IL CODICE SULLA PRIVACY
(NUOVO REGOLAMENTO EUROPEO UE 2016/679)
"TUTELA DELLE PERSONE E DI ALTRI SOGGETTI RISPETTO AL"
"TRATTAMENTO DEI DATI PERSONALI"
MANUALE DI FORMAZIONE 2018

INDICE

Presentazione 3

Ambito di riferimento 3

Entrata in vigore 3

Principale normativa di riferimento 4

Principali termini utilizzati dal Codice 4

Attività interessate dal Codice 9

Notificazione del trattamento dei dati 9

Violazione dei dati 10

Responsabilità del trattamento dei dati 10

Responsabile della protezione dei dati RPD o DPO 11

Particolari sui dati sensibili 12

Comunicazione e diffusione dei dati 13

- ✓ **Premessa**
- ✓ **Alcuni divieti alla comunicazione e alla diffusione**
- ✓ **Comunicazione e diffusione di dati personali all'Estero**

Modalità di erogazione delle informazioni 13

Consenso al trattamento dei dati personali 14

Esclusione del consenso al trattamento dei dati personali 15

Tutela dei diritti dell'Interessato 15

- ✓ **Richiesta dell'Interessato**
- ✓ **Verifica dell'identità dell'Interessato**
- ✓ **Riscontro all'Interessato**
- ✓ **Esercizio dei diritti dell'Interessato**

Ufficio del Garante 17

Sicurezza dei dati 18

- ✓ **Azioni di custodia e controllo**
- ✓ **Misure di sicurezza**

- **Obblighi di sicurezza**
- **Misure minime di sicurezza**
- **Trattamenti con strumenti elettronici**
- **Trattamenti senza l'ausilio di strumenti elettronici**

Registro dei trattamenti **20**

Valutazione di impatto Protezione Dati **22**

Cenni sul Disciplinare Tecnico **24**

- ✓ **Trattamenti con strumenti elettronici**

Principali novità armonizzate nel Codice sulla privacy - 1 **27**

- ✓ **Riorganizzazione dell'Ufficio del Garante**
- ✓ **Contenuti dei ricorsi all'Ufficio del Garante**

Principali novità armonizzate nel Codice sulla privacy - 2 **30**

- ✓ **Obbligo di produrre e aggiornare il D.P.S.**

Principali novità armonizzate nel Codice sulla privacy - 3 **31**

- ✓ **Sanzioni in cui incorreva chi trasgrediva**
- ✓ **Sanzioni in cui incorre chi trasgredisce**

Varianti introdotte negli ultimi anni **33**

Conclusioni **33**

Appendice:

- ✓ **Conservazione delle cartelle cliniche** **34**

Allegati:

1. **Modulistica da utilizzare per soddisfare il Codice**
2. **Istruzioni per l'uso della modulistica**
3. **Cenni sul nuovo Regolamento europeo, in vigore dal 28 Maggio 2018**

e, inoltre:

4. **Normativa in materia di pubblicità via SMS**
5. **Normativa in materia di scuola**

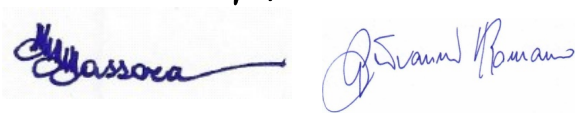
Manuale Redatto da: Ing. Mauro Maria Massara

Per. Agr. Giovanni Romano

Premessa

Questo manuale di formazione è stato rivisto integralmente per l'anno 2018, arricchendolo con ulteriori precisazioni sul Codice sulla privacy (*nel seguito:* Codice) e mantenendo tra gli allegati due nuove Linee guida di cui viene richiesto il pieno rispetto e, soprattutto, una sintesi delle novità che verranno introdotte dal nuovo Regolamento europeo sulla privacy a partire dal 28 Maggio 2018.
Si raccomanda di prenderne attenta visione e di rispettare i requisiti riportati, ove ne ricorrano i presupposti.

Come sempre, buona lettura!



Presentazione

L'attuale decreto (D. Lgs. 196 del 30 Giugno 2003, denominato anche Codice sulla privacy) aveva sostituito integralmente il D. Lgs. 675/96 e le sue ss.mm.ii., intervenute tra il 1997 e il 2003, armonizzandole e introducendo nuove regole e più significative sanzioni, garantendo *comunque* il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche nonché delle persone giuridiche e di ogni altro Ente o Associazione (con particolare riferimento alla riservatezza e all'identità personale).

Ambito di riferimento

Qualsiasi "dato personale" trattato o trattabile da chiunque nel territorio dello Stato Italiano ovvero trasmesso/ricevuto dall'Italia verso Paesi stranieri (in particolare: quelli che costituiscono l'Unione Europea) e viceversa.

Entrata in vigore

**L'attuale Codice sulla privacy era entrato in vigore dal 1° Gennaio 2004; nel mese di Maggio 2018 sarà sostituito dal nuovo Regolamento europeo [*nota: questo Regolamento promuove la responsabilizzazione (accountability) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati (vale a dire delle persone cui attengono questi dati). Il principio-chiave è quello della "privacy by design", ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema e adottare comportamenti che consentano di prevenire possibili*

problematiche; ad esempio: è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi. Viene inoltre introdotta la figura del «Responsabile della protezione dei dati» (Data Protection Officer o DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti].

Principale normativa di riferimento

Legge 241 del 1990 e ss.mm.ii.

D. Lgs. 675/96 (obsoleto)

D.P.R. 501 del 31 Marzo 1998

D.P.R. 318 del 28 Luglio 1999

D.P.R. 445 del 28 Dicembre 2000

D. Lgs. 196 del 30 Giugno 2003

Nuovo Regolamento europeo UE 2016/679

Principali termini utilizzati dal Codice

- ✓ **RGPD: Regolamento generale sulla Protezione dei Dati (in inglese)**
  GDPR, General Data Protection Regulation) - Regolamento UE 2016/679: è il Regolamento con il quale la Commissione Europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini della stessa. Pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia il 25 maggio 2018 abrogando in tale data le legislazioni nazionali vigenti, ove presenti
- ✓ **Valutazione d'impatto (in inglese DPIA: Data Protection Impact Assessment):consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli)**
- ✓ **Codice di condotta: il RGPD auspica la stesura di specifici Codici di Condotta da parte delle autorità, delle associazioni e degli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento, al fine di contribuire alla corretta applicazione del presente regolamento, in funzione delle**

specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese. Tali Codici sono soggetti ad autorizzazione da parte del Garante.

- ✓ **Trattamento: qualunque operazione o complesso di operazioni - svolte con o senza l'ausilio di mezzi elettronici - concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali (anche se non registrati in una banca dati); in particolare:**
  - **Registrazione: è l'atto di annotare o scrivere i dati trattati su registri a fini contabili, amministrativi e/o giuridici**
  - **Organizzazione: è l'atto di sistemare i dati trattati in base a esigenze di funzionalità e/o efficienza**
  - **Conservazione: è l'atto di custodire e archiviare i dati trattati**
  - **Modificazione: è l'atto di sottoporre a parziale trasformazione ovvero a mutamento i dati trattati, per lo più allo scopo di conseguire maggiore funzionalità e/o efficienza**
  - **Blocco: è l'atto di conservare dati personali con sospensione temporanea di ogni altra operazione di trattamento**
  - **Comunicazione: è l'atto del dare conoscenza di dati personali a uno o più soggetti "determinati" diversi dall'Interessato (in taluni casi necessita comunque il consenso dell'Interessato), in qualunque forma, anche mediante la loro messa a disposizione o consultazione**
  - **Diffusione: è l'atto del dare conoscenza dei dati personali a soggetti "indeterminati", in qualunque forma, anche mediante la loro messa a disposizione o consultazione (ed è sempre passibile di pesanti sanzioni)**
  - **Cancellazione: è l'atto di annullare, revocare e/o eliminare i dati trattati**
  - **Distruzione: è l'atto di "mandare al macero" documenti contenenti i dati trattati**
- ✓ **<u>Dato personale</u>: qualunque informazione relativa a una persona fisica o giuridica, a un Ente o a una Associazione (pubblici o privati) identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un codice o un numero di identificazione personale**

- ✓ **<u>Dati identificativi</u>: i dati personali che permettono l'identificazione diretta dell'Interessato**
- ✓ **<u>Banca dati</u>: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti**
- ✓ **<u>Titolare</u>: la persona fisica o giuridica, la pubblica amministrazione o qualsiasi altro Ente, Associazione ovvero organismo (pubblico o privato) cui competono le decisioni in ordine all'effettuazione, alle finalità e alle modalità del trattamento di dati personali, compreso il profilo della sicurezza. È Titolare del trattamento (dei dati) l'entità nel suo complesso ovvero l'Ente/l'Associazione nella figura del proprio Legale Rappresentante (LR) >>> le società fruitrici di questo manuale di formazione sono le "Titolari del trattamento"**
- ✓ **<u>Contitolare</u>: Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. In tale caso occorre definire mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento.**
- ✓ **<u>Responsabile del Trattamento</u>: la persona fisica o giuridica, la pubblica amministrazione o qual-siasi altro Ente, Associazione ovvero organismo (pubblico o privato) preposti dal Titolare del trattamento al trattamento di dati personali:**
    - **Il Responsabile del trattamento, *ove designato dal Titolare del trattamento* (*), deve essere nominato tra soggetti che per esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza**

      (*) *Non sussiste obbligo di designare uno o più Responsabili del trattamento: in questi casi il Responsabile del trattamento è il Legale Rappresentante*
    - **L'eventuale Responsabile del trattamento procede al trattamento attenendosi alle istruzioni impartite dal Titolare del trattamento il quale, anche per il tramite di verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni date e delle proprie istruzioni**

- **Ove necessario, per esigenze organizzative possono essere designati quali Responsabili del trattamento più soggetti, anche mediante suddivisione di compiti tra gli uni e gli altri**
- **Gli eventuali Responsabili del trattamento sono designati formalmente dal Titolare del trattamento (**)**
- **La designazione viene effettuata con lettera (= comunicazione) personale emessa dal Titolare del trattamento ai Responsabili del trattamento (**)**
- **I compiti affidati ai Responsabili del trattamento devono essere analiticamente specificati per iscritto dal Titolare del trattamento (**)**

  (**) ***Per procedere alla designazione e all'affidamento dei compiti si deve utilizzare il modulo "Modello 7 per la privacy", corredato del suo allegato, (per i moduli vedere l'All.to 1 a questo manuale) in cui sono riportati i compiti rispettivamente del Titolare del trattamento e del Responsabile del Trattamento***
- **Si provvede all'istruzione degli eventuali Responsabili del trattamento mettendo loro a disposizione:**
  - **la normativa vigente in materia e ogni eventuale o successiva integrazione o modificazione**
  - **il regolamento interno dell'entità di appartenenza (qualora presente)**
  - **un fac-simile di informativa e uno schema per l'assunzione del consenso per il trattamento dei dati sensibili, qualora sia previsto dalla normativa vigente**
  - **la partecipazione ad appositi corsi di formazione (di solito: interni)**

✓ **RPT - Responsabile della Protezione dei Dati (in inglese DPO, Data Protection Officer): la persona fisica designata, quando previsto dalla normativa, dal Titolare o dal Responsabile del trattamento con il compito di coadiuvarlo nella attuazione e gestione del RGPD**

✓ **Incaricato: la persona fisica o giuridica autorizzata a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento (*ove designato*):**

- **In pratica, gli Incaricati del trattamento sono coloro che effettuano le operazioni di trattamento operando sotto la diretta autorità del Titolare del trattamento o del Responsabile del trattamento (*ove designato*), attenendosi alle istruzioni impartite**

- **La loro designazione viene effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito (***)**

  (***) ***Per procedere alla designazione si deve utilizzare il modulo "Modello 1 per la privacy" (per le persone fisiche) ovvero il modulo "Modello 2 per la privacy" (per le persone giuridiche) (per i moduli vedere l'All.to 1 a questo manuale)***

- ✓ **<u>Interessato</u>: la persona fisica o giuridica, l'Ente o l'Associazione o l'organismo (pubblici o privati) cui si riferiscono i dati personali >>>** ***l'Interessato è il "proprietario" dei dati personali di cui al D. Lgs. 196/03 (Codice sulla privacy)***
- ✓ **<u>Informativa</u>: informazioni scritte rese all'Interessato al momento della raccolta dei dati personali (Art. 13 della Parte I del Codice) (****)**

  (****) ***Per formalizzare l'informativa si devono utilizzare, di caso in caso, secondo le indicazioni fornite nell'allegato 2 a questo manuale di formazione, i moduli all'uopo predisposti (obbligatori) (i soggetti pubblici, escluse le professioni sanitarie e gli organismi sanitari pubblici, non devono richiedere esplicito consenso)***
- ✓ **<u>Dato anonimo</u>: il dato che, in origine o a seguito di trattamento, non può essere associato a un Interessato identificato o identificabile >>>** ***i dati statistici sono, ad esempio, dati anonimi***
- ✓ **<u>Dati</u> (personali) <u>sensibili</u>: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni ovvero organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale**
- ✓ **<u>Dati</u> (personali) <u>giudiziari</u>: i dati personali idonei a rivelare provvedimenti giudiziari che s'iscrivono nel casellario giudiziale (= la "fedina" penale), di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti ovvero la qualità d'indagato ai sensi degli Artt. 60 e 61 del codice di procedura penale**
- ✓ **<u>Ufficio del Garante</u>: l'autorità istituita ai sensi del D. Lgs. 675/96 (*decreto reso obsoleto dalla pubblicazione del D. Lgs. 196/03*) e rimasta in carica anche con la promulgazione e l'entrata in vigore del Codice (*nota: questa autorità assumerà il nome di Autorità di protezione dei dati a partire dal 28 Maggio 2018*)**

Attività interessate dal Codice

- ✓ **Il trattamento dei dati personali (con strumenti cartacei e/o elettronici) e la sua notificazione (*ove del caso: per quanto attiene - o meno - all'obbligo della notificazione si faccia riferimento al testo del decreto D. Lgs. 196/03, Artt. 37 e 38 della Parte I del Codice e a quanto sotto riportato*)**
- ✓ **La comunicazione e la diffusione di dati personali**
- ✓ **La fornitura dell'informazione sul trattamento dei suoi dati all'Interessato; l'ottenimento del consenso e l'esercizio dei diritti da parte dell'Inte-ressato**
- ✓ **Le disposizioni relative a specifici settori (ambito giudiziario, pubblico, sanitario, statistico e giornalistico; forze di polizia; difesa e sicurezza dello Stato; istruzione; sistemi previdenziali, bancari, finanziari e assicurativi; libere professioni e investigazione privata; giornalismo ed espressione letteraria ed artistica; marketing diretto)**

Notificazione del trattamento dei dati

Ai sensi del D. Lgs 196/03 il Titolare del trattamento, qualora intenda procedere al trattamento di dati personali soggetti alle disposizioni del Codice e rientri nelle categorie previste dallo stesso, deve darne *obbligatoriamente* preventiva notifica in forma telematica all'Ufficio del Garante (dal mese di Maggio: Autorità di protezione dei dat), qualora non lo abbia già fatto in forma cartacea o informatizzata ai sensi del D. Lgs. 675/96 (*decreto reso obsoleto dalla pubblicazione del Codice*); per soddisfare questo requisito è sufficiente accedere al documento già predisposto, reperibile sul sito dell'Ufficio del Garante (www.garanteprivacy.it), e compilarlo seguendo le istruzioni.

Tale obbligo <u>decade</u> con l'entrata in vigore del RGPD in quanto la responsabilità sul trattamento dei dati rimane in capo al Titolare del trattamento, il quale è tenuto a tenere un Registro dei Trattamenti (*Nota: l'obbligo di notifica potrebbe essere reintrodotto con la legge di Bilancio 2018 "A tal fine, il Garante per la protezione dei dati personali, con proprio provvedimento dovrà adottare, entro i prossimi due mesi, la disciplina che regoli:*

1. *le modalità attraverso cui il Garante stesso monitora l'applicazione del regolamento RGPD e vigila sulla sua applicazione;*
2. *le modalità di verifica, anche attraverso l'acquisizione di informazioni dai titolari dei dati personali trattati per via automatizzata o tramite tecnologie digitali, della presenza di adeguate infrastrutture per l'interoperabilità di formati con cui i dati sono messi a disposizione dei soggetti interessati, sia ai fini della portabilità dei dati - ai sensi dell'art.*

20 del RGDP - che ai fini dell'adeguamento tempestivo alle disposizioni del regolamento stesso;

3. *definire linee-guida o buone prassi in materia di trattamento dei dati personali basato sull'interesse legittimo del titolare.*

Inoltre, per ottemperare a quanto stabilito dal Regolamento UE n. 679, la Legge di bilancio, all'art. 1 commi 1021 e 1022, prescrive che il Garante debba predisporre un modello di informativa che i titolari del trattamento saranno tenuti a compilare, per trattamenti fondati sull'interesse legittimo che prevedono l'uso di nuove tecnologie o di strumenti automatizzati. Il Regolamento UE stabilisce infatti che il titolare, ove effettui un trattamento che persegue un interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, prima di procedere al trattamento suddetto, debba darne tempestiva comunicazione al Garante per la protezione dei dati personali. A tale fine, ***la legge di bilancio prevede che il titolare sia tenuto a compilare un modello di informativa predisposto dal Garante e ad inviarlo al Garante stesso****, chiarendo l'oggetto, le finalità e il contesto del trattamento. Trascorsi quindici giorni lavorativi dall'invio dell'informativa, in assenza di risposta da parte del Garante, il titolare potrà procedere al trattamento."*

Violazione dei dati

La notifica al garante è resa obbligatoria in caso di violazione dei dati personali, ovvero di violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati, a meno che sia improbabile che la violazine dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.

In tale caso il titolare è tenuto a:

- ✓ **darne comunicazione al Garante entro 72 ore**
- ✓ **darne comunicazione agli interessati,**
- ✓ **Qualora tale comunicazione richiedesse sforzi sproporzionati la comunicazione può avvenire tramite comunicazione pubblica (stampa e/o sito web)**

La comunicazione agli interessati non è necessaria nel caso in cui il titolare abbia adottato misure tecnico-organizzative adeguate di protezione (per es. la cifratura)

Responsabilità del trattamento dei dati

L'eventuale designazione del Responsabile del trattamento, *come già citato*, è da effettuare per iscritto.

La designazione, *ove del caso*, può riguardare più di un Responsabile del trattamento (*magari* suddividendo i compiti); l'eventuale suddivisione deve essere formalizzata per iscritto.

L'assenza di una nomina fa sì, *come già citato*, che il Titolare del trattamento (vale a dire il suo Legale Rappresentante) assuma anche il ruolo di Responsabile del trattamento.

Nota: le istruzioni per il trattamento dei dati personali debbono essere fornite per iscritto dal Titolare del trattamento al Responsabile del trattamento (ove presente) e da questi agli Incaricati.

Responsabile della protezione dei dati RPD o DPO

<u>Obbligo di nomina</u>:

Dovranno designare obbligatoriamente un Responsabile della protezione dei dati:

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati;

c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Un titolare del trattamento o un responsabile del trattamento possono comunque designare un Responsabile della protezione dei dati anche in casi diversi da quelli sopra indicati.

Un gruppo di imprese o soggetti pubblici possono nominare un unico Responsabile della protezione dei dati.

<u>Requisiti</u>:

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

- ✓ **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;**
- ✓ **adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;**
- ✓ **operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio.**

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

<u>Compiti</u>:

Il Responsabile della protezione dei dati dovrà:

a) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

d) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

Nota: Il Nominativo del RPD (DPO) deve essere pubblicato e comunicato al Garante

Particolari sui dati sensibili

Per il loro trattamento possono essere richiesti:

- ✓ **il consenso scritto dell'Interessato (*come già citato*)**
- ✓ **l'autorizzazione aprioristica del Garante (*ove del caso*)**

Questi dati possono concernere:

1. **l'origine razziale e l'origine etnica**
2. **le convinzioni religiose (evidenziate ad esempio dalle richieste di fruizione di permessi per festività religiose) e quelle filosofiche**
3. **le opinioni politiche e/o l'adesione a organizzazioni e/o ad associazioni a carattere religioso/filosofico/politico/sindacale**
4. **dati idonei a rivelare lo stato di salute, come: certificati di malattia, infortunio, inidoneità a particolari mansioni, maternità, appartenenza a categorie protette, intolleranze, allergie, patologie**
5. **dati idonei a rivelare la vita sessuale**

6. **dati giudiziari!**
7. **dati genetici e biometrici**

Comunicazione e diffusione dei dati

<u>Premessa</u>

Ad integrazione di quanto già citato nelle pagine precedenti, alcuni dei casi in cui sono entrambe ammesse anche senza il consenso dell'Interessato sono i seguenti

- ✓ **se i dati provengono da pubblici registri, atti, elenchi, documenti accessibili a chiunque**
- ✓ **in adempimento a un obbligo previsto da Leggi, Regolamenti, Normative comunitarie, ecc.**
- ✓ **qualora i dati siano relativi allo svolgimento di attività economiche, benché nel rispetto delle vigenti Normative relative al segreto aziendale / industriale, …**

<u>Alcuni divieti alla comunicazione e alla diffusione</u>

Nessun dato può invece essere comunicato / diffuso in deroga alle finalità dichiarate ovvero se ne sia stata ordinata la cancellazione o, ancora, se sia decorso il periodo associato al trattamento previsto, consolidato all'atto della raccolta e, poi, notificato

<u>Comunicazione e diffusione di dati personali all'Estero</u>

È vietato il trasferimento dei dati personali verso Paesi situati al di fuori dell'Unione Europea e organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati *(Attenzione alla collocazione dei server per chi lavora o archivia dati con servizi in Cloud!)*

Il trasferimento può avvenire previa notifica all'Autorità di protezione dei dati

Il trasferimento viene *comunque* consentito, *tra l'altro*, qualora l'interessato abbia:

- ✓ **espresso per iscritto il proprio consenso nel caso dei dati cosiddetti "sensibili" o con preciso riferimento al codice di procedura penale**
- ✓ **espresso chiaramente il consenso in tutti gli altri casi**
- ✓ **per necessità di legge, contrattuali o di interesse pubblico**

Modalità di erogazione delle informazioni

Le informazioni all'Interessato o alla persona "fornitrice" dei dati <u>sono da effettuare per iscritto</u>; tra queste vi sono:

- ✓ **le finalità delle raccolta e del successivo trattamento**
- ✓ **le modalità del trattamento**

- ✓ **la natura obbligatoria / facoltativa della fornitura**
- ✓ **le conseguenze associate all'eventuale rifiuto di fornire detti dati**
- ✓ **i soggetti / le categorie di soggetti cui i dati raccolti possono essere comunicati o di cui possono venire a conoscenza in qualità di Responsabili del trattamento (*ove designati*) ovvero Incaricati del trattamento e il relativo ambito di diffusione**
- ✓ **gli estremi identificativi del Titolare del trattamento e del/dei Responsabile/i del trattamento (*ove designato/i*), indicando l'eventuale sito della rete di comunicazione ovvero le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato del/dei Responsabile/i del trattamento (*ove designato/i*) ovvero gli estremi anagrafici del Titolare del trattamento**
- ✓ **Il nome del Responsabile del trattamento dei dati (*quando sia stato designato*) per il riscontro all'Interessato in caso di esercizio dei diritti di cui al Codice**
- ✓ **L'esistenza del diritto all'accesso, rettifica, limitazione e cancellazione dei dati**
- ✓ **Il periodo di conservazione o i criteri utilizzati per determinare tale periodo**
- ✓ **Il diritto di porre reclamo a un'Autorità di Controllo**

Anche se chi fornisce i dati è diverso dall'Interessato, l'informativa, da fornire obbligatoriamente per iscritto, lo dovrà essere contestualmente all'atto della registrazione dei dati o, qualora sia prevista la comunicazione, non oltre il primo incontro.

Questo adempimento NON deve essere soddisfatto, *tra l'altro*, quando:

- ✓ **l'impiego di mezzi necessari venga dichiarato dall'Ufficio del Garante manifestamente sproporzionato rispetto al diritto tutelato, a fronte di richiesta scritta di giudizio formulata dal Titolare del trattamento allo stesso Ufficio del Garante >>> *si suggerisce - in merito a questa materia - di richiedere sempre il parere dell'Ufficio del Garante (ovvero dell'Autorità di protezione dei dati), utilizzando di preferenza le modalità di cui al sito dello stesso***
- ✓ **l'adempimento venga riconosciuto "impossibile" da soddisfare, a giudizio dell'Ufficio del Garante, a fronte di richiesta scritta di giudizio formulata dal Titolare del trattamento, … (*vedere il punto precedente*)**

Consenso al trattamento dei dati personali

I privati possono trattare dati *abitualmente* previo consenso dell'Interessato; detto consenso è libero, specifico, revocabile *ma* da fornire o revocare preferibilmente per iscritto anche in formato elettronico >>> *le Informative, già citate in precedenza,*

sono strutturate in modo da consentire di ottenere contestualmente il consenso dell'Interessato.

Esclusione del consenso al trattamento di dati personali

Il consenso non deve essere richiesto quando riguarda:

- ✓ **dati raccolti e detenuti in base a obblighi di Legge, Regolamenti, Normative comunitarie e/o per: soddisfare obblighi di contratto dei quali sia parte l'Interessato; acquisire informative precontrattuali attivate su richiesta dell'Interessato; adempiere a obblighi legali**
- ✓ **dati provenienti dai pubblici registri, elenchi, atti, documenti disponibili a chiunque**
- ✓ **dati anonimi da utilizzare per ricerche scientifiche e/o statistiche, …**

L'Interessato conserva comunque il diritto:

- ✓ **di avere accesso gratuito al Registro generale dei trattamenti (giacente c/o l'Ufficio del Garante)**
- ✓ **di essere informato in merito al Titolare del trattamento, al/ai Responsabile/i del trattamento (*ove designato/i*), ecc.**
- ✓ **di ottenere dal Titolare del trattamento (o dal/i Responsabile/i del trattamento, *ove designato/i*) *sùbito*:**
    - o **informazioni su dati che lo riguardano (registràti o meno)**
    - o **la cancellazione e/o la trasformazione in forma anonima o il blocco dei dati personali trattati**
    - o **aggiornamenti, rettifiche, integrazioni, …**

Tutela dei diritti dell'interessato

<u>Portabilità</u>

Il soggetto interessato ha il diritto alla Portabilità dei dati, ovvero al trasferimento mediante servizio automatizzato (fax, e-mail, ecc...) dei propri dati ad altro titolare nel caso ad esempio di variazione del fornitore di un servizio.

Tale diritto deve essere oggetto di un apposito prospetto informativo da parte del titolare del trattamento dei dati.

<u>Richiesta dell'Interessato</u>

Questi diritti sono esercitabili con richiesta rivolta senza formalità al Titolare del trattamento o al Responsabile del trattamento (*ove designato*) (anche per il tramite di un Incaricato), alla quale deve essere fornito idoneo riscontro senza ritardo.

La richiesta può essere trasmessa anche mediante lettera raccomandata, fax o posta elettronica (*in quest'ultimo caso si suggerisce "via Pec"*).

Quando riguarda l'esercizio dei diritti, la richiesta può essere formulata anche oralmente e, in tal caso, deve essere annotata sinteticamente a cura del Responsabile del trattamento (*ove designato*) o di un Incaricato.

Se l'Interessato è una persona giuridica, un Ente o un'Associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti ovvero ordinamenti.

Nota: i diritti riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'Interessato o per ragioni familiari meritevoli di protezione.

<u>Verifica dell'identità dell'Interessato</u>

L'identità dell'Interessato deve essere verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento.

La persona che agisce per conto dell'Interessato esibisce o allega copia della procura ovvero della delega sottoscritta in presenza di un Incaricato o sottoscritta e presentata unitamente a copia fotostatica (*non necessariamente autenticata*) di un documento di riconoscimento dell'Interessato.

<u>Riscontro all'Interessato</u>

Per garantire l'effettivo esercizio dei diritti il Titolare del trattamento è tenuto:

a) ad agevolare l'accesso ai dati personali da parte dell'Interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati a un'accurata selezione dei dati che riguardano singoli Interessati identificati o identificabili;

b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

I dati sono estratti a cura del Responsabile del trattamento (*ove designato*) o di Incaricati e possono essere comunicati al richiedente anche oralmente ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole.

Il termine per dare riscontro all'interessato è fissato in 1 mese, estendibile a 3 mesi qualora la elaborazione o ricerca dei dati per la risposta presenti elementi di particolare difficoltà.

Se vi è richiesta specifica da parte dell'Interessato (*e questi ne abbia titolo*), si provvede alla trasposizione dei dati su supporto cartaceo o informatico ovvero alla loro trasmissione per via telematica.

Quando, a seguito della richiesta, non risulta confermata l'esistenza di dati che riguardano l'Interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico; il contributo non può comunque superare l'importo determinato dall'Ufficio del Garante con provvedimento di carattere generale, *cui si rinvia*.

<u>Esercizio dei diritti dell'Interessato</u>

I diritti di cui all'Art. 13 / comma 1 del D. Lgs. 675/96 (*già reso obsoleto dalla pubblicazione del D. Lgs. 196/03*), *comunque* recepiti interamente dallo stesso, possono essere fatti valere di fronte all'autorità giudiziaria o con ricorso all'Ufficio del Garante; la prima alternativa, *se precedente*, esclude la seconda.

L'Ufficio del Garante può:

- ✓ **non pronunciarsi sul ricorso: equivale a rigetto a partire da 20 (venti) giorni dopo la presentazione del ricorso,**
- ✓ **pronunciarsi sul ricorso, emanando un provvedimento.**

Nei casi in cui esso sia provvisorio, cessa di avere effetto dopo 20 (venti) giorni dalla sua emanazione qualora l'Ufficio del Garante, nel frattempo, non si sia definitivamente pronunciato sul ricorso con provvedimento definitivo.

L'opposizione al Tribunale può avvenire, a cura del Titolare del trattamento o dell'Interessato, entro 30 (trenta) giorni dalla data di comunicazione del provvedimento o del rigetto (tacito), pur non sospendendosi l'applicazione del provvedimento, qualora ancora in vigore.

È soltanto il Tribunale che decide; avverso un suo decreto è ammesso solo il ricorso per Cassazione.

Nota: in generale, tutte le controversie sono di competenza dell'autorità giudiziaria ordinaria.

Ufficio del Garante (da Maggio: Autorità di protezione dei dati)

L'Ufficio del Garante è un organo collegiale attualmente composto da quattro membri, eletti due dalla Camera dei deputati e due dal Senato della Repubblica, di

cui uno viene eletto Presidente e ha voto prevalente in caso di parità (ad oggi: il Dr. A. Soro).

Essi sono e dovranno sempre essere esperti di riconosciuto valore nei settori del diritto e/o dell'informatica e durano abitualmente in carica 4 anni.

I principali compiti dell'Ufficio del Garante sono i seguenti:

- ✓ **Istituire e manutenere un Registro generale dei trattamenti sulla base delle notificazioni ricevute**
- ✓ **Verificare che i trattamenti siano effettuati nel rispetto di Leggi e Regolamenti e in conformità alle notificazioni ricevute**
- ✓ **Segnalare tempestivamente le modifiche conseguenti a variazioni delle disposizioni del Codice**
- ✓ **Gestire i reclami e i ricorsi, adottando, *ove del caso*, provvedimenti acconci**
- ✓ **Vigilare sui casi di cessazione del trattamento**
- ✓ **Denunciare i fatti configurabili come reati perseguibili d'ufficio**
- ✓ **Promuovere la sottoscrizione dei codici di deontologia professionale per le categorie interessate**
- ✓ **Divulgare fra il pubblico norme e finalità del Codice**
- ✓ **Segnalare al Governo eventuali necessità di variazioni, anche in ragione di varianti al Regolamento europeo ed essere sempre consultato nella fase di studio delle suddette**

Sicurezza dei dati

<u>Azioni di custodia e controllo</u>

Allo stato attuale delle cose sono definite "necessarie" e "dovute" azioni che garantiscano custodia / controllo tali da ridurre al minimo i rischi di: distruzione o perdita (*anche accidentale*) dei dati; accesso non autorizzato; trattamento non consentito o non conforme alle finalità notificate della raccolta

Esempi di comunicazioni:

- **Nomina del Responsabile del trattamento dei dati**
- **Nomina dell'Incaricato (al trattamento dei dati)**
- **Delega al trattamento operativo dei dati**
- **Notificazione, *ove del caso*, (**Vedi nota al capitolo specifico)
- **Informativa iniziale all'Interessato o a chi ne fa le veci (formula generalizzata), con consenso esplicito al trattamento di dati personali/sensibili da parte dell'Interessato o di persona da lui delegata ovvero alla comunicazione e/o**

diffusione di dati personali/ sensibili da parte dell'Interessato o di persona da lui delegata

- **Informativa iniziale all'Interessato (formula per i dipendenti/equipollenti e i candidati all'assunzione), con consenso esplicito al trattamento di dati personali/sensibili da parte dell'Interessato o di persona da lui delegata ovvero alla comunicazione e/o diffusione di dati personali/sensibili da parte dell'Interessato o di persona da lui delegata**

<u>Misure di sicurezza</u>

Obblighi di sicurezza:

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Misure minime di sicurezza:

Nel quadro dei più generali obblighi di sicurezza di cui al Codice o previsti da speciali disposizioni, i Titolari del trattamento sono comunque tenuti ad adottare le misure minime riportate nel seguito o ai sensi del Codice, volte ad assicurare un livello minimo di protezione dei dati personali.

Trattamenti con strumenti elettronici:

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti da detto Disciplinare Tecnico, le seguenti misure minime:

- **autenticazione informatica;**
- **adozione di procedure di gestione delle credenziali di autenticazione;**
- **utilizzazione di un sistema di autorizzazione;**
- **aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;**
- **protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;**
- **adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;**

- **tenuta di un aggiornato Documento Programmatico sulla Sicurezza dei dati personali (D.P.S.) (*obbligo decaduto a far data dall'anno 2012*);**
- **adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.**

Trattamenti senza l'ausilio di strumenti elettronici:

Il trattamento dì dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal Disciplinare Tecnico sopra citato, le seguenti misure minime:

- **aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati o alle unità organizzative;**
- **previsione di procedure per un'idonea custodia di atti e documenti affidati agli Incaricati per lo svolgimento dei relativi compiti;**
- **previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli Incaricati.**

Registro dei trattamenti

<u>Obbligo di tenuta</u>:

Tutti i Titolari e i Responsabili di trattamento devono tenere un registro delle operazioni di trattamento. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante

Tale obbligo intercorre per:

- ✓ **Organismi con più di 250 dipendenti**
- ✓ **Organismi che effettuano trattamenti a rischio**
- ✓ **Organismi che effettuano trattamento non occasionale di dati sensibili**

La tenuta di tale registro è peraltro consigliata a tutti in quanto strumento efficace per dimostrare l'ottemperanza alla normativa in caso di controlli

<u>Contenuti</u>:

Il RGPD prescrive che siano tenuti due registri, uno dal Titolare del trattamento dei dati e uno dal RTD (DTO) dove previsto. I contenuti minimi devono essere i seguenti:

1. Ogni titolare del trattamento e, se del caso, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

- ✓ **il nome e i dati di contatto del titolare del trattamento e, se del caso, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;**
- ✓ **le finalità del trattamento;**
- ✓ **una descrizione delle categorie di interessati e delle categorie di dati personali;**
- ✓ **le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;**
- ✓ **se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle appropriate garanzie;**
- ✓ **ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;**
- ✓ **ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del RGPD.**

2. Ogni responsabile del trattamento e, se del caso, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- ✓ **il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, se del caso, del responsabile della protezione dei dati;**
- ✓ **le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;**
- ✓ **se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o**

dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

- ✓ **ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del RGPD.**

Valutazione di impatto Protezione Dati (DPIA)

Quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Quando è necessaria:

Il GDPR non esprime in modo chiaro e definito i parametri di necessità della valutazione di impatto. Al fine di chiarire tale aspetto il Gruppo di Lavoro costituito dalla Commissione Europea (WP29) ha definito 9 criteri, dando indicazione per la necessità della DPIA quando sono soddisfatti almeno due degli stessi.

I 9 criteri sono i seguenti:

1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, in particolare a partire da "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 dell'interessato"

2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura: trattamenti finalizzati ad assumere decisioni su interessati che producano "effetti giuridici sulla persona fisica" ovvero che "incidono in modo analogo significativamente su dette persone fisiche". Per esempio, il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione.

3. Monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico".

4. Dati sensibili o dati di natura estremamente personale.

5. Trattamenti di dati su larga scala: il regolamento non offre definizioni del concetto di "larga scala", anche se il considerando 91 fornisce indicazioni in merito. In ogni

caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala:

- ✓ **numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;**
- ✓ **volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;**
- ✓ **durata, o persistenza, dell'attività di trattamento;**
- ✓ **ambito geografico dell'attività di trattamento.**

6. Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato

7. Dati relativi a interessati vulnerabili. La categoria degli interessati vulnerabili comprende anche i minori, che. si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti)

8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative, come l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via

9. Tutti quei trattamenti che, di per sé, "impediscono agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto" Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto. Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

<u>Il Gruppo di lavoro ritiene che una DPIA non sia necessaria nei casi seguenti</u>:

• se il trattamento non "può comportare un rischio elevato per i diritti e le libertà di persone fisiche"

• se la natura, l'ambito, il contesto e le finalità del trattamento sono molto simili a quelli del trattamento per cui è già stata condotta una DPIA. In casi del genere, si possono utilizzare i risultati della DPIA per trattamenti analoghi

• se il trattamento è stato sottoposto a verifica da parte di un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche

• se un trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri da parte del titolare del trattamento, trova la propria base legale nel diritto dell'Ue o di uno Stato membro, la base legale in questione disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta tranne ove uno Stato membro abbia previsto la necessità di condurre una DPIA per i trattamenti pregressi;

• se il trattamento è compreso nell'elenco facoltativo (redatto dall'autorità di controllo ai sensi dell'art. 35, paragrafo 5) dei trattamenti per i quali non è necessario procedere alla DPIA. <u>Ad oggi non presente</u>

<u>Contenuti:</u>

Il regolamento fissa le caratteristiche basilari di una DPIA che deve contenere:

- ✓ **"una descrizione [sistematica] dei trattamenti previsti e delle finalità del trattamento";**
- ✓ **"una valutazione della necessità e proporzionalità dei trattamenti";**
- ✓ **"una valutazione dei rischi per i diritti e le libertà degli interessati";**
- ✓ **"le misure previste per:**
  - **"affrontare i rischi";**
  - **"dimostrare la conformità con il presente regolamento".**

In termini di gestione del rischio, una DPIA mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche attraverso i processi di seguito indicati:

- ✓ **Definizione del contesto: "tenendo conto della natura, dell'ambito, del contesto e delle finalità del trattamento e delle fonti di rischio";**
- ✓ **Valutazione dei rischi: "valutare la particolare probabilità e gravità del rischio elevato";**
- ✓ **Gestione dei rischi: "attenuare tale rischio" "assicurando la protezione dei dati personali" e "dimostrando la conformità al presente regolamento".**

Cenni sul Disciplinare Tecnico [in materia di misure minime di Sicurezza

<u>Trattamenti con strumenti elettronici</u>:

Sistema di autenticazione informatica:

- **Il trattamento di dati personali con strumenti elettronici è consentito agli Incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.**
- **Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato, eventualmente associato a un codice identificativo o a una parola chiave.**
- **A ogni Incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.**
- **Con le istruzioni impartite agli Incaricati deve essere prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso e uso esclusivo dell'Incaricato medesimo.**
- **La parola chiave (password), quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non può contenere riferimenti agevolmente riconducibili all'Incaricato (ad es.: il suo nome o soprannome, la sua data di nascita, la sua posizione, …) ed è modificata da quest'ultimo al primo utilizzo e, successivamente, a frequenza prestabilita dal Titolare del trattamento, *comunque* non superiore a n. 6 (sei) mesi (nel rispetto di procedure scritte e adeguatamente divulgate).**
- **In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni n. 3 (tre) mesi ovvero con frequenza maggiore, nel rispetto di scelte oculate fatte sempre dal Titolare del trattamento, formalizzate con procedure scritte e adeguatamente divulgate.**
- **Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri Incaricati, neppure in tempi diversi.**
- **Le credenziali di autenticazione non utilizzate da almeno n. 6 (sei) mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.**

- **Le credenziali sono disattivate anche in caso di perdita della “qualità” che consente all'Incaricato l'accesso ai dati personali.**
- **Devono infine essere impartite istruzioni agli Incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.**

Principali novità armonizzate nel Codice sulla privacy - 1

Riorganizzazione dell'Ufficio del Garante

Il 19 febbraio 1999 si deliberò di raddoppiare l'organico dell'Ufficio del Garante, consentendo all'ufficio dell'autorità sulla *privacy* di passare da ca. 50 a ca. 100 unità.

Di queste, alcune hanno assunto la veste di ufficiale o agente di polizia giudiziaria, così che l'eventuale rifiuto del Responsabile del trattamento (*ove designato*) o del Titolare del trattamento a fornire collaborazione a fronte di richieste di accertamenti, ispezioni, controlli vari formulate dall'Ufficio del Garante possa prefigurare una eventuale denuncia per resistenza a pubblico ufficiale.

Questa particolare qualifica attribuita agli ispettori delegati dall'Ufficio del Garante consente loro di effettuare, oltre a verifiche di tipo amministrativo, accertamenti in merito a violazioni di natura diversa (ad esempio: l'eventuale trattamento illecito di dati personali relativi a minori - cui si fa cenno nel decreto 196/03 e nel decreto 448 del 22 Settembre 1988 -, ecc.).

Questi accertamenti, anche ai sensi delle modifiche a suo tempo apportate dal D.P.R. 501 del 31 Marzo 1998, possono essere effettuati da detti ispettori, *ove del caso assistiti da consulenti specialisti e/o da altri organi dello Stato*, sempre e solo su autorizzazione del Presidente del Tribunale avente giurisdizione sul Titolare del trattamento interessato all'accertamento.

L'accertamento può avere inizio dopo le ore 7 e non dopo le ore 20, *senza o con preavviso (verbale o scritto)*.

L'accertamento può essere effettuato senza la preventiva autorizzazione del Presidente del Tribunale avente giurisdizione solo qualora vi sia l'assenso scritto e informato del Titolare del trattamento o del Responsabile del trattamento (*ove designato*).

In caso di rifiuto da parte del Titolare del trattamento o del Responsabile del trattamento (*ove designato*) a fornire una risposta, vigono le sanzioni riportate nel testo del D. Lgs. 675/96, riprese …e "appesantite" dal D. Lgs. 196/03.

Con l'ufficializzazione del regolamento per l'organizzazione e il funzionamento dell'Ufficio del Garante si era colta anche l'occasione per sottolineare la necessità di offrire la massima tutela agli Interessati al trattamento dei dati, dando maggiore enfasi ai diritti di questi ultimi in merito alla possibilità loro offerta di richiedere a qualsiasi Titolare del trattamento e/o Responsabile del trattamento (*ove designato*)

informazioni precise e incontestabili sulla tipologia dei dati che li riguardano e da questi ultimi detenuti e sulle modalità di trattamento adottate per garantirne la sicurezza ai sensi delle disposizioni legislative che tutelano i dati personali.

***In estrema sintesi*: nessun Titolare del trattamento potrà rifiutarsi di fornire una risposta tempestiva ed esaustiva a fronte di richieste verbali o scritte da parte di qualsiasi Interessato, potendo, in cambio, richiedere solo una piccola tassa per la ricerca [regolamentata, ma comunque sino a un massimo prestabilito qualora la stessa sia negativa (vedere Nota)] e fornendo, in caso contrario, un servizio totalmente gratuito.**

Nota: s'intende con ciò la rilevazione - incontestabile - e la conferma (scritta, ove richiesto) da parte del Titolare del trattamento o del Responsabile del trattamento (ove designato), che nessun dato personale del postulante è dallo stesso detenuto.

In caso di rifiuto da parte del Titolare del trattamento o del Responsabile del trattamento (*ove designato*) a fornire una risposta, scattano le sanzioni in vigore alla data.

Anche in merito ai ricorsi di cui all'Art. 29 del "vecchio" D. Lgs. 675/96, il regolamento successivamente emesso dall'Ufficio del Garante fornisce maggiori delucidazioni rispetto al mero testo di legge, in particolare in merito ai loro contenuti, alle clausole di inammissibilità e al procedimento che i medesimi generano.

<u>Contenuti dei ricorsi all'Ufficio del Garante</u>

- ✓ **Nome, denominazione o ragione sociale, domicilio o residenza o sede del ricorrente (corredati di un recapito, di un numero telefonico e/o di e-mail/fax per facilitare l'eventuale prosecuzione del rapporto) e del Titolare del trattamento o dell'eventuale Responsabile del trattamento**
- ✓ **Nome dell'eventuale procuratore speciale e indicazioni sul domicilio eletto dallo stesso**
- ✓ **Indicazione del provvedimento richiesto, con evidenza della data della richiesta al Titolare del trattamento o all'eventuale Responsabile del trattamento e degli elementi che avevano giustificato la domanda …e il conseguente ricorso a fronte della mancata risposta**
- ✓ **Firma/e di sottoscrizione del ricorrente (e dell'eventuale procuratore); …**

***…tra gli allegati si rammentano invece:* eventuale procura, copia della domanda posta al Titolare al trattamento o al Responsabile del trattamento (*ove designato*),**

prova del versamento effettuato dei diritti di segreteria e tutta l'eventuale documentazione reputata utile per una corretta valutazione del ricorso.

Fatte salve le clausole d'inammissibilità riportate nel testo del "vecchio" D. Lgs. 675/96 e interamente recepite dal D: Lgs. 196/03, il procedimento adottato comporta l'assunzione in prima persona del ruolo di giudice e di moderatore da parte dell'Ufficio del Garante, che richiede innanzitutto al Titolare del trattamento o al Responsabile del trattamento (*ove designato*) di soddisfare la domanda del ricorrente.

Qualora ciò si verifichi e il ricorrente ne abbia espressamente fatta richiesta, il Titolare del trattamento dovrà sopportare ogni eventuale costo sostenuto dal ricorrente per operare il ricorso.

In caso di prosecuzione del rifiuto, l'azione si svilupperà analogamente a una causa giudiziale, con la presentazione di memorie, documenti, …; l'eventuale richiesta di intervento periziale; un possibile contraddittorio; la decisione, assunta dall'Ufficio del Garante anche in merito agli oneri connessi al procedimento ...e l'attuazione delle decisioni a cura dell'Ufficio del Garante o di altro organo dello Stato a ciò delegato.

Le decisioni dell'Ufficio del Garante possono essere impugnate solo rivolgendosi all'autorità giudiziaria!

Le principali novità armonizzate nel Codice sulla privacy - 2

<u>Obbligo di produrre e aggiornare il D.P.S.</u> (*decaduto alla data; in merito vedere la Circolare su Documento Programmatico Sicurezza emessa nel 2013, inviatavi anni or sono*).

Si tratta del Documento Programmatico sulla Sicurezza (D.P.S.) previsto dall'Art. 6 "Regolamento sulle misure minime di sicurezza" del D.P.R. 28 Luglio 1999, n. 318 e recepito dal Codice.

Questo documento intendeva definire formalmente, sulla base di un'adeguata "analisi dei rischi" e della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati medesimi, quanto segue:

- ✓ **i criteri tecnici e organizzativi adottati per proteggere aree e locali interessati dalle misure di sicurezza e le procedure adottate per controllare l'accesso delle persone autorizzate alle aree/ai locali medesime/i**
- ✓ **i criteri e le procedure adottati/e per assicurare l'integrità dei dati**
- ✓ **i criteri e le procedure adottati/e per garantire la sicurezza della trasmissione dei dati (comprese quelli/e adottati/e per *restringere* gli accessi per via telematica)**
- ✓ **i piani di formazione di tutti gli incaricati del trattamento [Responsabile (*ove designato*)/Incaricati], al fine di renderli adeguatamente edotti in merito ai criteri e alle procedure adottati/e per prevenire danni associati ai rischi individuati**

L'obiettivo finale era di garantire non solo l'introduzione e la conservazione, oltre al possibile miglioramento, delle misure minime di sicurezza dei dati di cui al D.P.R. sopra citato, *ma* di misure "idonee" a offrire garanzie "certe" in merito alla sicurezza medesima.

Questo documento doveva essere rivisto e aggiornato, a cura di un Esperto della materia, con frequenza annuale ed entro ogni 31 Marzo, a seguito di:

- ✓ **una puntuale verifica dell'efficacia delle misure adottate**
- ✓ **l'eventuale decisione in merito all'attivazione di processi correttivi e/o preventivi e/o di miglioramento continuo**

…ambedue comunque documentate con l'emissione di apposito verbale.

Nel caso di strutture certificate in Qualità ai sensi della Norma ISO 9001:2008 questo documento, di fatto, assumeva (*e assume, nella sua ultima revisione dell'anno 2012*) la veste di *input* a uno dei riesami della Direzione, nella fase di analisi e consolidamento delle misure da adottare per garantire un miglioramento continuo.

Le principali novità armonizzate nel Codice sulla privacy - 3

<u>Sanzioni in cui incorre chi trasgredisce ai sensi del D. Lgs. 196/03</u> (*Codice attualmente vigente*)

- ✓ **Per inidonea o omessa informativa all'Interessato: da € 5.000 a € 30.000,00**
- ✓ **Per danni cagionati per effetto del trattamento di dati personali: risarcibili ai sensi dell'Art. 2050 del codice civile**
- ✓ **Per omessa o intempestiva ovvero infedele notificazione: da € 10.000,00 a € 60.000,00 e da 6 mesi a 3 anni**
- ✓ **Per omessa adozione delle misure minime di sicurezza dei dati: da € 10.000,00 a € 50.000,00**
- ✓ **Per inosservanza dei provvedimenti dell'Ufficio del Garante: da € 4.000,00 a € 24.000,00 e da 3 mesi a 2 anni**

<u>Sanzioni in cui incorre chi trasgredisce ai sensi del nuovo Regolamento europeo</u>:

Le sanzioni possono essere di tipo pecuniario, ammonitivo o prescrittivo oppure in combinazione tra loro

Il regolamento non fissa un importo specifico per violazioni specifiche, ma solo un massimale.

La sanzione viene erogata tenendo conto dei seguenti elementi:

- ✓ **la natura, la gravità e la durata della violazione**
- ✓ **danno subito dagli interessati e relativa entità dello stesso**
- ✓ **carattere doloso o colposo della violazione**
- ✓ **adozione di misure tecniche che seguono i principi della protezione dei dati fin dalla progettazione o per impostazione predefinita**
- ✓ **attuazione di misure organizzative che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita a tutti i livelli dell'organizzazione**
- ✓ **attuazione di un livello di sicurezza adeguato**
- ✓ **l'intervento con cui il titolare del trattamento abbia limitato o addirittura azzerato le ripercussioni negative sui diritti delle persone**
- ✓ **violazione riguarda il trattamento di dati di cui agli articoli sensibili**
- ✓ **notifica delle violazioni**
- ✓ **precedente violazione.**
- ✓ **non conformità con le misure di autoregolamentazione**

- ✓ **profitti derivanti da una violazione**

I massimali previsti soni i seguenti:

Inosservanza degli obblighi del titolare e del responsabile del trattamento; inosservanza degli obblighi dell'organismo di certificazione; inosservanza degli obblighi dell'organismo di controllo:

- ✓ **fino a 10 milioni di Euro o, per le imprese, fino al 2% del fatturato annuo mondiale dell'esercizio precedente.**

Inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati; inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali; inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo:

- ✓ **fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente.**

Inosservanza di un ordine correttivo dell'autorità di controllo:

- ✓ **fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente.**

Varianti introdotte negli ultimi anni

L'Ufficio del Garante ha prodotto nel tempo numerose circolari, comunicando, tra l'altro:

- ✓ **l'attuazione del sistema sanzionatorio senza alcuna esclusione;**
- ✓ **l'obbligo di continuare a somministrare l'informativa a tutte le persone fisiche di cui si detengano dati personali e gli incarichi al trattamento dei dati a tutti coloro che - per ragioni di lavoro - trattano dati personali (propri e) di altri;**
- ✓ **l'interruzione dell'obbligo di produrre annualmente, entro il termine del 31 Marzo, il Documento Programmatico sulla Sicurezza dei dati personali (D.P.S.);**
- ✓ **l'obbligo di aggiornare annualmente (formazione continua) il personale dell'entità interessata;**
- ✓ **l'obbligo di formare e aggiornare tutto il personale neo-inserito.**

Conclusioni

Fermo restando il suggerimento di leggere i testi delle variazioni intervenute e, in particolare, una "versione per il pubblico" del Codice, qual'è il presente manuale, qui si vuole ancora una volta sottolineare che le variazioni e integrazioni apportate alle modalità di cui al D. Lgs. 675/96 (*ora obsoleto*) e riviste e armonizzate nel testo del Codice (il suddetto D. Lgs. 196/03, obsoleto dal prossimo mese di Maggio) non sono esigue e si presentano, talvolta, di non semplice applicazione (*nota: …e lo saranno ancor di più con l'introduzione del nuovo Regolamento europeo*).

Appendice

Conservazione delle cartelle cliniche

RIFERIMENTI NORMATIVI

Costituzione italiana Art. 97

D.P.R. 27 Marzo 1969 numero 128 Art. 7

D.P.R. 14 Marzo 1974 numero 225

D.P.R. 27 Marzo 1969 numero 128 Artt. 2 - 5

Nuovo codice di deontologia medica Art.10

Circolare Ministero della sanità 19 Dicembre 1986

Riferimenti ai trattamenti in ambito sanitario di cui alla Parte II - Titolo V del Codice

Riferimento alle cartelle cliniche di cui all'Art. 12 della Parte II del Codice

Le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente, poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario.

La documentazione diagnostica assimilabile alle radiografie va conservata almeno 20 (venti) anni.

È prevista la possibilità della microfilmatura:

- **Legge 4 Gennaio 1968 numero 15**
- **D.p.c.m. 11 Settembre 1974**
- **Decreto Ministro per i Beni culturali e ambientali 29 Marzo 1979**
- **D.P.R. 28 Dicembre 2000 numero 445**