# GDPR:
# CHE FARE?

INFORMATICA F.M.

# GDPR: Che cosa è...

**General Data Protection Regulation (o GDPR o anche RGPD)**

**Regolamento 2016/679/UE**

Siamo nell'ambito della tutela della privacy (diritto fondamentale della persona=diritto ad essere lasciati indisturbati e di «escludere» altri dalla propria sfera privata o diritto di controllare come gli altri trattino i propri dati)
Riguarda la tutela delle persone fisiche con riferimento al trattamento dei dati personali e la libera circolazione dei dati (come la Direttiva 1995/46 e il D. Lgs. 196/03)

**Attenzione:** trattamento di dati è qualsiasi operazione che riguarda dati quali - ad esempio - la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, la comunicazione e la la diffusione

# GDPR: Che cosa è

- È un regolamento europeo che si applica al trattamento dei dati personali (nome, cognome, codice fiscale, ect.). Coinvolgerà tutte le persone fisiche e **tutte le aziende di qualsiasi dimensione.**
- È entrato in vigore il **24 maggio 2016**.
- Diventerà direttamente applicabile in tutti gli Stati membri dal 25 maggio 2018 Introduce regole più chiare in materia di informativa e consenso.
- Definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (Data Breach).
- Si applica ai trattamenti di dati di interessati che si trovano in UE (offerta di prodotti o servizi destinati a soggetti presenti in UE)

# Adempimenti previsti in D.LGS 196/03.

- Notifica (preventiva) al Garante, se necessario
- Autorizzazione al trattamento (Autorizzazioni Generali)
- Informativa e raccolta del consenso dell'Interessato
- Accorgimenti ed adempimenti per comunicazione e/o trasferimento all’estero dei dati
- Cessazione del trattamento
- Misure di sicurezza (idonee e minime)

# Con il regolamento 679/2016

**COSA RESTA**

- Protezione delle sole persone fisiche
- Definizione di trattamento
- Definizione di dato personale
- Principi relativi al trattamento dei dati
- Liceità del trattamento
- Obbligo di informativa
- Obbligo di consenso
- Soggetti che effettuano il trattamento (eccetto DPO)
- Adozione di misure tecniche e organizzative idonee = adeguate

**COSA CAMBIA**

- Diritto all'oblio
- Portabilità dei dati
- Privacy by default e privacy by design
- Responsabilizzazione di titolare e responsabile
- Registro dei trattamenti
- Obbligo di notifica e comunicazione in caso di data breach
- Valutazione d'impatto
- Misure tecniche adeguate (=idonee) quali ad es. pseudonimizzazione, cifratura, ..
- DPO
- Certificazioni
- Entità delle sanzioni

# Diritto all’oblio Art. 17

L'interessato ha diritto di ottenere la cancellazione **senza ingiustificato ritardo** qualora:

- I dati non siano più necessari rispetto alle finalità per le quali sono stati raccolti
- Il consenso al trattamento venga revocato
- L’interessato si opponga al trattamento
- I dati siano trattati illecitamente
- I dati debbano essere cancellati per legge

# Portabilità dei dati Art. 20

L’articolo 20 del regolamento generale sulla protezione dei dati (RGPD) introduce il nuovo diritto alla portabilità dei dati. Tale diritto consente all’interessato di ricevere i dati personali forniti a un titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare del trattamento senza impedimenti. Il diritto in questione è soggetto a determinate condizioni e mira a promuovere la libertà di scelta degli utenti, il loro controllo sui trattamenti e i loro diritti.

L’esercizio del diritto di accesso previsto dalla direttiva sulla protezione dei dati (95/46/CE) è vincolato al formato che il titolare decide di utilizzare nel fornire le informazioni richieste.

Il nuovo diritto alla portabilità intende promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all’altro (che si tratti dei propri sistemi, dei sistemi di soggetti terzi fidati, o di quelli di un diverso titolare del trattamento).

# Accountability (Artt. 23 25 e capo IV)

Aspetto principale per quanto riguarda la governance

• Si riferisce all'obbligo per un soggetto di rendere conto delle proprie decisioni e di essere responsabile per i risultati conseguiti.

• Disposizioni tese a promuovere approcci proattivi in un’ottica di prevenzione di possibili problematiche e di riduzione degli oneri solo burocratici

• Il principio dell’accountability richiede che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Secondo questo principio è sempre il titolare del trattamento ad avere la piena responsabilità delle scelte messe in campo.

• **ATTENZIONE**: responsabilità SOLIDALE per violazioni e conseguenti sanzioni

# Privacy by Default e by Design – Art 25

Il GDPR introduce l'obbligo di trattare i dati secondo due tipo di progettazione:

**By Design** cioè analizzando il trattamento per tutto il ciclo di vita dei dati. Fa riferimento all'obbligo di tutelare i diritti dell'interessato nell'attività di trattamento fin dalla fase della progettazione e per l'intera gestione del ciclo di vita dei dati, ponendo in essere misure di carattere tecnico ed organizzativo quali la minimizzazione e la pseudonimizzazione

**By Default** cioè il partire da configurazioni "chiuse" dei sistemi informatici, per poi gradualmente ampliarle solo dopo avere valutato l'impatto di eventuali aperture ovvero le impostazioni predefinite devono essere quella che garantiscono il maggior rispetto della privacy, affinché i dati personali non siano resi accessibili ad un numero indefinito di persone senza l'intervento umano

# Registri dei trattamenti - Art 30

**Vi ricordate il «vecchio» DPS?**

Redazione a carico sia del Titolare che del Responsabile del Trattamento (uno ciascuno)

Dovrà contenere:

- I dati dei soggetti coinvolti (titolare, contitolare, rappresentante responsabile della protezione dei dati);
- Finalità del trattamento;
- Descrizione delle categorie di interessati e delle categorie di dati trattati;
- Elenco dei destinatari dati (anche in Paesi terzi);
- Descrizione dei trasferimenti anche extra UE;
- Indicazione dei termini ultimi di cancellazione, ove possibile;
- Descrizione delle misure di sicurezza tecniche e organizzative.

Il suddetto registro sarà obbligatorio **SOLO** per organizzazioni con più di 250 dipendenti ovvero che trattino dati con modalità che determinino un rischio per i diritti e le libertà dell'interessato, ovvero nei casi in cui il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (=sensibili, art. 9.1) o i dati personali relativi a condanne penali e a reati (art. 10).

# Obbligo di notifica e comunicazioni in caso di Data Breach- Artt. 33 e 34

Termine brevissimo : **72 ore dalla scoperta**

**Eccezione**: non è obbligatorio se è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone.

Deve indicare almeno la natura della violazione, le categorie, il numero di interessati e di registrazioni coinvolti, le probabili conseguenze, le misure adottate o da adottare per porre rimedio alla violazione

Se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati è obbligatorio comunicare agli stessi la violazione senza giustificato ritardo, salvo che dati fossero stati resi incomprensibili (ad es. cifratura), oppure siano adottate misure per scongiurare il rischio di lesione, ovvero la comunicazione richieda uno sforzo sproporzionato (in questo caso è necessaria una comunicazione pubblica o similare)

# Valutazione d’impatto-Art. 35

Necessaria quando un trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone soprattutto se effettuato con nuove tecnologie.

- È richiesta se c’è:
  - trattamento automatizzato, compresa profilazione
  - trattamento su larga scala di dati sensibili e giudiziaria
  - sorveglianza sistematica su larga scala di aree accessibile al pubblico

- Deve essere preventiva
- L’autorità di controllo può redigere l’elenco delle tipologie di trattamenti per i quali è necessaria valutazione d’impatto
- Deve contenere almeno la descrizione sistematica dei trattamenti previsti e la finalità (compreso l’interesse del titolare), la valutazione di necessità e proporzionalità del trattamento rispetto alle finalità, la valutazione dei rischi per i diritti e le libertà degli interessati, le misure per affrontare i rischi.

# Misure tecniche adeguate - Art. 32

E’ necessario mettere in atto misure tecniche ed organizzative adeguate a garantire un livello adeguato al rischio quali ad esempio:

- pseudonimizzazione
- cifratura
- capacità di assicurare su base permanente riservatezza, integrità, disponibilità e
- resilienza dei sistemi e dei servizi di trattamento
- capacità di ripristinare tempestivamente disponibilità e accesso dei dati in caso di incidente fisico o tecnico
- implementazione di una procedura di test deirefficacia delle misure

# Data Protection Officier (DPO) – Artt. 37 e 39

- Ne è obbligatoria la nomina per le pubbliche autorità e gli organismi pubblici, **per chi opera monitoraggio sistematico degli interessati su larga scala e quando trattamento si svolge su larga scala su dati sensibili** (precisazioni a pag. successiva) e giudiziari e per aziende con più di 250 dipendenti.

- Deve avere conoscenze specialistiche, deve essere coinvolto nelle questioni riguardanti il trattamenti di dati, deve essere autonomo e indipendente, deve avere budget di spesa.

- La scelta del DPO è esclusivo compito del responsabile del trattamento dei dati

- L'orientamento del garante è che il DPO non sia un dipendente della società.

# Precisazione: trattamento su Larga Scala e DPO

Vengono in seguito esplicitati quattro elementi da tenere in considerazione per valutare se il trattamento viene effettuato su "**larga scala**" e quindi se necessita o meno della **nomina di un DPO**:

a) il numero degli interessati coinvolti;
b) la quantità dei dati e/o il tipo dei dati oggetto di trattamento;
c) la durata o la permanenza del processo di trattamento dei dati;
d) l'estensione geografica del trattamento.

L'interpretazione del concetto di "larga scala" **non è pacifica e univoca**.

Infatti ci sono delle situazioni rientranti in una "**zona grigia**" come, ad esempio, **il singolo Medico** che tratta un rilevante numero di dati in un'estesa zona geografica rispetto ad un **Poliambulatorio** con **più di un medico cooperante**. Nei casi dubbi **e' consigliabile procedere comunque alla nomina**, a fini precauzionali.

# Certificazioni - Artt. 42 e 43

- Al momento non esistono certificazioni ufficiali
- Possibile certificazione della protezione dei dati e di sigilli e marchi di protezione dei dati
- Organismi di certificazione (ad oggi forse uno, per quanto a nostra conoscenza)

# Entità delle sanzioni - Art. 83

- **Fino a 10 milioni di euro o al 2% del fatturato mondiale totale annuo** dell'anno precedente se superiore ad esempio qualora siano violati gli obblighi posti a carico del titolare e del responsabile del trattamento, dell'organismo di certificazione e dell'organismo di controllo.

- **Fino a 20 milioni di euro o al 4% del fatturato mondiale totale annuo** dell'anno precedente se superiore ad esempio qualora siano violati i principi dettati in materia di principi base del trattamento ed in particolare del consenso, i diritti degli interessati, le disposizioni in materia di trasferimenti di dati in paesi terzi, inosservanza di ordini o limitazioni di trattamento o in caso di negato accesso.

# Dopo l’approvazione del GDPR

# E dopo il 25 maggio 2018…

# GDPR: Legal…

La parte legal, ovvero quella che riguarda gli aspetti legali del GDPR è la più corposa e forse la più complicata.

In particolare per quanto riguarda i concetti di:

- Accountability
- DPO
- Registro dei trattamenti
- Informative

**Inoltre non può essere standardizzata**; va declinata su misura per ogni tipologia di dati trattati e azienda.

Lo Studio di Informatica F.M. si avvale di **esperti di Privacy** e di uno **studio legale** per accompagnare i propri clienti alla **GDPR compliance**.

# GDPR: Conclusioni…

“Riprendere in mano” il sistema gestione privacy dell’azienda in essere (partendo da informative e consensi, lettere di nomina, eventuale DPS, contrattualistica, etc.) e verificarne la conformità ai principi del GDPR analizzare le modalità di trattamento dei dati ed i rischi ad esso connessi per valutare l’adeguatezza delle misure di sicurezza (tecniche ed organizzative) in essere ai principi del GDPR ed eventualmente programmare le relative implementazioni.

- **RIGUARDA TUTTE LE AZIENDE**

- **C’È TEMPO FINO AL 24 MAGGIO 2018 PER ADEGUAMENTI**

**ATTENZIONE** agli interventi sulla normativa nazionale (Codice Privacy D. Lgs. 196/03) e agli interventi del Garante con Provvedimenti e Linee Guida.