Privacy dello Studio professionale
GDPR n. 2016/679

Gianfranco Costa
Aggiornata al 10/10/2018

1

Le norme di riferimento

- D.Lgs. 30/6/2003, n. 196, che prevedeva:
  - la tutela dei dati sensibili
  - la richiesta di autorizzazioni al trattamento
  - autorizzazioni generiche rilasciate dal Garante
- Regolamento UE 27/4/2016, n. 2016/679
  - rivisitazione delle regole con un cambio totale di visione delle problematiche di tutela dei dati personali e sensibili

2

Ambito di applicazione

Il regolamento della privacy si applica:

1. al trattamento **interamente o parzialmente automatizzato** di dati personali
2. al trattamento **non automatizzato** di dati personali **contenuti in un archivio** o destinati a figurarvi;
3. al trattamento dei **dati delle persone fisiche**.

3

Ambito di applicazione

- **NON si applica:**
  - ai dati personali delle persone giuridiche o dotate di personalità giuridica;
  - **fra** persone fisiche per attività domestiche;
  - **per i dati di persone decedute**
    - **Salvo gli eredi non abbiano interesse a tutelare alcuni o tutti i dati (D.Lgs. 101/2018).**
- **Non riguarda:**
  - I dati **inseriti volontariamente** dall'interessato **in elenchi pubblici** (es. Camera di commercio)

4

Ambito di applicazione

- **Le nuove regole entrano in vigore dal 25/5/2018**
  - **in tutti i Paesi della Comunità europea**
  - **anche nei rapporti con Paesi extra UE**

5

Le novità

6

Le novità

- ✓ **Estensione dell'ambito di applicazione territoriale** del GDPR:
  - ✓ si applica **anche ai titolari stabiliti fuori UE**;
- ✓ **Trasparenza**: **obbligo di informare gli interessati** in forma:
  - ✓ **concisa, trasparente, intellegibile e facilmente accessibile, in linguaggio semplice e chiaro;**
- ✓ **Responsabilizzazione:** obbligo del Titolare di **mettere in atto misure tecniche e organizzative adeguate che devono essere costantemente monitorate e aggiornate**
  - ✓ per **garantire**, ed **essere in grado di dimostrare**,
  - ✓ che il **trattamento è effettuato conformemente al Regolamento**

7

Le novità

- ✓ **Preventiva valutazione dell'impatto del trattamento sulla protezione dei dati personali:** valutazione **se il trattamento presenta rischi elevati per i diritti e le libertà** degli interessati, soprattutto quando vengono utilizzate nuove tecnologie;
  - ✓ **Tutela dei dati personali fin dalla progettazione (Privacy by design):** adozione di misure tecniche ed organizzative adeguate per attuare i principi di protezione dei dati;
  - ✓ Trattare per **impostazione predefinita solo i dati personali necessari** per ogni specifica finalità di trattamento **(Privacy by default):**
    - ✓ per i trattamenti generici è utile adottare misure tecniche organizzative adeguate;

8

Le novità

- ✓ **Registro delle attività di trattamento:** da realizzare in **forma scritta o in formato elettronico**;
  - ✓ è obbligatorio per **imprese con più di 250 dipendenti**, a **meno che il trattamento:**
    - ✓ **possa presentare un rischio per i diritti e le libertà** dell'interessato;
    - ✓ **non sia occasionale;**
    - ✓ **includa categorie particolari di dati**
      - ✓ **personali** (sensibili)
      - ✓ o **relativi a condanne penali e reati**;

9

Le novità

- ✓ **Contitolare:** nuova figura che **va contrattualizzata** qualora più soggetti **utilizzino il medesimo archivio;**
- ✓ **Responsabile del trattamento**: nomina che va fatta in forma scritta da parte del Titolare del trattamento;
- ✓ **Responsabile della protezione dei dati (DPO-RDP): la nomina è obbligatoria solo in alcune fattispecie:**
  - **trattamento, su larga scala**, di:
    - **categorie particolari di dati personali** salute, razza, politica, religione, sindacali, dati biometrici o genetici, ecc.
    - **dati relativi a condanne penali e a reati**

  la nomina **va notificata al Garante** alla privacy;

Le novità

Incaricati al trattamento

Il Titolare e il responsabile del trattamento:

1. **Possono nominare degli incaricati al trattamento**
   1. La nomina **è solo scritta**
   2. Nella nomina devono risultare gli archivi ai quali hanno accesso gli incaricati
2. **Devono istruire gli incaricati al trattamento**

11

Le novità

- ✓ **Notifica della violazione dei dati personali (data breach):** obbligatoria **entro 72 ore** dall'accadimento;
- ✓ **Nuovi diritti dell'interessato**: **informativa sul**:
  - ✓ diritto alla portabilità,
  - ✓ diritto all'oblio,
  - ✓ diritto di limitazione del trattamento,
  - ✓ diritto di rettifica,
  - ✓ informativa e consenso preventivi;
- ✓ **Regime sanzionatorio**: molto più gravoso del passato:
  - ✓ 2% del fatturato; max. € 10.000.000

12

Le definizioni giuridiche

13

Definizioni

- **«dato personale»:** qualsiasi informazione riguardante una persona fisica **identificata** o **identificabile** («interessato»);
  - **si considera identificabile** la persona fisica che può essere **identificata, direttamente o indirettamente**, con particolare riferimento a **un identificativo** come:
    - **il nome,**
    - **un numero di identificazione (es. codice fiscale),**
    - **dati relativi all'ubicazione,**
    - **un identificativo online (es. e-mail)**
    - **o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;**
- **archivio»:** qualsiasi **insieme strutturato di dati personali accessibili secondo criteri determinati**, indipendentemente dal fatto che tale insieme sia
  - **centralizzato, decentralizzato o ripartito** in modo funzionale o geografico;

14

Definizioni

- **«trattamento»:** qualsiasi **operazione o insieme di operazioni**, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come:
  - la raccolta,
  - la registrazione,
  - l'organizzazione, la strutturazione,
  - la conservazione, l'adattamento o la modifica,
  - l'estrazione, la consultazione,
  - l'uso, la comunicazione mediante trasmissione, diffusione
  - o qualsiasi altra forma di messa a disposizione,
  - il raffronto o l'interconnessione,
  - la limitazione, la cancellazione o la distruzione;
- **«limitazione di trattamento»:** il **contrassegno dei dati personali** conservati **con l'obiettivo di limitarne il trattamento in futuro;**

15

Definizioni

- **«destinatario»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo **che riceve comunicazione di dati personali**, che si tratti o meno di terzi.
- **«terzo»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che non sia:**
  - l'interessato,
  - il titolare del trattamento,
  - il responsabile del trattamento
  - le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (es. gli incaricati);

16

Definizioni

- **«profilazione»: qualsiasi forma di trattamento automatizzato di dati** personali consistente:
  - nell'utilizzo di tali dati personali
  - **per valutare determinati aspetti personali** relativi a una persona fisica, in particolare **per analizzare o prevedere aspetti riguardanti**
    - **il rendimento professionale,**
    - **la situazione economica,**
    - **la salute,**
    - **le preferenze personali,**
    - **gli interessi,**
    - **l'affidabilità,**
    - **il comportamento,**
    - **l'ubicazione o gli spostamenti di detta persona fisica.**

17

Definizioni

- **«consenso dell'interessato»:** qualsiasi **manifestazione di volontà libera, specifica, informata** e **inequivocabile** dell'interessato, con la quale lo stesso **manifesta il proprio assenso**, al trattamento **mediante:**
  1. **dichiarazione**
  2. **o azione positiva inequivocabile;**

NB

- **«violazione dei dati personali»:** la **violazione di sicurezza** che comporta
  - **accidentalmente (colpa?) o in modo illecito (dolo!!)**
    - **la distruzione,**
    - **la perdita,**
    - **la modifica,**
    - **la divulgazione non autorizzata**
    - **o l'accesso ai dati personali trasmessi, conservati o comunque trattati;**

18

Definizioni

- **«dati genetici»:** i dati personali relativi alle **caratteristiche genetiche ereditarie o acquisite** di una persona fisica che forniscono informazioni univoche
  - sulla fisiologia o sulla salute di detta persona fisica,
  - e che **risultano in particolare dall'analisi di un campione biologico**;
- **«dati biometrici»:** i dati personali ottenuti da un **trattamento tecnico specifico** relativi alle **caratteristiche fisiche, fisiologiche o comportamentali** di una persona fisica
  - che ne consentono o confermano l'identificazione univoca, quali
    - **l'immagine facciale o i dati dattiloscopici;**
- **«dati relativi alla salute»**: i dati personali attinenti alla **salute fisica o mentale** di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, **che rivelano informazioni relative al suo stato di salute**;

19

Consenso

È **vietato trattare dati personali** che rivelino o trattino:

- l'origine razziale o etnica,
- le opinioni politiche,
- le convinzioni religiose o filosofiche,
- l'appartenenza sindacale,
- 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.

Deroga

20

Consenso

Il trattamento **non è vietato se:**

- l'interessato **ha prestato il proprio consenso** esplicito al trattamento di tali dati personali;
- il trattamento **è necessario**
  - per **assolvere gli obblighi ed esercitare i diritti specifici** del titolare del trattamento o dell'interessato
  - in **materia di diritto del lavoro e della sicurezza sociale e protezione sociale,**
  - **a sensi di legge**, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
  - per **tutelare un interesse vitale** dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

21

L'informativa

22

L'informativa

Art. 12

- Il titolare del trattamento adotta misure appropriate **per fornire all'interessato** tutte le informazioni relative al trattamento in forma
  - **concisa,**
  - **trasparente,**
  - **intelligibile e facilmente accessibile,**
  - **con un linguaggio semplice e chiaro,**

  in particolare nel caso di informazioni destinate specificamente ai minori.
- Le informazioni **sono fornite per iscritto o con altri mezzi**, **anche elettronici**.
- Se richiesto dall'interessato,
  - le informazioni **possono essere fornite oralmente,**
  - **purché sia comprovata con altri mezzi l'identità dell'interessato.**

23

L'informativa

Art. 14

L'informativa deve contenere:

- **l'identità e i dati di contatto del titolare del trattamento** e/o del suo rappresentante;
- **i dati di contatto del responsabile della protezione dei dati**, ove applicabile;
- se il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi;
- gli **eventuali destinatari** o le eventuali categorie di destinatari dei dati personali;
- se i dati personali vengono **trasferiti in un paese terzo** o a un'organizzazione internazionale.

Segue

L'informativa

Art. 14-15

Contenuto dell'informativa

- le **finalità del trattamento**;
- la **base giuridica** del trattamento;
- le **categorie di dati personali in questione**;
- i **destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati**;
- il **periodo di conservazione dei dati** personali, oppure, i **criteri utilizzati per determinare tale periodo**;
- il **diritto di proporre reclamo** a un'autorità di controllo;

Segue

25

L'informativa

Art. 14-15

Contenuto dell'informativa

- se i dati **non** siano raccolti presso l'interessato
  - tutte le informazioni sulla loro origine;
- l'esistenza **del diritto dell'interessato di chiedere:**
  - **l'accesso** ai dati personali **(fissare appuntamento!)**
  - la **rettifica** dei dati
  - la **cancellazione** dei dati **(nei limiti tecnologici disponibili)**
  - la **limitazione** del trattamento
  - di **opporsi** al loro trattamento **(con indicazione delle conseguenze)**
  - la **portabilità** dei dati **(trasferimento di archivi);**

Segue

26

L'informativa

Art. 14-15

Contenuto dell'informativa

- **se il trattamento è stato oggetto di consenso** dell'interessato,
  - il diritto di **revocare il consenso** in qualsiasi momento
    - **rimane impregiudicata la liceità del trattamento fino alla data della revoca;**
- la **fonte da cui hanno origine i dati personali** e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
- **l'esistenza di un processo decisionale automatizzato**, compresa la profilazione (fidelity-card)
  - es.: negozio di abbigliamento: invio di mail a tutti coloro che acquistano scarpe da ginnastica.

27

L'informativa

Art. 14-15

Il titolare del trattamento **fornisce le informazioni per l'ottenimento dei dati personali:**

1. **al più tardi entro 1 mese**, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
2. nel caso in cui i dati personali **siano destinati alla comunicazione con l'interessato:**
   - **non oltre la prima comunicazione** all'interessato;
3. nel caso sia prevista la **comunicazione ad altro destinatario:**
   - **non oltre la prima comunicazione** dei dati personali.

28

Misure di sicurezza

29

Sicurezza del trattamento

Art. 32

Misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, possono essere:

a) **la pseudonimizzazione (es. crittografia, funzione di Hash, Tokenizzazione) e la cifratura dei dati personali;**

b) **la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi (= capacità di affrontare i rischi)** e dei servizi di trattamento;

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

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

30

Sicurezza del trattamento

Art. 32

- **Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento** che possono derivare:
  - **dalla distruzione,**
  - **dalla perdita,**
  - **dalla modifica,**
  - **dalla divulgazione non autorizzata**
  - **dall'accesso, in modo accidentale o illegale**,

  a dati personali **trasmessi, conservati o comunque trattati**.

31

Sicurezza del trattamento

Come proteggere

Personal computer:

- Dotati di password
  - minino 8 caratteri, difficilmente individuabili
- Server e client:
  - dopo un periodo di inutilizzo (max 20 minuti) devono andare in stand by
  - alla riattivazione devono chiedere la password
- copie di sicurezza:
  - almeno una volta a settimana
  - luogo di conservazione delle copie
  - eventuali modalità di verifica del buon fine della copia e della leggibilità della stessa

32

Sicurezza del trattamento

Come proteggere

Trattamento:

- Durante il trattamento sulla scrivania solo i documenti del singolo cliente e non quello di altri
- Finito il trattamento i documenti vanno riposti:
  - nel contenitore
  - e nell'armadio
- Chi e come accede agli archivi

33

Sicurezza del trattamento

Come proteggere

Trattamento:

- Armadi: muniti di **chiavi**
- **Appositi archivi**: ambienti inaccessibili al pubblico
- I clienti vengono **incontrati in appositi ambienti** e non presso la postazione di lavoro dell'incaricato

34