dal 19 settembre, introduce queste novità:</u>

a) per i **<u>primi otto mesi dall'entrata in vigore del GDPR</u>** (dunque sino al maggio 2019), nell'erogare le sanzioni, il Garante per la protezione dei dati personali tiene conto del fatto di essere ancora in una fase iniziale di attuazione della normativa;

b) il consenso dei minori italiani sin dall'età di 14 anni per il trattamento dei dati personali nella fruizione dei servizi della società dell'informazione;

c) la possibilità, per il titolare e il responsabile, di nominare persone fisiche espressamente designate per svolgere specifici compiti e funzioni in relazione al trattamento dei dati personali;

Il d.lgs. n. 101/2018 di armonizzazione del Codice (d.lgs. 196/2003) al GDPR (2)

d) nei casi di ricezione di curriculum spontaneamente trasmessi al fine della instaurazione di un rapporto di lavoro, l'informativa deve esser fornita al momento del primo contatto utile dopo l'invio. Il consenso al trattamento dei dati personali presenti nel curriculum non è dovuto;

e) integrazione dell'art. 23 GDPR, lulla limitazione dell'esercizio dei diritti degli interessati (v. *infra*)

f) la gestione dei diritti riguardanti le persone decedute, che possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

Il nuovo Regolamento Generale sulla protezione dei dati personali - GDPR (679/2016/UE)
I ruoli soggettivi

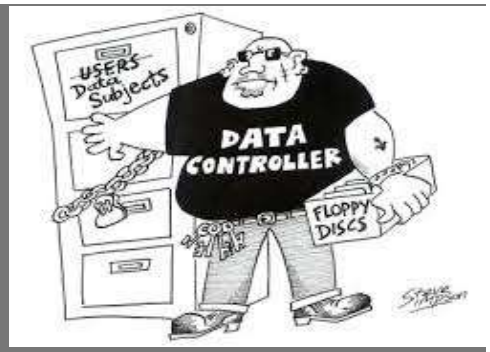
- **Titolare:** la persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali (sono qualificabili, ad es., come titolare la società, l'associazione professionale, l'avvocato, il commercialista, la fondazione, il consiglio dell'ordine, ecc.).

- **Contitolare**: l'art. 26 del GDPR prevede che in ogni caso in cui le finalità ed i mezzi del trattamento vengano determinati congiuntamente da parte di più titolari, potrà essere nominato uno o più "contitolare/i" del trattamento: il rapporto interno tra contitolari deve essere disciplinato da apposito accordo.

- **Responsabile**: la persona fisica o giuridica che tratta dati personali per conto del Titolare del trattamento. La nomina del Responsabile del trattamento deve avvenire con apposito atto scritto, contratto, o comunque per clausole tipizzate, e deve contenere gli elementi individuati dall'art. 28 del GDPR e tassativamente almeno le materie riportate al paragrafo 3 della medesima disposizione, al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento; le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel GDPR.

- Il Titolare e per il Responsabile possono avvalersi **di persone autorizzate "*al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*"** e secondo le finalità e le istruzioni da essi impartite.

Risk-Based Approach e trattamento dei dati personali (1)



Art. 4(1) - Nozione di dato personale : estesa a tutti i dati (anche quelli pseudonimi) che, anche a seguito di combinazione con altre informazioni, possano condurre all'identificazione di una persona fisica (cc.dd. trattamenti multipli).

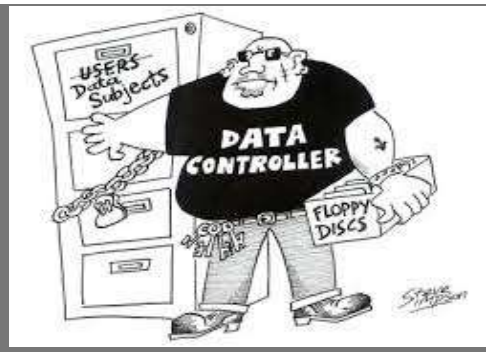
Art. 7 - Consenso: Il GDPR riafferma in maniera più incisiva il principio del consenso, affiancato ai doveri di informazione e trasparenza posti in capo al titolare o responsabile del trattamento. La disciplina è declinata in maniera analitica e puntuale anche con riguardo alla tutela di particolari figure soggettive, quali i minori (v. art. 8) e, ancora, con riferimento a particolari tipologie di trattamento dei dati (art. 9: dati relativi alla salute, genetici, biometrici ecc.).

Art. 6(4) – Trattamenti secondari: In assenza di consenso dell'interessato o di altro atto legislativo che sancisca la liceità dell'attività, il titolare è tenuto a valutare se il trattamento sia astrattamente conforme ai principi di necessità e proporzionalità di cui all'art. 23 del Regolamento , con particolare riguardo agli scopi perseguiti dal trattamento principale.

Art. 35 – Valutazione d'impatto e consultazione preventiva: Nelle ipotesi di trattamento avente "un elevato rischio per i diritti e le libertà delle persone fisiche", il titolare è tenuto ad attuare una valutazione preventiva dell'impatto delle attività sulla protezione dei dati personali e, ove lo ritiene opportuno, consulta preventivamente l'autorità nazionale di garanzia al fine di ottenere l'autorizzazione per svolgere il trattamento.

- **Registro dei trattamenti**: obbligatorio + 250 dipendenti

Risk-Based Approach e trattamento dei dati personali (2)



Consenso: limiti e deroghe (art. 6(1) GDPR)

Considerando n. 43: è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica. **Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.**

Trattamento necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.

Trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri.

Trattamento necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica.

Trattamento 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.

La c.d. *Accountability* (Responsabilizzazione) del titolare o responsabile del trattamento

- La responsabilizzazione richiede l'adozione attiva di misure da parte dei titolari del trattamento dei dati per la promozione e la salvaguardia della protezione dei dati nel corso delle loro attività di trattamento. Esempi di tali nuove misure sono:

1) L'obbligo di tenuta del registro dei trattamenti (+ 250 dipendenti, trattamenti rischiosi per i diritti e la libertà dell'interessato, non occasionale e avente come oggetto particolari tipologie di dati);
2) Obbligo di designazione del **Responsabile della protezione dei dati personali** (v. *infra*).

- I titolari del trattamento sono responsabili per e devono essere in grado di provare in ogni momento l'osservanza dei principi in materia di protezione dei dati alle persone interessate, al pubblico in generale e alle autorità di controllo.

- Il GDPR stabilisce nuovi obblighi in termini di responsabilizzazione che richiedono altresì l'adozione di nuove significative misure di carattere tecnico e organizzativo per dimostrare il rispetto del GDPR.

- Tali requisiti comprendono la privacy "by design", la notifica delle violazioni della sicurezza alle autorità di controllo, la nomina di un rappresentante del titolare o del responsabile del trattamento stabilito al di fuori del territorio dell'Unione europea, nonché la conduzione di valutazioni d'impatto sulla protezione dei dati per trattamenti a elevato rischio.

La responsabilità civile del titolare e/o del responsabile del trattamento: dal pericolo al rischio?

Art. 82 GDPR – Diritto al risarcimento e responsabilità

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

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. **Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.**

3. **Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile**.

Art. 15 "vecchio" Codice privacy

(Danni cagionati per effetto del trattamento)

1. **Chiunque cagiona** danno ad altri per effetto del trattamento di dati personali **è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.**
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 153 "nuovo" Codice privacy

(Autorità giudiziaria ordinaria)

1. Tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, **nonché il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo regolamento**, sono attribuite all'autorità giudiziaria ordinaria.

Le sanzioni amministrative pecuniarie (art. 83 GDPR)

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

Condizioni generali per infliggere sanzioni amministrative pecuniarie (2)

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

Condizioni generali per infliggere sanzioni amministrative pecuniarie (3)

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

(…)

Le altre sanzioni tra GDPR e n. 101/2018 (1)

L'art. 83 del Regolamento e l'art. 166 del Codice così come riformulato dal d.lgs. 101/2018, delineano il seguente quadro sanzionatorio amministrativo:

► **Sanzione amministrativa pecuniaria fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni delle seguenti disposizioni del regolamento (art. 83, par. 4):**

- obblighi del titolare e del responsabile del trattamento in relazione al consenso dei minori per i servizi della società dell'informazione (art. 8), al trattamento dati che non richiede identificazione (art. 11), al trattamento dati (artt. da 25 a 31), alla alla sicurezza dei dati personali (artt. da 32 a 34), alla valutazione di impatto e consultazione preventiva (artt. da 35 a 36), alla nomina del responsabile della protezione dati (artt. da 37 a 39); alla certificazione (artt. 42 e 43);

- obblighi dell'organismo di certificazione (artt. 42 e 43);

- obblighi dell'organismo di controllo eventualmente istituito per il monitoraggio dei codici di condotta (art. 41, par. 4).

Le altre sanzioni tra GDPR e n. 101/2018 (2)

<u>La stessa sanzione si applica, ai sensi dell'articolo 166 del codice, comma 1, a:</u>

- la violazione, da parte del titolare del trattamento, dell'obbligo di redigere con linguaggio particolarmente chiaro e semplice, comprensibile e accessibile al minore, le informazioni e le comunicazioni relativa al trattamento che lo riguardi (art. 2-quinquies, comma 2, del Codice);

- la violazione delle misure a garanzia dell'interessato introdotte dal Garante con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che può presentare rischi particolarmente elevati (art. 2-quaterdecies);

- violazione delle modalità di redazione e conservazione di cartelle cliniche (art. 92, comma 1);

- violazione delle disposizioni sulla redazione del certificato di assistenza al parto (art. 93, comma 1);
- violazione, da parte del titolare, degli obblighi di informativa all'utente sulla natura dei dati di traffico telefonico e telematico e sulla durata del trattamento (art. 123, comma 4);

- violazione, da parte del fornitore del servizio di comunicazione elettronica, degli obblighi relativi alla fatturazione dettagliata dei dati di traffico (art. 124), al trasferimento automatico della chiamata (art. 128) e violazione degli obblighi relativi alla sicurezza del trattamento (art. 132-ter);

- violazione del provvedimento del Garante di individuazione delle modalità di manifestazione del consenso all'inclusione negli elenchi telefonici cartacei e elettronici e all'utilizzo dei relativi dati per marketing (art. 129, comma 2).

Le altre sanzioni tra GDPR e n. 101/2018 (3)

►Sanzione amministrativa pecuniaria fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni delle seguenti disposizioni del regolamento (art. 83, par. 5):

- principi base del trattamento, comprese le condizioni del consenso (artt. da 5 a 7 e 9);
- diritti degli interessati (artt. da 12 a 22);
- trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale (artt. da 44 a 49);
- qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX del regolamento. Si tratta delle disposizioni che autorizzano gli Stati a dotarsi di una disciplina ulteriore con riferimento ai trattamenti che concernono la libertà di espressione e di informazione, ai trattamenti in ambito lavorativo, ai fini di archiviazione nel pubblico interesse;
- l'inosservanza di un ordine, di un provvedimento di limitazione del trattamento o di un ordine di sospensione dei flussi di dati adottato dall'autorità di controllo nell'ambito dei poteri correttivi (art. 58, par. 2);
- il diniego di accesso all'autorità di controllo che svolga poteri di indagine (art. 58, par. 1).

Le altre sanzioni tra GDPR e n. 101/2018 (4)

La stessa sanzione si applica, ai sensi dell'articolo 166 del codice, comma 2, a:

- la violazione delle disposizioni relative alla comunicazione e diffusione di dati personali da parte di titolari che effettuato il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 2-ter);
- la violazione, da parte del titolare del trattamento, delle disposizioni sul consenso dei minori in relazione ai servizi della società dell'informazione (art. 2-quinquies, comma 1);
- violazione delle norme sul trattamento di particolari categorie di dati personali per rilevanti motivi di interesse pubblico rilevante (2- sexies);
- la diffusione in dati genetici, biometrici e relativi alla salute (art. 2- septies, comma 7);
- violazione delle norme sul trattamento dei dati relativi a condanne penali (art. 2-octies);
- violazione delle disposizioni sul trattamento dei dati personali relativi a persone decedute (art. 2-duodecies);
- l'indicazione dei dati identificativi degli interessati in provvedimenti giurisdizionali in violazione della disciplina che consente all'interessato di precludere tale indicazione nella riproduzione dei provvedimenti (art. 52);
- la violazione della disciplina sul trattamento dei dati sanitari (art. 75),
- la violazione delle disposizioni sull'informativa da fornire all'interessato nell'ambito dei trattamenti sanitari, anche d'emergenza (artt. 78-80, 82)
- la violazione delle disposizioni sulla presa visione e il rilascio di cartella clinica a soggetto diverso dall'interessato (art. 92, comma 2);
- rilascio a terzi di certificato di assistenza al parto (art. 93, commi 2 e 3);
- la violazione delle disposizioni sulla comunicazione e diffusione di dati relativi a studenti (art. 96);

Le altre sanzioni tra GDPR e n. 101/2018 (5)

- la violazione delle disposizioni sulla durata del trattamento in caso di trattamento a fini di archiviazione nel pubblico interesse o di ricerca scientifica (art. 99)
- diffusione di dati per fini di studio da parte di università ed enti di ricerca (art. 100, commi 1, 2 e 4);
- modalità di trattamento di dati per scopi storici (art. 101), per scopi statistici e scientifici (art. 105, commi 1, 2 e 4);
- violazione delle disposizioni sul diritto di rettifica in relazione al trattamento dei dati relativi alla salute per fini di ricerca medica, biomedica ed epidemiologica (art. 110, comma 2);
- violazione delle regole deontologiche nei trattamenti in materia di lavoro e previdenza (art. 111);
- violazione della disciplina sull'informativa all'interessato nel primo contatto dopo la ricezione del curriculum (art. 111-bis);
- violazione delle disposizioni sul trattamento dei dati da parte degli istituti di patronato (art. 116, comma 1)
- trattamento e comunicazione di dati all'istituto di vigilanza sulle assicurazioni a fini di contrasto delle frodi assicurative (art. 120, comma 2);
- la violazione delle disposizioni sul trattamento di informazioni nell'apparecchio terminale del contraente o utente di servizi di comunicazione elettronica (art. 122);
- mancata cancellazione di dati relativi al traffico telefonico e telematico, conservazione degli stessi a fini di fatturazione oltre i sei mesi, mancato consenso al trattamento dei dati a fini di commercializzazione di servizi e trattamento da parte di soggetti diversi dal delegato (art. 123, commi 1, 2, 3 e 5);
- violazione, da parte del fornitore del servizio di comunicazione elettronica, degli obblighi relativi alla fatturazione dettagliata dei dati di traffico (art. 124);
- violazione dell'obbligo, a richiesta, di impedire l'identificazione della linea (art. 125);
- violazione delle disposizioni sui dati relativi all'ubicazione diversi dai dati del traffico (art. 126);
- violazione delle disposizioni sulle comunicazioni indesiderate (art. 130, commi da 1 a 4);

Le altre sanzioni tra GDPR e n. 101/2018 (6)

- violazione delle disposizioni su informazioni a contraenti e utenti (art. 131);
- violazione delle disposizioni sulla conservazione dei dati di traffico telefonico e telematico (art. 132);
- violazione degli obblighi per i fornitori dei servizi di comunicazione elettronica di fornire al Garante le informazioni sulle procedure interne (art. 132-bis, comma 2);
- violazione delle disposizioni sulle informazioni del fornitore ad abbonati e utenti sui rischi di violazioni della sicurezza (art. 132- quater);
- violazione delle regole deontologiche (art. 2-quater);
- violazione delle misure di garanzia e delle misure tecniche introdotte dal Garante in relazione ai dati genetici, biometrici e relativi alla salute (art. 2-septies).

La stessa sanzione si applica inoltre, in base all'articolo 166, comma 3 a:

- la comunicazione a terzi, il trasferimento e la diffusione di dati personali degli interessati iscritti al registro delle opposizioni da parte del titolare del trattamento, per fini di pubblicità o di vendita ovvero per il compimento di ricerche di mercato o di comunicazione commerciale non riferibili alle attività, ai prodotti o ai servizi offerti dal titolare del trattamento (art. 1, comma 9, L. n. 5/2018);
- la violazione del diritto di opposizione al trattamento di dati per fini di invio di materiale pubblicitario o di vendita diretta o per ilcompimento di ricerche di mercato o di comunicazione commerciale, mediante l'impiego del telefono; (art. 1, comma 10, L. n. 5/2018).

La legge n. 5 del 2018, che ha tra l'altro regolamentato il registro delle opposizioni, ha previsto, per le suddette violazioni di cui ai commi 9 e 10 dell'articolo 1, il rinvio alle sanzioni di cui all'articolo 162, comma 2-bis, del Codice della privacy: si applica dunque attualmente a tali violazioni la sanzione amministrativa pecuniaria da 10 mila a 120 mila euro. Con l'abrogazione dell'art. 162 da parte dello schema (art. 27), la violazione delle disposizioni sul registro delle opposizioni resterebbe priva di sanzione. L'articolo 166, comma 3, prevede quindi l'applicazione delle più severe sanzioni previste dal Regolamento UE.

Il GDPR nel sistema giudiziario: Princìpi generali

La protezione dei dati personali in ambito giudiziario nel GDPR (1)

- **Ambito di applicazione (art. 23, considerando nn. 20, 97):**

Il GDPR **si applica anche alle attività delle autorità giurisdizionali e di altre autorità giudiziarie,** ma il diritto dell'Unione o degli Stati membri può specificare le operazioni e le procedure di trattamento relativamente al trattamento dei dati personali effettuato da tali autorità.

Per i trattamenti effettuati da un'autorità pubblica, **eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, (…), o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati**, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento.

- **Controllo sulle violazioni (considerando n. 20):**

Non è opportuno che rientri nella competenza delle autorità di controllo il trattamento di dati personali effettuato dalle autorità giurisdizionali nell'adempimento delle loro funzioni giurisdizionali, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento dei suoi compiti giurisdizionali, compreso il processo decisionale. Si dovrebbe poter affidare il controllo su tali trattamenti di dati **ad organismi specifici all'interno del sistema giudiziario** dello Stato membro, che dovrebbero in particolare assicurare la conformità alle norme del presente regolamento, rafforzare la consapevolezza della magistratura con riguardo agli obblighi che alla stessa derivano dal presente regolamento ed esaminare i reclami in relazione a tali operazioni di trattamento dei dati.

La protezione dei dati personali in ambito giudiziario nel GDPR (2)

- **Deroga al divieto di trattamento di particolari categorie di dati (Art. 9; considerando n. 52):**

Art. 9(1) GDPR: "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".

La deroga dovrebbe anche consentire di trattare tali dati personali se necessario per accertare, esercitare o difendere un diritto, che sia in sede giudiziale, amministrativa o stragiudiziale.

- **Deroghe all'esercizio dei diritti dell'interessato (artt. 17, 18, 21; considerando n. 65)**

Un interessato dovrebbe avere **il diritto di ottenere la rettifica dei dati personali che lo riguardano e il «diritto all'oblio»** (…) Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, (…) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, **ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.**

- **Trasferimento dei dati personali (art. 49; considerando n. 111)**

È opportuno prevedere la possibilità **di trasferire dati in alcune circostanze** se l'interessato vi ha esplicitamente acconsentito, **se il trasferimento è occasionale e necessario in relazione a un contratto o un'azione legale, che sia in sede giudiziale,** amministrativa o stragiudiziale, compresi i procedimenti dinanzi alle autorità di regolamentazione. (….).

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (1)

Art. 2-octies (Principi relativi al trattamento di dati relativi a condanne penali e reati)

1. Fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento, che non avviene sotto il controllo dell'autorità pubblica, è consentito, ai sensi dell'articolo 10 del medesimo regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le liberta' degli interessati.

2. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonché le garanzie di cui al medesimo comma sono individuati con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante.

3. Fermo quanto previsto dai commi 1 e 2, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare: (….)
e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; (…)

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (2)

Art. 2-undecies (Limitazioni ai diritti dell'interessato)

1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:
a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;
f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.
2. Nei casi di cui al comma 1, lettera c), si applica quanto previsto dai regolamenti parlamentari ovvero dalla legge o dalle norme istitutive della Commissione d'inchiesta.
3. Nei casi di cui al comma 1, lettere a), b), d), e) ed f) i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d), e) ed f). In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonche' del diritto

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (3)

Art. 2-duodecies (Limitazioni per ragioni di giustizia)

1. In applicazione dell'articolo 23, paragrafo 1, lettera f), del Regolamento, in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonchè dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, **i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento.**

2. Fermo quanto previsto dal comma 1, l'esercizio dei diritti e l'adempimento degli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento **possono, in ogni caso, essere ritardati, limitati o esclusi, con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari.**

3. Si applica l'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo.

4. Ai fini del presente articolo si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonchè i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi e strutture, quando non è

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (4)

Art. 50. Notizie o immagini relative a minori

1. Il divieto di cui all'articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448, di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale. La violazione del divieto di cui al presente articolo è punita ai sensi dell'articolo 684 del codice penale.

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (5)

Capo III - Informatica giuridica

Art. 51. Principi generali

1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet.

2. Le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo.

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (6)

Art. 52. Dati identificativi degli interessati

1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, **l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento**.

2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (7)

Art. 52. Dati identificativi degli interessati (segue)

3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: 'In caso di diffusione omettere le generalità e gli altri dati identificativi di.....".

4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l'annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l'indicazione delle generalità e degli altri dati identificativi dell'interessato.

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (8)

Art. 52. Dati identificativi degli interessati (segue)

5. Fermo restando quanto previsto dall'articolo 734-bis del codice penale relativamente alle persone offese da atti di violenza sessuale**, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità,** altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di **rapporti di famiglia e di stato delle persone.**

6. Le disposizioni di cui al presente articolo si applicano **anche in caso di deposito di lodo** ai sensi dell'articolo 825 del codice di procedura civile. La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l'annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi dell'articolo 209 del Codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50, provvede in modo analogo in caso di richiesta di una parte.

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (9)

Si vedano anche:

- **Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica* (2 dicembre 2010)**

- **Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero* (26 giugno 2008)**

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (10)

Art. 160-bis (Validità, efficacia e utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento)

La validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali.

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (11)

Art. 160-bis (Validità, efficacia e utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento)

- **Processo penale: l'art. 191 c.p.p., relativo alle prove illegittimamente acquisite stabilisce la loro inutilizzabilità in sede processuale se sono state acquisite in violazione di norme di legge (rilevabile anche d'ufficio). Secondo la giurisprudenza maggioritaria e la dottrina dominante la disposizione non si estenderebbe alla normativa del codice privacy (che rimarrebbe limitata ai soli casi di inutilizzabilità per i titolari dei trattamenti o per i responsabili). E' pertanto al giudice che spetta l'interpretazione e la decisione sull'utilizzabilità o inutilizzabilità delle prove illegittimamente raccolte.**

- **Processo civile: Il c.p.c. non contiene una norma che sancisca un principio di inutilizzabilità delle prove illegittimamente acquisite in violazione di legge. Separata la questione processuale della produzione dei documenti connessa al diritto di difesa dalla questione sostanziale relativa alle modalità di acquisizione della documentazione, che può essere oggetto di separata controversia civile, lasciando all'apprezzamento del giudice nel caso concreto l'utilizzabilità di prove di cui pure sia dubbia la liceità soprattutto quando sono le parti ad aver contestato l'illecito accesso alle stesse.**

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (12)

Art. 175 (Forze di polizia)

3. L'articolo 10 della legge 1° aprile 1981, n. 121, e successive modificazioni, è sostituito dal seguente:

"Art. 10 (Controlli)

1. Il controllo sul Centro elaborazione dati è esercitato dal Garante per la protezione dei dati personali, nei modi previsti dalla legge e dai regolamenti.

2. I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie indicate nel primo comma dell'articolo 7, fermo restando quanto stabilito dall'articolo 240 del codice di procedura penale. Quando nel corso di un procedimento giurisdizionale o amministrativo viene rilevata l'erroneità o l'incompletezza dei dati e delle informazioni, o l'illegittimità del loro trattamento, l'autorità precedente ne dà notizia al Garante per la protezione dei dati personali.

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (13)

Art. 175 (Forze di polizia) segue

(…) 3. La persona alla quale si riferiscono i dati può chiedere all'ufficio di cui alla lettera a) del primo comma dell'articolo 5 la conferma dell'esistenza di dati personali che lo riguardano, la loro comunicazione in forma intellegibile e, se i dati risultano trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.

4. Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre trenta giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ciò può pregiudicare azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità

5. Chiunque viene a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale del luogo ove risiede il titolare del trattamento di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi.".

La protezione dei dati personali in ambito giudiziario nel d.lgs. 101/2018 (13)

Art. 2-sexiesdecies (Responsabile della protezione dei dati per i trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni)

1. Il responsabile della protezione dati è designato, a norma delle disposizioni di cui alla sezione 4 del capo IV del Regolamento, anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni.

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (1)

Articolo 37 - Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (2)

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

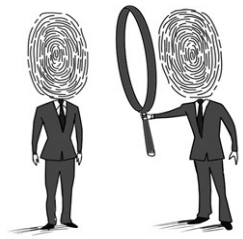
4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (3)



La nozione di «larga scala»: esempi

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile del trattamento specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (4)

«Monitoraggio regolare e sistematico»

"Regolare":

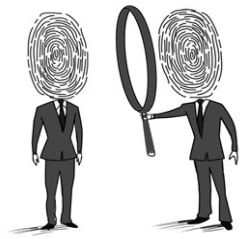
- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

"Sistematico":

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Esempi: curare il funzionamento di una rete di telecomunicazioni; prestazione di servizi di telecomunicazioni; reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring.

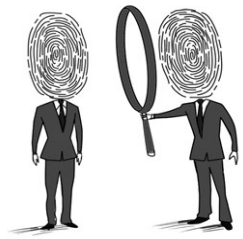
Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (5)



Posizione e compiti (art. 38 GDPR):

- deve essere adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- deve essere sostenuto dal titolare del trattamento e dal responsabile nell'esecuzione dei compiti assegnati;
- deve avere le risorse necessarie per adempiere ai compiti assegnati;
- deve poter accedere ai dati personali e ai trattamenti che riguardano la struttura in cui è inserito;
- deve mantenere la sua conoscenza specialistica (corsi di aggiornamento);
- deve essere indipendente nell'esercizio delle sue funzioni;
- non deve essere penalizzato o rimosso per l'adempimento dei propri compiti;
- è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti;
- non può svolgere altre funzioni o compiti che determino un conflitto di interessi.

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (6)



Ai sensi dell'art. 39 GDPR, i compiti del responsabile della protezione dei dati sono almeno i seguenti:

- informare e consigliare il titolare del trattamento o il Responsabile nonché i dipendenti;
- sorvegliare l'osservanza del Regolamento e delle altre leggi vigenti nell'Unione Europea in materia nonché delle policy;
- fornire se richiesto un parere sulla valutazione di impatto sulla prote-zione dei dati personali e sorvegliare lo svolgimento;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento di dati personali.

N.B.: La professione del responsabile della protezione dei dati non è regolamentata **e non è obbligatoriamente soggetta a esami, certificazioni, né all'iscrizione ad albi professionali**. In italia, si rientra nell'ambito di applicazione della Legge 4/2013 sulle professioni non organizzate in ordini e collegi.

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (7)

L'atto di designazione del DPO è parte costitutiva dell'adempimento.

Nel caso in cui la scelta del RPD ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di designazione a "Responsabile per la protezione dei dati".

In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dall'art. 37 del GDPR.

Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuato in maniera inequivocabile il soggetto che opererà come DPO, riportandone espressamente le generalità, i compiti (eventualmente anche ulteriori a quelli previsti dall'art. 39 del GDPR), le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento e l'eventuale assegnazione di compiti aggiuntivi.

Nell'atto di designazione o nel contratto di servizi devono risultare succintamente indicate anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD, al fine di consentire la verifica del rispetto dei requisiti previsti dall'art. 37, par. 5 del GDPR, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata.

Responsabilità civile e ruolo del DPO (1)

Art. 12,(3) GDPR:

Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Art. 38(4) e (6), GDPR (Posizione del DPO):

Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento. (…)

Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni **non diano adito a un conflitto di interessi.**

I DPO non rispondono personalmente in caso di inosservanza del GDPR. Quest'ultimo chiarisce che spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, paragrafo 1). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

Responsabilità civile e ruolo del DPO (2)

Art. 39 GDPR (Compiti del DPO):

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; (…)

Dal sito web del Garante italiano:

«il modello, debitamente compilato, va indirizzato al titolare del trattamento dei dati personali (azienda, sito, pubblica amministrazione, banca, etc.), anche per il tramite del Responsabile della Protezione dei Dati (RPD), ove designato dal titolare»

European Data Protection Supervisor:

The DPO has to ensure that the data protection rules are respected in cooperation with the data protection authority (for the EU institutions and bodies, this is the EDPS). In the EU institution and bodies, the DPO must:

Ensure that controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them; (…)

Responsabilità civile e ruolo del DPO (3)

Step	Description	Person
Data subject request received	The data subject submits a request via one of a number of methods, including electronically (via email or via our website), by letter or on the telephone. A *Data Subject Request Form* is available for this purpose. Requests may be received by any part of the organisation but should be forwarded to Information Governance, along with the date they were received, as quickly as possible to prevent delays.	Information Governance Team All Staff
Log data subject request	The fact that the request has been received is logged and the date of the request recorded.	Information Governance Team
Confirm identity of data subject	The identity of the data subject is confirmed via an approved method. More information may be requested to confirm identity if required. If the identity of the data subject cannot be confirmed, the request is rejected and the reason for this communicated to the data subject.	Information Governance Team
Evaluate validity of request	The test of whether the request is *"manifestly unfounded or excessive"* is applied. If so, a decision is made whether to reject the request or apply a charge to it. In the case of requests for rectification, erasure, restriction of, or objection to, processing, a decision is also taken about whether the request is reasonable and lawful. If not, the request is rejected and the data subject informed of the decision and their right to complain to the supervisory authority.	Information Governance Team Data Protection Officer

Il GDPR e l’avvocato

Il nuovo Regolamento nella prassi: FAQ (1)

- Il GDPR rivoluziona tutta l'organizzazione privacy fino ad ora implementata?

- Occorre ricominciare da zero oppure qualcosa può essere salvato?

- Posso continuare a fare riferimento alle misure di sicurezza previste dal disciplinare tecnico?

****

- La pluriventennale esperienza italiana in materia di protezione dei dati personali non verrà cancellata dall'entrata in vigore del Regolamento, ma subirà, come si è visto, un'evoluzione. La parte generale del Codice è stata sostituita in modo naturale dalle disposizioni del Regolamento, che su queste prevalgono e quasi nulla resta della parte generale del Codice.
- La parte speciale del Codice è stata invece rimodulata, con i necessari adeguamenti imposti dal Regolamento europeo, dal d.lgs. 101/2018 (ad es.: Codici deontologici).
- In ossequio al principio di responsabilizzazione, non esistono più le «Misure minime di sicurezza»: nell'attesa di nuove Linee guida del garante, il Disciplinare, rimane un valido punto di riferimento per avviare una introdotti dal Regolamento.

Il nuovo Regolamento nella prassi: FAQ (2)

- Da dove e come comincio a implementare il GDPR?

- Posso farcela da solo, oppure occorre un consulente esterno?

****

- La prima operazione da svolgere è una lettura del testo del Regolamento, ampio ed articolato proprio per rendere accessibili a tutti i principi-base in materia di protezione dei dati personali.

- E' imprescindibile una verifica della conformità delle misure adottate rispetto alle nuove norme del Regolamento ai fini di una loro efficacia successiva (es.: informative e consenso al trattamento dei dati);

- Le attività di *audit* e consulenza svolte da soggetti qualificati rappresentano una base fondamentale per espletare in maniera corretta tutte le attività di verifica ed adeguamento alle norme introdotte dal Regolamento.

Il GDPR e il professionista forense (1)

- **<u>Quando l'avvocato è titolare del trattamento?</u>**

L'avvocato è titolare del trattamento di tutte le informazioni che vengono allo stesso fornite dagli assistiti in virtù o in correlazione del mandato ricevuto.

Nel caso in cui, invero, ciascun avvocato riceva mandato per specifiche prestazioni o attività, pur inerenti lo stesso oggetto di controversia, consulenza o problematica, non si ravvisa una collaborazione nelle finalità e, pertanto, ciascuno sarà autonomo titolare del trattamento elaborando autonomamente le modalità di trattamento (Es: Assistenza specifica di più avvocati ciascuno in ambiti diversi ed autonomi, come - anche all'interno dello stesso studio - l'avvocato cui è affidata la difesa in sede civile e l'avvocato cui è affidata la difesa in sede penale da parte del medesimo soggetto per fatti correlati).

Il GDPR e il professionista forense (2)

- **<u>In uno studio associato chi è il titolare?</u>**

Nel caso di società o associazioni **è sempre l'ente giuridico - in nome del legale rappresentante - ad essere qualificato titolare**; ciononostante, in virtù del mandato tra assistito e avvocato, mandato di natura prettamente personale e fiduciaria, si reputa che il titolare non potrà che ravvisarsi nell'avvocato che riceve incarico della prestazione e non nel legale rappresentante della persona giuridica.

Nel caso, infatti, in cui il fiduciario cessi i propri rapporti professionali con l'associazione o la società, l'incarico fiduciario con quel professionista è autonomo, e la società o associazione non dovrebbe più reputarsi titolata a detenere la totalità delle informazioni fornite. Nella pratica non potrebbe avocare un diritto di titolarità delle informazioni del fascicolo o di tutti i dati relativi al singolo assistito, ma, per applicazione dei criteri di necessità, proporzionalità e minimizzazione dei soli dati pertinenti e necessari, come ad esempio, a fini fiscali.

- **<u>L'avvocato domiciliatario è titolare?</u>**

L'avvocato mero domiciliatario, trattando dati personali per conto del dominus mandatario (titolare del trattamento), può essere qualificato **<u>Responsabile del trattamento</u>** ai sensi dell'art. 4 par. 8 del GDPR.

Il GDPR e il professionista forense (3)

- **Responsabile esterno**: Il titolare, nel momento in cui affida la gestione di alcuni dati personali a soggetti terzi (come la società che gestisce i servizi informatici) deve nominarli, mediante atto di nomina o contratto, come Responsabile ai sensi dell'art. 28 del GDPR.
- Il Regolamento (e il Codice) prevede la possibilità per il Titolare e per il Responsabile di avvalersi di persone autorizzate "al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile". Ci si riferisce a categorie di soggetti interni, che ben potrebbero figurare nell'organigramma come dipendenti e collaboratori, i quali sono tenuti ad eseguire le operazioni di trattamento secondo le finalità e le istruzioni impartite, ad assicurarsi che l'esecuzione delle operazioni di trattamento avvenga nel pieno rispetto dei principi generali del GDPR e ad adottare tutte le cautele necessarie ad evitare rischi di violazioni di dati (pertanto, anche nel caso di *data breach*).
- Il Titolare e il Responsabile devono preoccuparsi anche di formare ciclicamente le persone autorizzate sul GDPR.

Il GDPR e il professionista forense (4)

- **Il registro dei trattamenti:**

Ai sensi dell'articolo 30 del GDPR "Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità".

Ogni titolare del trattamento di dati deve quindi tenere un registro delle categorie di trattamento dei dati personali implementati sotto la sua responsabilità. Tale obbligo non vige per le organizzazioni con meno di 250 dipendenti, a meno che il trattamento non includa un rischio per i diritti e le libertà delle persone interessate, non occasionale o se si riferisce in particolare a dati sensibili o a dati relativi a condanne e reati.

Il Registro dei Trattamenti (elettronico o cartaceo) è comunque uno strumento fondamentale non soltanto allo scopo di disporre di un quadro aggiornato ed accurato dei trattamenti svolti ed in essere all'interno Consiglio per la corretta valutazione ed analisi del rischio, ma anche ai fini dell'eventuale supervisione e richiesta di esibizione da parte del Garante. La tenuta del registro dei trattamenti non costituisce, infatti, un mero adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali.

Il GDPR e il professionista forense (5)

- **Il DPO:**

Ogni studio professionale deve valutare puntualmente se è obbligato o meno a nominare un DPO, tenendo conto di quanto disposto dal Regolamento all'art. 37. Ad esempio, è obbligatorio per uno studio professionale che tratta in larga scala dati sanitari provvedere alla nomina di un DPO.

Il Garante ha chiarito che non ricorre trattamento dati "su larga scala", ai fini della nomina del DPO, **nel caso in cui l'attività venga posta in essere da liberi professionisti operanti in forma individuale (es. il singolo avvocato).**

Nella valutazione sulla necessità della nomina bisogna tenere in debita considerazione la struttura dello studio professionale e la forma in cui la prestazione del servizio è resa (es. società tra avvocati).

Il GDPR e il professionista forense (6)

- **L'informativa:**

Ai sensi dell'art. 13 del GDPR, i clienti di uno studio legale devono essere almeno Informati su:

• l'identità e i dettagli di contatto del titolare del trattamento (la ditta);
• i dettagli di contatto del responsabile della protezione dei dati quando ce n'è uno;
• L'obiettivo perseguito (gestione e monitoraggio dei file dei clienti);
• La base giuridica del trattamento (prestazione contrattuale o precontrattuale su richiesta del cliente);
• interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. comma 1 lettera f;
• destinatari di dati (subappaltatori, ufficiali giudiziari, ecc.);
• flussi transfrontalieri;
• la durata di conservazione;
• i diritti che hanno;
• Condizioni per l'esercizio di questi diritti;
• Il diritto di revocare il consenso se è la base giuridica del trattamento;
• Il diritto di presentare un reclamo all'autorità di controllo;
• Informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.

Tali informazioni possono essere incluse nell'accordo con il cliente; possono anche essere comunicate via e-mail o in occasione della trasmissione di una nota di onorario, in particolare per regolarizzare la situazione con i clienti che non sono stati adeguatamente informati.

Il GDPR e il professionista forense (7)

- **Il consenso:**

- Identificare le attività di elaborazione che sono legittimate attraverso il consens

Valutare se altre (potenzialmente più sicure) condizioni di elaborazione o giustificazioni legali potrebbero essere invocate.

Il consenso dell'interessato è "qualsiasi manifestazione di volontà" con la quale l'interessato medesimo presti, in maniera libera, specifica, informata ed inequivocabile, il proprio "assenso (...) che i dati personali che lo riguardano siano oggetto di trattamento", ricorrendo ad una dichiarazione o, in alternativa, ad una "azione positiva inequivocabile".
Il Considerando 32 del GDPR chiarisce che il consenso può intendersi prestato in "un atto positivo ed inequivocabile".
N.B.: silenzio, caselle pre-spuntate e inattività non saranno sufficienti a dimostrare il consenso dell'interessato al trattamento del dato.
Per i dati di cui all'art. 9 del GDPR (Categorie particolari di dati) – quali, ad esempio, i dati sanitari, i dati biometrici e genetici, i dati giudiziari – il Regolamento prevede che il consenso debba essere "esplicito", e tanto vale anche con riguardo alle decisioni basate su trattamenti automatizzati.
Il consenso **non deve essere necessariamente documentato per iscritto**, né viene prevista la forma scritta *ad substantiam* per particolari categorie di dati. Ciò che viene posto in rilievo dal Regolamento è la necessità di documentare l'attività di trattamento svolta: in tale ottica, il titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Il GDPR e il professionista forense (8)

- **<u>La valutazione d'impatto:</u>**

- L'art. 35 del GDPR prescrive - quando sia probabile che un tipo di trattamento possa creare un elevato rischio per i diritti e le libertà delle persone fisiche, ivi compreso il trattamento su larga scala di dati particolari - che il titolare del trattamento debba effettuare una preliminare valutazione d'impatto (DPIA).

- Con specifico riferimento alla figura dell'avvocato ed al trattamento dei dati dei relativi ai propri assistiti, tale trattamento non dovrebbe mai essere considerato su larga scala.
- La valutazione di impatto è comunque necessaria laddove vengano soddisfatti almeno due dei nove dei criteri indicati dal WP29 (valutazione-punteggio, decisione automatica con effetto legale o simili; monitoraggio sistematico; raccolta di dati sensibili; collezione dati personali su larga scala; riferimenti incrociati di dati; persone vulnerabili; uso innovativo; esclusione del beneficio di un diritto-contratto).

Il GDPR e il professionista forense (9)

- ***Data Breach*:**

Uno studio di avvocato che agisce quale titolare del trattamento deve notificare tutte le violazioni dei dati personali al Garante e comunicare con le persone interessate in caso di alto rischio per i diritti e la libertà personali
Se lo studio legale si è avvalso di un responsabile del trattamento, quest'ultimo ha l'obbligo di notificare al titolare, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza, qualsiasi violazione dei dati personali. È raccomandabile che tale obbligo sia oggetto di una specifica clausola contrattuale con il responsabile.

In caso di alta probabilità di rischio dei diritti e delle libertà personali, deve notificare al Garante e comunicare agli interessati tutte le violazioni dei dati personali di cui viene a conoscenza.
Laddove il titolare valuti che sia probabile che la violazione sia suscettibile di presentare un elevato rischio per i diritti e le libertà di una persona fisica, sarà necessario comunicare anche all'interessato il *data breach*.

Il GDPR e il professionista forense (10)

- **Il diritto di accesso:**

Tempo di risposta a una richiesta: un mese dal ricevimento della ex art. 12(3).
Commissioni di riproduzione: il GDPR prevede un principio di gratuità copie fornite come parte di una richiesta di accesso (art. 12(5). questo solo quando la domanda è manifestamente infondata o eccessiva che il il responsabile del trattamento può richiedere il pagamento di "costi ragionevoli" che tengono conto dei costi amministrativi sostenuti per la fornitura delle informazioni. La medesima regola si applica quando viene richiesta una copia aggiuntiva dei dati.
Modalità di comunicazione dei dati: il GDPR prevede che se la persona inoltra una domanda per via elettronica, l'informazione richiesta è comunicata in forma elettronica di uso comune, a meno che l'interessato non richieda diversamente.
Il responsabile del trattamento assista il titolare nell'adempimento dei suoi obblighi riguardo al diritto di accesso.

UNIVERSITÀ DEGLI STUDI DI SALERNO
Facoltà di Scienze Giuridiche (Scuola di Giurisprudenza)

Grazie per l'attenzione!

ggiannonecodiglione@unisa.it