ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Privacy 2018

Parte prima

Nuovo GDPR e

novità rispetto al D.Lgs. 196/2003

Andrea Pardo
Studio Pardo
andrea.pardo@studiopardo.com

6 aprile 2018, corso Europa 11 – Milano

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

ORIGINI E STORIA

Norme che seguono l'evoluzione tecnologica ed il "progresso" a tutela dell'individuo ?

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

GENERAL DATA PROTECTION REGULATION

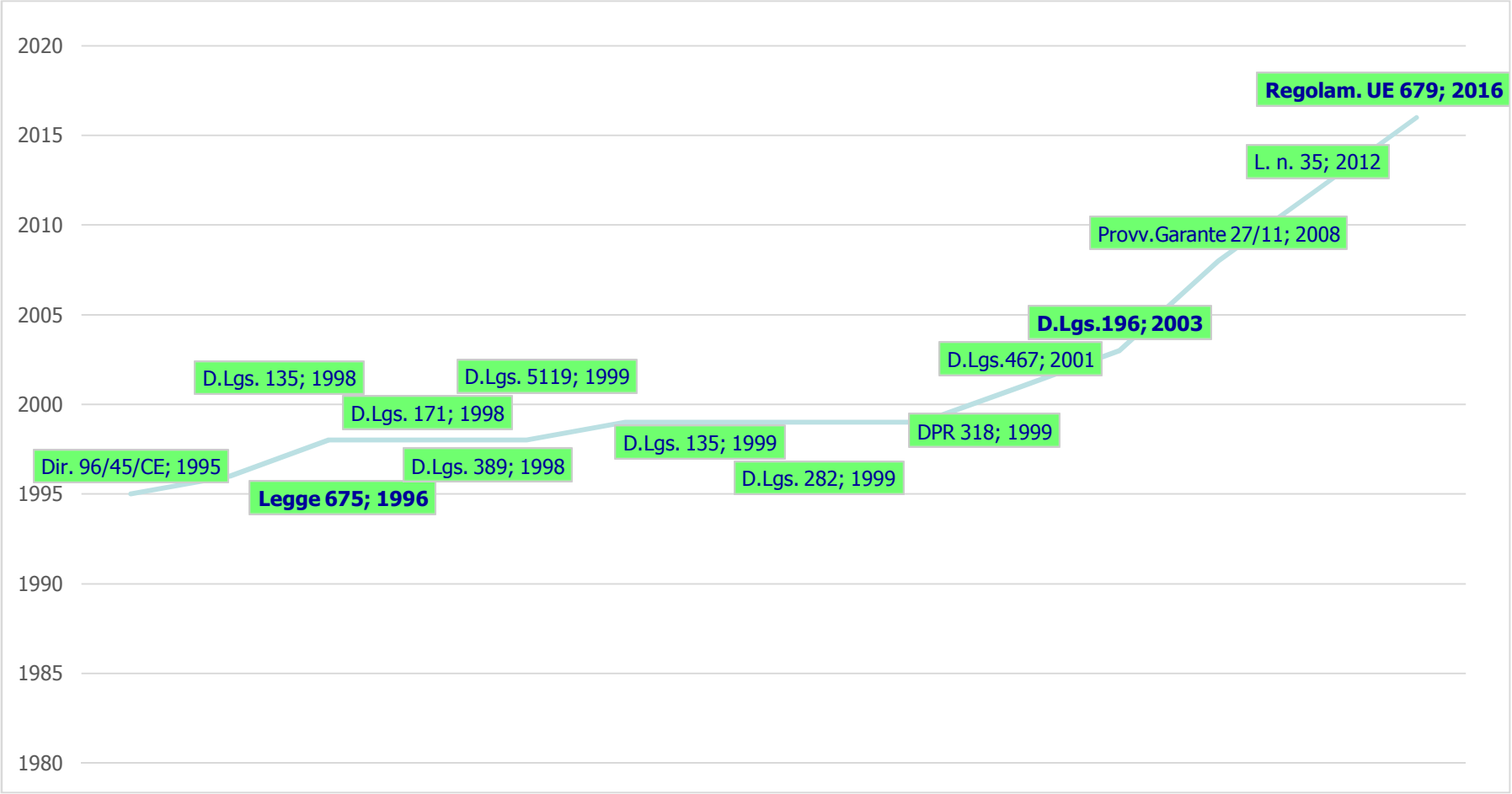
173 “Considerando”

99 articoli

«Milestones» e ratio della Privacy
Un ventennio di storia

- Dir. 96/45/CE 1995 - Direttiva Comunitaria
- Legge 675/1996 - Legge «Madre»
- D.Lgs. 123/1997 e 255/1997 - Correzioni alla 675/96
- D.Lgs. 135/1998 - Pubblica amministrazione
- D.Lgs. 171/1998 - Telecomunicazioni
- D.Lgs. 389/1998 - Pubblica amministrazione
- D.Lgs. 5119/1999 - Ufficio del Garante
- D.Lgs. 135/1999 - Pubblica amministrazione
- D.Lgs. 281/1999 - Attività storiche e statistiche
- D.Lgs. 282/1999 - Ambito sanitario
- DPR 318/1999 - Misure minime di sicurezza (Decreto Presidenziale di attuazione)
- L. 325/2000 - Ulteriori regole
- D.Lgs.467/2001 – Modifiche alla 675/96
- L.196/2003 – Codice nazionale della Privacy

«Milestones» e ratio della Privacy
Un ventennio di storia



Entrata in vigore – 25 Maggio 2018

- Regolamento Europeo n. 679/2016, pubblicato in G.U.C.E. il 4 maggio 2016 con entrata in vigore dal 20° giorno successivo alla pubblicazione: **25 Maggio 2016**.

- Applicabilità a partire dal **25 Maggio 2018**

- Abrogazione della Direttiva 95/46/CE

Princìpi "cardine" e carattere della norma

- Impianto normativo a "tutela delle persone fisiche e dei valori dell'individuo" e del diritto alla protezione dei loro dati
- Norma di sistema "flessibile"
- Norma di armonizzazione (comunitario) con eccezioni "specialistiche"
- Norma di metodo "preventivo"
- Norma "da evoluzione tecnologica"
- Obiettivo economico della «sana concorrenza» (multinazionali)
- Criteri auto-valutativi
- Sistema sanzionatorio Europeo uniforme ed unitario
- Codici di condotta
- Certificazioni (raccomandate)

La norma e l'evoluzione tecnologica

- 14 anni di distanza dalla L. 196/2003 e integrazioni
- Nuove soluzioni tecnologiche applicate all'ambiente e agli strumenti che utilizziamo ogni giorno
  - Internet 2.0 – dispositivi mobili – apparati di misura
  - IoT – Internet of things
  - Sistemi di identificazione e riconoscimento dei soggetti per mezzo di dati biometrici (riconoscimento del volto, impronte digitali, dell'occhio etc.) già parzialmente oggetto di disciplina D.Lgs. 196
  - Applicazioni di profilazione automatica e scoring dei soggetti
  - Dispositivi di geolocalizzazione e tracking dei soggetti
  - Conclusione di contratti in modo automatizzato (mutui, assicurazione, hotels e viaggi)
  - Big data

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4 del Gdpr)

- Oggetto e finalità
  - Protezione delle persone fisiche dei loro diritti e libertà fondamentali attraverso la protezione dei loro dati.
  - Libera circolazione dei dati (nell'UE)

- Ambito materiale

  Non si applica:
  - ai trattamenti effettuati dagli Stati membri UE per Sicurezza, giustizia e libertà
  - finalità ed uso personale o domestico
  - ai dati trattati dalle Autorità competenti per prevenzione, indagine, accertamento o perseguimento di reati, sanzioni penali, salvaguardia contro minacce per la pubblica sicurezza

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

- Ambito territoriale

  Si applica a trattamenti di dati:

  - Personali nell'ambito delle attività di uno stabilimento di un titolare o responsabile del trattamento localizzato nell'UE anche se il trattamento viene effettuato fuori dall'UE.
  - di Interessati localizzati nell'UE effettuati da un titolare, non stabilito nell'UE, quando l'attività di trattamento ha finalità di offerta di beni e servizi ai suddetti anche senza corrispettivo o finalità di monitoraggio del comportamento dei suddetti nell'ambito UE.
  - In questo caso il titolare o responsabile del trattamento deve designare un rappresentante nell'Unione Europea

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

- Definizioni principali
  - Dato personale
  - Interessato
  - Trattamento
  - Limitazione
  - **Profilazione**
  - **Pseudonimizzazione**
  - Archivio
  - Titolare
  - Responsabile
  - Destinatario
  - Terzo
  - **Consenso dell'interessato**
  - **Violazione dei dati personali**
  - Dati genetici
  - Dati biometrici
  - Dati relativi alla salute
  - Stabilimento principale
  - **Rappresentante**
  - Impresa
  - **Gruppo imprenditoriale**
  - Norme vincolanti d'impresa
  - **Trattamento transfrontaliero**
  - **Obiezione pertinente e motivata**

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

NOVITA'

- Limitazione
  - Contrassegno o marcatura dei dati con obiettivo di limitarne il trattamento in futuro

- Pseudonimizzazione
  - Previsione di trattamento che preveda che i dati non possano più essere attribuibili a un interessato specifico senza l'utilizzo di informazioni aggiuntive a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

- Consenso dell'interessato

  - Per i dati "sensibili" (art. 9) il consenso **DEVE** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la *profilazione* – art. 22). Si segnalano, al riguardo, le Linee-guida in materia di profilazione e decisioni automatizzate recentemente pubblicate dal Gruppo "Articolo 29" (WP 251) e attualmente in consultazione pubblica, disponibili qui

http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963.

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

- Consenso dell'interessato

  - **NON** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) **DEVE** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

  - Il **consenso dei minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale).

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

- Consenso dell'interessato

  - **DEVE** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **NON** è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

  - Il **consenso dei minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale).

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

- Consenso dell'interessato

RACCOMANDAZIONI DEL GARANTE (agg. FEBBRAIO 2018)

- Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.
- In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20).

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

NOVITA'

- Violazione dei dati
  - La violazione di sicurezza che comporta accidentalmente o in modo illecito la distrazione, la perdita, la modifica. La divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

- Rappresentante
  - Persona fisica o giuridica stabilita nell'UE che, designata dal titolare, o dal responsabile del trattamento per iscritto (art.27) li rappresenta per quanto riguarda gli obblighi del GDPR

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

NOVITA'

- Gruppo imprenditoriale
  - Un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate
- Trattamento transfrontaliero
  - a) Trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento responsabile del trattamento nell'Unione ove il titolare del trattamento o responsabile del trattamento siano stabiliti in più di uno Stato membro oppure
  - b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento dell'Unione ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro

Oggetto e finalità, ambiti di applicazione, definizioni (art. 1 a 4)

- Obiezione pertinente e motivata
  - un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e ove applicabile alla libera circolazione dei dati personali all'interno dell'Unione

Abrogazioni ed eliminazioni

- Direttiva CE 96/45/CE 1995
- D.Lgs. 196/2003 (non nelle logiche e concettuali)
- Sistema delle Notificazioni preventive al Garante

Principali novità e obblighi (rispetto alla 196/03)

- **Trattamento**
  - Liceità, Informativa, Consenso, Privacy by design e by default, Sicurezza, violazione dei dati (data breach), valutazione d'impatto (PIA) e consultazione preventiva, DPO, Registri, Codici di condotta, etici e certificazioni
- **Diritti**
  - Oblìo, portabilità dei dati, profilazione, opposizioni e limitazioni, sportello unico "One stop shop"
- **Sanzioni**
  - Pecuniarie e penali
- **Autorità**
  - Comitato di controllo europeo – "Garante Europeo"

Princìpi e liceità del trattamento (art.5 e 6)

- **Liceità e Consenso**

  - Il GDPR conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica i cui fondamenti sono indicati all'art. 6 (coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003):

    - Consenso dell'interessato al trattamento
    - adempimento obblighi contrattuali
    - salvaguardia interessi vitali della persona interessata o di terzi
    - obblighi di legge cui è soggetto il titolare
    - interesse pubblico o esercizio di pubblici poteri del titolare
    - interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati

Princìpi e liceità del trattamento (art.5 e 6)

- **Modalità del trattamento**

I dati personali devono essere trattati:

- in modo lecito corretto e trasparente nei confronti dell'interessato
- raccolti per finalità determinate esplicite e legittime
- adeguati pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
- esatti e aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità del trattamento
- conservati in un modo che consenta l'identificazione degli interessati per un periodo non superiore conseguimento delle finalità per le quali sono trattati
- in modo da garantire un'adeguata sicurezza dei dati personali compresa la protezione, mediante misure tecniche e organizzative adeguate da trattamenti non autorizzati o illeciti e dalla perdita , dalla distruzione o dal danno accidentali.

Informativa (art.13)

- **Contenuti dell'informativa**

- I contenuti dell'informativa sono elencati in modo tassativo (artt. 13, par.1, e 14, par. 1), e in parte sono più ampi rispetto al Codice. In particolare, il titolare DEVE SEMPRE specificare:
- i dati di contatto del RPD-DPO (Responsabile della protezione dei dati-*Data Protection Officer*), ove esistente,
- la base giuridica del trattamento,
- qual è il suo interesse legittimo e se quest'ultimo costituisce la base giuridica del trattamento,
- se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

Informativa (art.13)

- **Contenuti dell'informativa**

- Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

- Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Informativa (art.13)

- **Tempi dell'informativa**

➢ Nel caso di dati personali non raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**NON** della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice 196/2003).

Informativa (art.13)

▪ Modalità dell'informativa

➢ Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee *(si veda anche considerando 58)*.

➢ L'informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: (*art. 12 par.1, considerando 58*), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra *(art. 12, paragrafo 1)*. Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa***(art. 12, paragrafo 7)*; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

Informativa (art.13)

- **Modalità dell'informativa**

➢ Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** *(si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo)*, anche se occorre sottolineare che **spetta al titolare**, in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** *(si veda art. 14, par.5, lett.c)*

Diritti degli interessati (art.12)

- **Modalità per l'esercizio dei diritti**

➢Il titolare agevola l'interessato all'esercizio dei diritti ai sensi degli artt. da 15 a 22

➢Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), **1 mese, estendibile fino a 3 mesi in casi di particolare complessità;** il titolare deve comunque **dare un riscontro all'interessato entro 1 mese dalla richiesta**, anche in caso di diniego.

➢ il titolare valuta la complessità del riscontro all'interessato e stabilisce l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive), a differenza di quanto stabilisce il Codice vigente.

Diritti degli interessati (art.12)

- **Modalità per l'esercizio dei diritti**

➢ Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

➢ La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

➢ Come per la 196/2003 il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea ed è il solo a dover dare riscontro in caso di esercizio dei diritti (art. 15-22) anche se il responsabile è tenuto a collaborare ai fini dell'esercizio dei diritti degli interessati (art. 28)

Diritti degli interessati (art.15)

- **Diritto di accesso**

Å Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **una copia dei dati** personali oggetto di trattamento.

Å Fra le informazioni che il titolare deve fornire **non rientrano le "modalità" del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

RACCOMANDAZIONI

Oltre al rispetto delle prescrizioni relative alla modalità di esercizio di questo e degli altri diritti (si veda "Modalità per l'esercizio dei diritti"), i titolari possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Diritto alla cancellazione (art.17)

NOVITA'

- **Diritto all'oblio**

➢ Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).

➢ Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).

Diritto di limitazione del trattamento (art.18)

- **Limitazione**

➢ Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

➢ Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

RACCOMANDAZIONI

Il diritto alla limitazione prevede che **il dato personale sia "contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Diritto alla Portabilità dei dati (art. 20)

NOVITA'

- **Portabilità dei dati**

➢ E' un ulteriore novità del GDPR. E possibile chiedere **la portabilità dei dati dell'interessato ad altro titolare di trattamenti**, (se possibile tecnicamente) oppure ottenerne la restituzione in un formato di uso comune e che sia leggibile da dispositivo automatico.

➢ Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare (considerando 68)

Profilazione (art.22)

NOVITA'

- **Processi decisionali automatizzati compresa la profilazione**

➢ Qualsiasi forma di trattamento automatizzato di dati personali di un interessato consistente nell'utilizzo al fine di valutare determinati aspetti personali relativi a una persona fisica (i.e. per analizzare o prevedere aspetti riguardanti: rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi l'affidabilità, il comportamento, l'ubicazione o gli spostamenti.

➢ Il regolamento sancisce il diritto a non subire profilazioni e decisioni automatizzate inconsapevoli, stabilendo il diritto all'intervento umano nei casi in cui la profilazione possa avere luogo.

Privacy by design e Privacy by default (art.25)

NOVITA'

La privacy diventa un **PROCESSO AZIENDALE** volto a prevenire e non correggere eventuali problemi successivi

(primo criterio di responsabilizzazione/accountability)

- **Privacy by design**: deve essere, sin dall'origine, identificata e codificata mediante la progettazione dei **sistemi ed applicazioni** dimensionati **sull'uso minimo e indispensabile** dei dati personali che garantiscano sicurezza nel tempo (ciclo del prodotto), trasparenza, centralità dei diritti dell'interessato e approccio basato sul rischio.

- **Privacy by default**: si devono progettare misure e sistemi che nascano e abbiano come impostazione predefinita **l'uso dei soli dati necessari** per una determinata finalità.

Privacy by design e Privacy by default (art.25)

- **Dalla centralità dell'interessato alla Responsabilità del titolare**

➢ Nel concetto di **privacy by design e by default** si evidenziano i princìpi ispiratori e un cambiamento di approccio alla regolamentazione sulla privacy.

CODICE PRIVACY	GDPR 2018
PRECISE PRESCRIZIONI E PREVISIONE DI MISURE E STANDARD MINIMI PER IL TRATTAMENTO E LA SICUREZZA DEI DATI	FLESSIBILITA' PROATTIVITA' ED AUTOVALUTAZIONE PER IL TRATTAMENTO E LA SICUREZZA DEI DATI RESPONSABILITA' / ACCOUNTABILITY

Sicurezza (art. 32)

- **Misure di sicurezza**
- Il titolare del trattamento è obbligato, in determinati casi, ad effettuare l'analisi dei rischi e di vaglio dell'adeguatezza delle misure di tutela degli interessati. Deve adottare, ad esempio, sistemi di *pseudonimizzazione.* Utile, soprattutto in caso di contenzioso per danni da perdita/accesso non autorizzato ai dati, l'adesione sistemi di certificazione e codici di condotta che devono essere emanati dalle Associazioni di categoria.
- La Guida al GDPR impone che le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento e la lista all'art. 32 **è "aperta e non esaustiva".** Non potranno quindi sussistere, dopo il 25 maggio 2018, obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati

Sicurezza (art. 32)

- **Misure di sicurezza**

Il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la ***pseudonimizzazione*** e la cifratura dei dati personali;

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

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

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

Sicurezza (art. 32)

- **Misure di sicurezza**

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Violazione dei dati (Data breach) (art.33/34)

- **Notifica delle violazioni di dati personali**

NOVITA'

- Si estende a tutti la regola della notifica di violazione dei dati personali al garante e all'interessato ma quest'ultimo in caso di rischio elevato per i suoi diritti

- La Guida evidenzia che partire dal 25 maggio 2018, **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 (si veda considerando 85).

Violazione dei dati (Data breach) (art.33/34)

- **Notifica delle violazioni di dati personali**

- Pertanto, **la notifica all'autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo";
- fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice.
- **I contenuti della notifica** all'autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli artt. 33 e 34 del regolamento**.
- Sono in corso di formulazione linee-guida specifiche, alle quali sta già lavorando il Gruppo "Articolo 29". (agg. Febbraio 2018)

Violazione dei dati (Data breach) (art.33)

- **Notifica di una violazione dei dati all'autorità di controllo**

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Violazione dei dati (Data breach) (art.33)

- **Notifica di una violazione dei dati all'autorità di controllo**

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

Violazione dei dati (Data breach) (art.33)

- **Notifica di una violazione dei dati all'autorità di controllo**

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Violazione dei dati (Data breach) (art.33)

RACCOMANDAZIONI

- Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice. Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Violazione dei dati (Data breach) (art.34)

NOVITA'

- **Notifica di una violazione dei dati all'interessato**

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

Violazione dei dati (Data breach) (art.34)

NOVITA'

- **Eccezioni alla notifica**

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura.

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

Violazione dei dati (Data breach) (art.34)

- **Eccezioni alla notifica**

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Violazione dei dati (Data breach) Infografica del Garante

SOCIETA' TELEFONICHE E INTERNET PROVIDER

Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- **L'obbligo di comunicazione al Garante** *(mediante un apposito modello di comunicazione)* riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tlc e Isp **devono**:
  - **a. entro 24 ore** dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
  - **b. entro 3 giorni dalla scoperta,** informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti **non è dovuta** se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un **inventario** costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

BIOMETRIA

Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]

- **Entro 24 ore** dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

DOSSIER SANITARIO ELETTRONICO

Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]

- **Entro 48 ore** dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

AMMINISTRAZIONI PUBBLICHE

Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

- **Entro 48 ore** dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

Violazione dei dati (Data breach) -Azioni

- **Precauzioni e azioni**

- Esistono diversi modi di verifica se una persona o un'azienda è stata oggetto o se è soggetta ad un Data Breach. Il modo più facile per una persona è attraverso la verifica della propria mail (personale o aziendale) attraverso portali come ad esempio

- *https://haveibeenpwned.com*

- *https://hacked-emails.com/*

- *https://Breachalarm.com/*

Violazione dei dati (Data breach) -Azioni

➢ Precauzioni e azioni

I consigli di base per gestire eventuali furti di dati sia per le aziende sia per le singole persone sono:

➢ **Utilizzare sempre per ciascuno servizio una password diversa**. La cosa migliore è crearsi una regola memonica non banale per costruire password preferibilmente di almeno 12 caratteri o parti di una frase;

➢ **Cambiare con una certa regolarità la password** come la mail, servizi di home banking o social network;

➢ **Verificare con regolarità sui portali di cui sopra l'eventuale furto delle credenziali**.

➢ **Attivare le notifiche di login nei vari servizi**come la posta elettronica, home banking, etc;

➢ **Utilizzare autenticazione multi-fattore** (es. token, SMS sul telefono, etc).

Valutazione di impatto (art.35)

NOVITA'

- **DPIA (o anche PIA)**

  (secondo criterio di responsabilizzazione/accountability)

- In casi specifici come il ricorso a tecnologie a rischio per i diritti delle persone in trattamento deve essere attestato con una valutazione di impatto privacy ed eventualmente con una consultazione preventiva del Garante della privacy
- La Guida identifica come Fondamentali le attività connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi

Valutazione di impatto (art.35)

- **Cos'è la DPIA**

➢ processo di analisi che il titolare del trattamento deve compiere qualora i trattamenti, specie se prevedono in particolare l'uso di nuove tecnologie, possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

➢ È analisi volta a descrivere le attività di trattamento, valutandone necessità e proporzionalità e determinandone l'origine, la natura, la particolarità e la gravità del rischio connesso. La DPIA è infine un procedimento atto a costruire e dimostrare la conformità al GDPR, uno strumento di fondamentale importanza messo a disposizione del titolare del trattamento per rispettare il principio di *accountability*, criterio che pervade tutto il GDPR.

Valutazione di impatto (art.35)

- **Cos'è la DPIA**

Uno dei primi temi affrontato dalle *guidelines* riguarda la possibilità di svolgere una singola DPIA per far fronte a più trattamenti simili tra loro in termini di rischi, purché adeguatamente considerate natura, portata, contesto e finalità del trattamento. Ad esempio, nell'ambito della videosorveglianza che è di uso ormai comune, potrebbe accadere che:

- diversi titolari del trattamento che vogliano implementare tecnologie simili (ad es. impianti TVCC con caratteristiche simili) possano chiedere una sola DPIA; oppure
- il medesimo titolare che voglia utilizzare la medesima tecnologia in vari luoghi (ad es. lo stesso impianto di videosorveglianza in più stazioni ferroviarie), possa svolgere una sola valutazione d'impatto.

Valutazione di impatto (art.35)

- **Importanza della DPIA**

➢ **Aiuta e guida** il titolare, oltre che al rispetto delle prescrizioni del GDPR, anche ad attestare di aver adottato misure idonee a garantire gli interessati in relazione al trattamento dei loro dati personali.

➢ La DPIA è una procedura volta a valutare e dimostrare al conformità con la normativa in materia di protezione dei dati personali.

➢ Le prescrizioni, trattate dal Gruppo di lavoro Art. 29, suggeriscono di valutarne l'impiego anche laddove il Regolamento non la prescrive come obbligatoria.

Valutazione di impatto (art.35)

- **Responsabilità della DPIA**

➢ **E' in carico al titolare del trattamento.**

➢ La valutazione dell'impatto può essere affidata ad altri soggetti non necessariamente interni all'organizzazione aziendale.

➢ Tuttavia è obbligo del titolare monitorarne lo svolgimento eventualmente per il tramite dell'RPD (Responsabile della protezione – DPO in inglese) avvalendosi del parere di esperti di settore e coordinandosi con il responsabile della sicurezza dei sistemi informativi. (CIO – CISO) e del responsabile IT (ove presenti).

➢ La DPIA deve essere condotta prima di procedere ad un qualsivoglia trattamento e deve essere assoggettata ad un continuo riesame, con valutazioni ad intervalli regolari (Audit sessions).

Valutazione di impatto (art.35)

NOVITA'

- **DPIA obbligatoria quando …**

Il Gruppo di lavoro Art. 29 individua alcuni CRITERI e linee guida specifici, ad esempio:

- trattamenti che implichino la valutazione dell'interessato, la Sua profilazione e il suo *SCORING;*
- la conclusione di contratti in modo automatizzato (es. mutui, assicurazioni, viaggi, tickets etc.);
- il monitoraggio degli interessati (es. videosorveglianza o ad esempio *log-books* interni dai quali si evincano costantemente le abitudini degli interessati od anche metatags-data delle fotografie, o *logs* di geolocalizzazione);

Valutazione di impatto (art.35)

- **DPIA obbligatoria quando …**

- dati relativi a soggetti (ritenuti) vulnerabili (anziani, minori, soggetti con patologie psichiatriche;
- dati sensibili, giudiziari o di natura estremamente personale;
- dati trattati su larga scala;
- utilizzo di soluzioni tecnologiche e organizzative innovative (es. acquisizione di foto, riconoscimento del volto, applicazioni IoT, *metatags* di foto);
- trattamenti di dati che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. *screening* di una banca attraverso dati registrati in una centrale rischi per stabilire la concessione di un mutuo)

Valutazione di impatto (art.35)

- **DPIA obbligatoria quando …**

➢ **Una DPIA è obbligatoria quando ricorrono almeno due dei criteri elencati in precedenza anche se, tenuto conto delle circostanze, il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri esposti.**

Consultazione preventiva(art. 36)

NOVITA'

- **Valutazione "ex post"**

➢ All'esito della valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) **ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale;** l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

➢ Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare;

Registri del trattamento(art.30)

NOVITA'

- **Registro delle attività di trattamento**

➢ Le Pubbliche amministrazioni e tutti i titolari e i responsabili di trattamento, ad eccezione degli organismi con meno di 250 dipendenti ma solo se non effettuano **trattamenti a rischio** *(si veda art. 30, par.5)*, e **non trattino dati su larga scala**, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

➢ 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.

Responsabile protezione dei dati RDP – DPO (art.37)

NOVITA'

- Nominato dal titolare o dal responsabile del trattamento
- Funzioni di supporto e controllo, consultive, formative e informative
- Coopera con l'Autorità e costituisce il punto di contatto in tema di trattamento dati
- Esperto della normativa, capacita di gestione di attività complesse, indipendenza, non occorrono particolari certificazioni, informa e fornisce consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi
- E' figura obbligatoria quando vengano trattati dati personali in modo sistematico **su larga scala** (Banche, Assicurazioni, società di revisione contabile, recupero crediti, partiti e sindacati) **e nelle Pubbliche amministrazion**i - **No** in ditte individuali e PMI
- Figura interna o esterna (anche Persona giuridica) non ha attività esclusiva (anche se viene raccomandata per enti di grandi dimensioni)

Codici di condotta e certificazioni (art.40/41/42)

NOVITA'

▪ Procedure

- Sempre in tema di **Valutazione d'impatto** la Guida richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.
- L'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Sportello "one stop shop" (art. 56 e 60-67)

NOVITA'

- **Sportello unico**

- Il titolare del trattamento ha diritto di rivolgersi a una autorità di controllo capofila per tutta l'Unione Europea interessato può rivolgersi all'autorità di protezione dei dati del proprio paese per segnalare eventuali violazioni qualunque sia il luogo in cui il trattamento è effettuato

Sanzioni (art. 83)

NOVITA'

- **Pecuniarie – condizioni generali**

Inosservanza degli obblighi del titolare e del responsabile del trattamento; inosservanza degli obblighi dellôorganismo di certificazione; inosservanza degli obblighi dellôorganismo di controllo:	fino a **10 milioni di Euro**, o per le imprese, fino al **2% del fatturato** annuo mondiale dellôesercizio 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 dellôautorità di controllo:	fino a **20 milioni di Euro**, o per le imprese, fino al **4% del fatturato** annuo mondiale dellôesercizio precedente.
Inosservanza di un ordine correttivo dellôautorità di controllo:	fino a **20 milioni di Euro**, o per le imprese, fino al **4% del fatturato** annuo mondiale dellôesercizio precedente.

Sanzioni (art.84)

NOVITA'

- **Prescrittive - Correttive**

All'aumento del massimo edittale corrisponde un maggiore spazio di manovra per le autorità di controllo che potranno anche applicare misure prescrittive in luogo di quelle punitive pecuniarie.

- **Rivolgere avvertimenti** al titolare del trattamento o al responsabile del sul fatto che i trattamenti previsti possono violare il GDPR
- **Rivolgere ammonimenti** al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR
- **Ingiungere** al titolare del trattamento o al responsabile del trattamento **di soddisfare le richieste** dell'interessato di esercitare i relativi diritti
- **Ingiungere** al titolare o al responsabile del trattamento **di conformare i trattamenti alle disposizioni del GDPR**, anche specificando in che modo ed entro quale termine

Sanzioni (art.84)

NOVITA'

- **Prescrittive – Correttive**
  - **Ingiungere** al titolare del trattamento **di comunicare all'interessato una violazione** dei dati personali
  - **Imporre una limitazione** provvisoria o definitiva al trattamento, incluso il divieto di trattamento
  - **Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento** e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali
  - **Revocare la certificazione** o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli artt. 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti
  - **Infliggere una sanzione amministrativa pecuniaria** in aggiunta alle presenti misure (v. sopra)
  - **Ordinare la sospensione dei flussi** di dati verso un destinatario in un paese terzo o un'organizzazione internazionale

GDPR cosa fare in pratica

NOVITA'

- Valutazione impatto DPIA
  - Puntuale profilazione del cliente/studio tramite *check list* e questionari (attenzione ad attività-servizi particolari)
  - Identificazione dei soggetti (titolari, referenti, responsabili, DPO)
  - Verifica dei luoghi dove i dati vengono archiviati (ed eventualmente distrutti)
  - Audit informatico (informativa ai dipendenti sull'uso delle mail e delle informazioni riservate ï adozione di sistemi di messaggistica criptata e repository di dati sicuri e certificati ï prove simulate di *backup* e *restore* e *disaster recovery*)
  - Data penetration test (documentati)
  - Interviste al personale e dichiarazioni di responsabilità
  - Rilascio di documento di valutazione (e identificazione del rischio)
  - Inventario della documentazione esistente

GDPR cosa fare in pratica

NOVITA'

- Adozione di codici di condotta
- Istituzione di Privacy policies documentali
- Formazione degli addetti
- Adozione di procedure interne (specie in caso di DATA BREACH per la comunicazione dell'evento ai soggetti interessati / Garante

- Verificare sovrapposizioni con **ISO 27001 e 27002** Se un'organizzazione ha già implementato questo standard, è almeno a metà strada verso il garantire la protezione dei dati personali dati e minimizzare il rischio di una perdita.