







***“Dalla privacy as possible a quella by default e by design”***

- 
- Privacy:” Diritto alla riservatezza o alla *privatezza*, cioè ad includere/escludere alcuno dalla nostra sfera privata”.
  - *“The right to be let alone”, (Samuel D. Warren e Louis D. Brandeis, Dottrina Nordamericana sul finire del XIX secolo).*

- 
- *...dal Codice in materia di protezione dei dati personali...(prima del D.Lgs.101/2018)*
  - *Art.1:"Chiunque ha diritto alla protezione dei dati personali che lo riguardano."*

- 
- *Art.2:"1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei **diritti** e delle **liberta'** **fondamentali**, nonche' della **dignita'** dell'interessato, con particolare riferimento alla **riservatezza**, all'**identita' personale** e al **diritto alla protezione** dei dati personali.*

- 
- *...tutto questo fino al 4 maggio 2016...*

- 
- ...giorno in cui viene pubblicato nella Gazzetta Ufficiale dell'Unione Europea: Il Regolamento UE2016/679, *“relativo alla protezione delle persone fisiche con riguardo al*
    - *trattamento dei dati personali, nonché,*
    - *Alla libera circolazione di tali dati.*



# Art.15 - Diritto di accesso.

**L'interessato** ha diritto di ottenere queste informazioni:

- NON esiste un trattamento a suo carico;
- ESISTE un trattamento, ed in tal caso, oltre ai propri dati deve avere accesso a...



# Art.15 - Diritto di accesso.

- Finalità;
- La categoria;
- I destinatari;
- Se possibile, il periodo di conservazione e/o i criteri per determinare tale periodo;
- L'esistenza della facoltà di proporre reclamo, di chiedere la rettifica o la cancellazione dei dati

# Art.15 - Diritto di accesso.

Caso particolare, ma non infrequente:

- l'esistenza di un processo decisionale automatizzato, compresa la profilazione,...., ed in tali casi informazioni sulla logica di utilizzata, sull'importanza e le conseguenze.
- In caso di dati trasferiti in un paese terzo o ad un'organizzazione internazionale, l'interessato deve conoscere l'adeguatezza delle garanzie in merito al trasferimento.

# Art.16 - Diritto di rettifica.

L'interessato può ottenere:

- L'integrazione dei dati, in caso di incompletezza;
- La rettifica, senza ingiustificato ritardo.

# Art.17 - Diritto alla cancellazione (oblio).

- I dati non sono necessari in relazione alle finalità;
- Revoca del consenso;
- Opposizione al trattamento, per “motivi propri” ed assenza di una ragione prevalente e legittima per procedere;
- Opposizione al trattamento di marketing diretto;
- Trattamento illecito;
- Obbligo di legge

# Art.17 - Diritto alla cancellazione (oblio).

## ECCEZIONI:

- Esercizio del diritto alla libertà di espressione informazione;
- Adempimento di un obbligo di legge;
- Svolgimento di un compito di pubblico interesse, anche nell'ambito sanitario
- Esercizio di pubblici poteri;
- Ricerca scientifica, storica o fini statistici qualora l'oblio renda impossibile o pregiudichi il conseguimento degli obiettivi del trattamento;
- Esercizio del diritto di difesa in sede giudiziaria;

# Art.18 - Diritto di limitare...

Cosa vuol dire limitare il trattamento?

- Trasferire i dati “limitati” verso un altro sistema di trattamento;
- Rimuoverli temporaneamente dai siti web o renderli inaccessibili agli utenti;

# Art.18 - Diritto di limitare...

Quando?

- Se si deve contestare l'esattezza dei dati personali, per il periodo necessario alla verifica;
- Se, nel caso di trattamento illecito, l'interessato si oppone alla cancellazione dei dati personali e chiede che ne sia limitato l'utilizzo;
- L'interessato può averne bisogno in caso di accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, quando il titolare non debba più trattarli;
- In caso di opposizione al trattamento dei dati effettuato per motivi di interesse pubblico o connesso all'esercizio di pubblici poteri. (\*)

# Art.20-Diritto alla portabilità.

I dati seguono la persona(fine ultimo della tutela).Quindi **l'interessato** ha diritto di trasmettere o far trasmettere direttamente, se tecnicamente possibile, i propri dati ad un altro titolare.

- **il titolare originario** del trattamento svolto in formato automatizzato deve:
- Rendere i dati in formato strutturato, di uso comune e leggibile da dispositivo automatico.



# Art.23-Limitazioni

In misura proporzionata, necessaria e legittima i diritti di cui abbiamo parlato possono essere limitati per ragioni più varie, tra cui:

- Difesa e sicurezza nazionale e pubblica;
- Attività giudiziaria e svolgimento dell'attività giurisdizionale;
- Attività di prevenzione, ecc.



# L'interessato

- È il soggetto a cui si riferiscono i dati

# Art.4-II Titolare

Attua misure tecniche ed organizzative per

- Garantire
- Essere in grado di dimostrare(c.d.*accountability*)

che il trattamento è *compliant* col GDPR.

# Art.4-il Titolare

Come garantisce la compliance?

- Tiene conto del contesto, della natura, delle **finalità**, dello stato dell'arte dei rischi connessi;
- Attua politiche adeguate o aderisce a codici di condotta o a meccanismi di certificazione.

# Art.4-II Titolare

- Adotta la *pseudonimizzazione* e la *minimizzazione* per attuare i principi di protezione sia quando determina i mezzi, sia all'atto del trattamento stesso (*by default*);
- Tratta solo i dati personali necessari per ogni specifica finalità di trattamento, tenuto conto della quantità dei dati, della portata del trattamento, del periodo di conservazione e dell'accessibilità (*by design*).

# Art.26-Contitolari

Due o più titolari...

- Regolano mediante accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento.
- In relazione a sé stessi ed in relazione all'interessato.
- L'accordo, nelle sue parti essenziali è portato a conoscenza dell'interessato.

# Art.28-Responsabile del t.

Soggetto(\*) preposto al trattamento dal Titolare.

- Effettua il trattamento solo su istruzione documentata del titolare del trattamento;
- Mette in atto tutte le misure di sicurezza(art.32);
- Garantisce che le persone autorizzate al trattamento si siano impegnate o abbiano un adeguato obbligo legale di riservatezza;
- Stipula un contratto con il titolare.



# DPO

Data Protection Officer



# Art.37-Responsabile della protezione dei dati.

È designato dal titolare o dal responsabile, quando:

- Trattamento effettuato da un'autorità o da un organismo pubblici, quelle giudiziarie, quando esercitano funzioni giurisdizionali;
- I trattamenti svolti per loro natura richiedono il monitoraggio regolare e sistematico degli interessati, su larga scala
- Il trattamento su larga scala riguarda dati sull'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche

# Art.39 e 38 Compiti e Posizione del DPO

- Coopera con l'Autorità di controllo (Garante);
- Informa e fornisce consulenza (titolare, responsabile dipendenti);
- Fornisce un parere in merito alla V.I.P.D;
- Viene tempestivamente e adeguatamente coinvolto in tutte le questioni riguardante la protezione dei dati;
- Titolare e responsabile forniscono le risorse adeguate allo svolgimento del compito;
- Titolare e responsabile assicurano che tali compiti e funzioni non siano svolte in conflitto di interessi.

# Art.39 e 38 Compiti e Posizione del DPO

Cosa fa concretamente(per esempio):

- Comunica il Data Breach al Garante;
- Rendiconto nel merito(annuale) e finanziario;
- Garantisce tempi certi di risposta;
- Visita periodicamente la sede;
- Programma sessioni di consulenza ed informazione;
- È designato con un contratto(\*).

# Art.5 Trattamento e principi.

- Lecito: se fondato sul consenso dell'interessato o su altra base prevista per legge (art.6);
- Corretto: i dati devono essere adeguati, pertinenti e limitati a quanto necessario a quanto necessario rispetto alla finalità; Extrema ratio-minimizzazione;
- Il trattamento deve garantire la conservazione in una forma che consenta l'identificazione per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

# Art.7-Condizioni per il consenso.

- Chi riceve il consenso al trattamento (il titolare, altri) deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso;
- Ovviamente, a fronte di una richiesta di consenso esplicita e distinguibile.

# Art.9-Categorie particolari di dati.

È vietato trattare i dati relativi a

- Origine razziale o etnica;
- Le opinioni politiche o sindacali;
- Le convinzioni religiose o filosofiche;
- Genetici e/o biometrici, allorché consentano l'identificazione in modo univoco della p.f;

Il divieto non sussiste se vi è il consenso o se ricorrono le ipotesi richiamate dal comma 2°.

# Art.32-Sicurezza del trattamento.

Il titolare ed il responsabile

- Mettono in atto misure tecniche ed(\*) organizzative,
- Tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del rischio di varia probabilità per i diritti e le libertà.

# Art.32-Sicurezza del trattamento.

Misure attuabili e previste:

- 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.





# Art.30-Registri delle attività di trattamento.

- Nome e dati di contatti del titolare e di tutti i soggetti coinvolti;
- Finalità del trattamento;
- Descrizione delle categorie di interessati e dei dati personali;
- Destinatari a cui i dati saranno comunicati, compresi quelli dei paesi terzi;
- Se i dati sono trasferiti verso un paese o un'organizzazione o un paese terzo;
- Una descrizione generale delle misure di sicurezza attuate.
- I termini ultimi previsti per la cancellazione.

# Art.35-Valutazione d'impatto sulla protezione dei dati.

Quando si utilizzano nuove tecnologie per il trattamento il titolare deve fare la valutazione.

- È preventiva;
- Se c'è il DPO, deve essere sentito;
- Può raccogliere le opinioni sul trattamento previsto degli interessati o dei loro rappresentanti.

# Art.35-Valutazione d'impatto sulla protezione dei dati.

Contenuto minimo:

- Valutazione della necessità e della proporzionalità, in relazione alle finalità;
- Una valutazione dei rischi per i diritti e le libertà degli interessati;
- Una valutazione delle misure e delle garanzie previste per affrontare i rischi e dimostrare la conformità al GDPR;
- Tiene conto dei diritti e degli interessi legittimi degli interessati e di una eventuale adozione dei codici di condotta.

# Art.35-Valutazione d'impatto sulla protezione dei dati.

Dalla valutazione può emergere:

- Assenza di rischio;
- Rischio. In tal caso il titolare può:
- Procedere ad un riesame, quando insorgono variazioni del rischio;
- Consultare il Garante, se la valutazione indica un rischio elevato, assunto in assenza di misure adeguate.

# Art.35-Valutazione d'impatto sulla protezione dei dati.

Il Garante fornisce un parere scritto al titolare, entro il termine di otto settimane (prorogabili di altre sei) sospendibile per consentire una più completa istruttoria.

- Se riscontra violazioni del GDPR ed, in particolare, qualora il titolare non abbia identificato o attenuato sufficientemente il rischio.

**TRASFERIMENTO  
DATI PERSONALI**



# Art.44-Trasferimento dati.

Trasferimento:

- Sulla base di una decisione di adeguatezza;
- Soggetto a garanzie di adeguatezza;



# Art.44-Trasferimento dati.

## **Decisione di adeguatezza.**

Il trasferimento non necessita di autorizzazione specifica, se:

- Lo Stato o l'organizzazione terza garantiscono o operano in una condizione di garanzia che si evince dallo stato di diritto, dal rispetto dei diritti umani, sia dotato di legislazione pertinente efficacemente attuata;
- Esistenza e l'effettivo funzionamento di un'autorità di controllo;
- Impegni internazionali assunti dal paese terzo o dall'organizzazione.

# Art.44-Trasferimento dati.

In esito alla valutazione di adeguatezza, la Commissione emana i c.d. *atti di esecuzione* che attestino la reale adeguatezza assicurata da un determinato paese o una determinata organizzazione.

- Sono revisionati periodicamente ogni quattro anni;
- Qualora non vengano più soddisfatte le condizioni di adeguatezza, la Commissione revoca, modifica o sospende gli atti;
- L'elenco dei paesi compliant e non sono pubblicati sulla Gazzetta Ufficiale dell'Unione Europea.

# Art.44-Trasferimento dati.

## **Trasferimento soggetto a prestazione di garanzie adeguate.**

Se la commissione non si pronuncia il titolare e il responsabile possono effettuare il trasferimento a condizione che l'interessato disponga di diritti azionabili e mezzi effettivi di ricorso. Vi sono poi:

- Garanzie che non presuppongono di autorizzazione dell'autorità di controllo;
- Garanzie che invece la prevedono.



# Mezzi di ricorso, responsabilità e sanzioni.

- **Reclamo al Garante:** Se ritengo che il trattamento violi il regolamento;
- **Ricorso giurisdizionale effettivo:** contro le decisioni giuridicamente vincolanti del Garante, oppure se quest'ultimo non tratta un reclamo o non informi l'interessato entro tre mesi;
- Si propone anche qualora il titolare o il responsabile violino un diritto garantito dal GDPR;

# Mezzi di ricorso, responsabilità e sanzioni.





# Mezzi di ricorso, responsabilità e sanzioni.

Sanzioni:

- Amministrative pecuniarie;
- Amministrative non pecuniarie.



# INFOLEX MARKETING



# GRAZIE

## Contatti:

- [ginopappalardo@gmail.com](mailto:ginopappalardo@gmail.com)
- [www.facebook.com/studiopappalardo](http://www.facebook.com/studiopappalardo)
- [www.linkedin.com/ginopappalardo](http://www.linkedin.com/ginopappalardo)
- [GinoPappalardo@Gino1Pappalardo](https://twitter.com/GinoPappalardo)
- [www.infolexmarketing.it](http://www.infolexmarketing.it)



Quest'opera è distribuita con Licenza  
Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Int  
ernazionale