# LE NOVITÀ DEL GDPR E GLI IMPATTI PER LE AZIENDE

Francesca Lonardo
Avvocato specializzato nel diritto delle nuove tecnologie e data protection – Partners4Innovation (P4I)

6 dicembre 2017

# STRUMENTO GIURIDICO, ENTRATA IN VIGORE ED APPLICABILITÀ

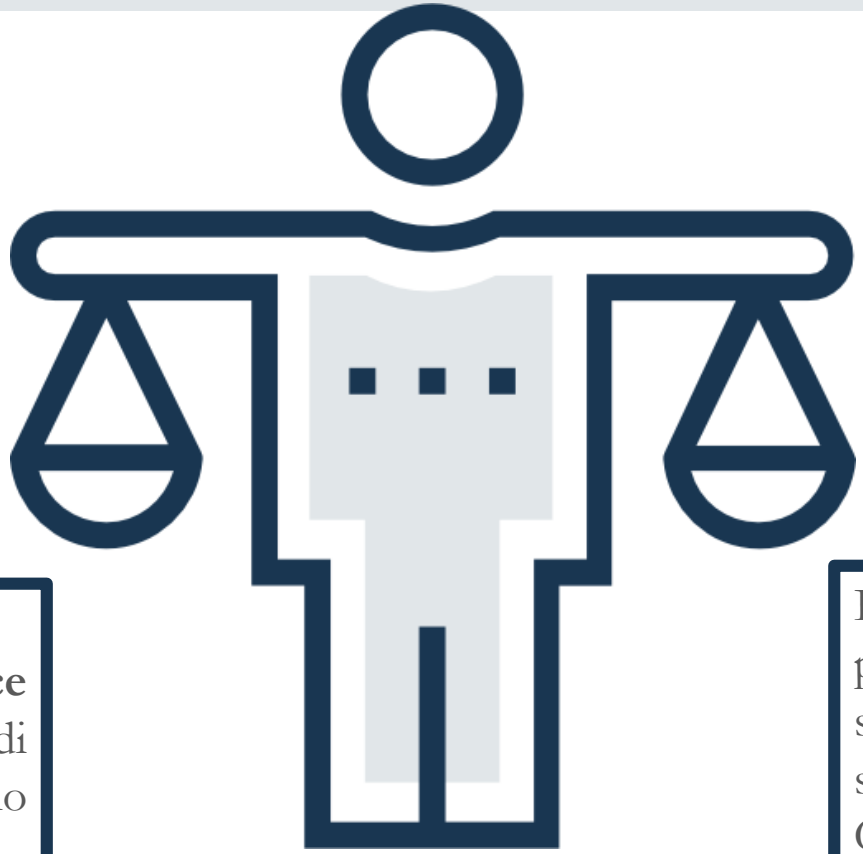
Il Regolamento UE 2016/679 (Regolamento Generale sulla protezione dei dati personali) che **ABROGA** la **Direttiva 95/46/CE** (da cui deriva il nostro **Codice Privacy**), **è entrato in vigore** il 24 maggio 2016 e **diventerà applicabile** a partire dal **25 maggio 2018** dopo un periodo di transizione di **due anni.**

La nuova normativa europea in materia di tutela dei dati personali è un **REGOLAMENTO** e non più una Direttiva

→ **direttamente applicabile** in tutti gli stati membri senza bisogno di trasposizioni nazionali

# COSA ACCADE AL CODICE PRIVACY?

Il nostro legislatore è recentemente intervenuto con 2 provvedimenti legislativi



**Riorganizzazione** complessiva del **Codice Privacy** (che sarà quindi modificato per renderlo conforme al GDPR)

Intervento fin da ora, in particolare, sull'art. 29 sul Responsabile e sull'art. 110 bis del Codice

# COSA ACCADE AL CODICE PRIVACY?

## Legge 163/2017 «Legge di delegazione»

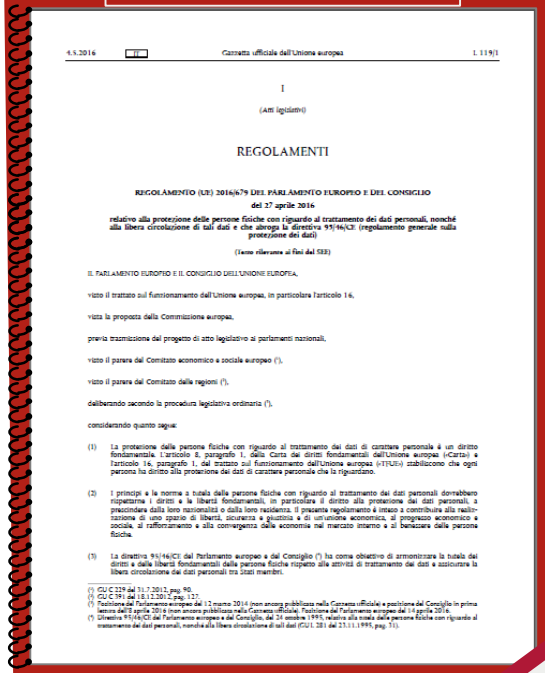
L'**art. 13** della legge delega specificamente il Governo ad adottare, entro **sei mesi** dalla data della sua entrata in vigore, **decreti legislativi** per **adeguare** la **normativa nazionale** alle **disposizioni del GDPR**.

Il Governo nell'esercizio della delega dovrà seguire i seguenti **principi** e **criteri direttivi**:

- **abrogare** le disposizioni del Codice Privacy che siano **incompatibili** con le disposizioni di cui al GDPR;
- **modificare** le norme del Codice Privacy al fine di **dare puntuale attuazione alle disposizioni del Regolamento non direttamente applicabili**;
- **coordinare** le disposizioni vigenti del Codice Privacy con **le disposizioni** di cui al Regolamento;
- prevedere, ove opportuno, il ricorso a **provvedimenti** attuativi e integrativi **del Garante** nell'ambito e per le finalità previste dal Regolamento;
- **adeguare,** nell'ambito delle modifiche al Codice Privacy, **l'attuale regime sanzionatorio penale** e **amministrativo**, alle disposizioni del Regolamento.

# COSA ACCADE TRA SEI MESI?

## GDPR



4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/1

I

(Atti legislativi)

REGOLAMENTI

**REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**
**del 27 aprile 2016**
**relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)**

**(Testo rilevante ai fini del SEE)**

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo (1),

visto il parere del Comitato delle regioni (2),

deliberando secondo la procedura legislativa ordinaria (3),

considerando quanto segue:

(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

(3) La direttiva 95/46/CE del Parlamento europeo e del Consiglio (4) ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali della persona fisica rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

(1) GU C 229 del 31.7.2012, pag. 90.
(2) GU C 391 del 18.12.2012, pag. 127.
(3) Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura del 8 aprile 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 14 aprile 2016.
(4) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

## CODICE PRIVACY

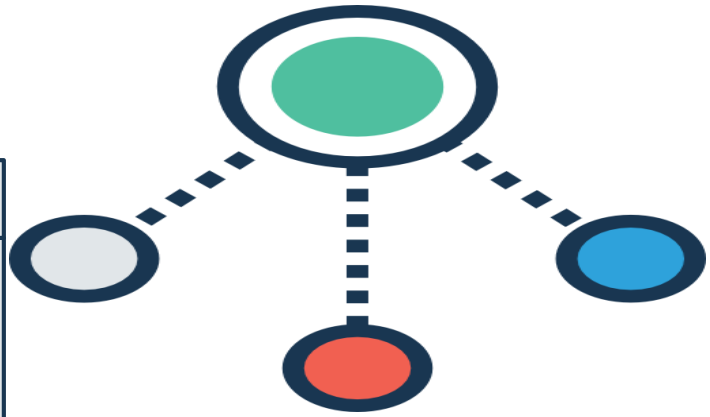
# COSA ACCADE AL CODICE PRIVACY?

## Legge 167/2017

Nel contempo, con la legge del 20 novembre 2017, n. 167, "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea*" sono state già apportate **modifiche al Codice Privacy**, in particolare all'art. 29 (Responsabile del trattamento), probabilmente per consentire al Garante di adottare fin da ora «**schemi tipo**» per gli **«atti giuridici»** che regolano i rapporti fra titolare e responsabile previsti dall'art. 28, co. 8 del GDPR.

# COSA SI INTENDE PER «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, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».*



## DATI COMUNI

- Dati anagrafici (es. nome e cognome)
- Dati di contatto (es. indirizzo fisico e di posta elettronica)
- Dati fiscali (es. codice fiscale)
- Dati contabili (es. IBAN)
- Immagini
- (…)

## RELATIVI A CONDANNE PENALI E REATI

- Qualità di imputato o indagato
- Casellario giudiziale
- Carichi pendenti

## CATEGORIE PARTICOLARI DI DATI

- Dati genetici
- Dati biometrici (es. impronta digitale)
- Dati relativi allo stato di salute
- Dati che rilevano l'appartenenza sindacale
- Dati che rivelano opinioni politiche
- (..)

# QUALI NOVITÀ?

Le definizioni ed i principi generali previsti dal Codice Privacy restano sostanzialmente invariati, ma **cambia la filosofia**

Viene introdotto un nuovo approccio metodologico, ***risk-based***, basato sulla protezione dei dati dell'utente e sull'effettivo rischio per ogni azienda

La «privacy» deve essere calata all'interno dei processi e dell'organizzazione aziendale, non più come elemento/adempimento successivo, ma presupposto da considerare già nella fase di progettazione dei processi, servizi, prodotti o applicativi (cfr. «**privacy by design**»).

Si passa da un sistema di tipo formalistico (basato sulla previsione di regole formali e su un elenco di adempimenti e misure minime da adottare), ad un sistema di governance dei dati personali basato su un'alta responsabilizzazione sostanziale («***accountability***») del **Controller**, a cui è richiesto proattività, cioè di prevenire e non correggere, nonché di **dimostrare,** tramite l'elaborazione di un idoneo sistema **documentale** di gestione della privacy (che includa l'adozione di specifici modelli organizzativi, analoghi a quelli utilizzati nell'applicazione della 231, e di appropriate **policy interne,** da esibire in caso di richiesta da parte dell'Autorità), **la conformità al GDPR** e l'adeguatezza delle proprie scelte/valutazioni.

# IMPLICAZIONE DELL'«ACCOUNTABILITY» PER I TITOLARI

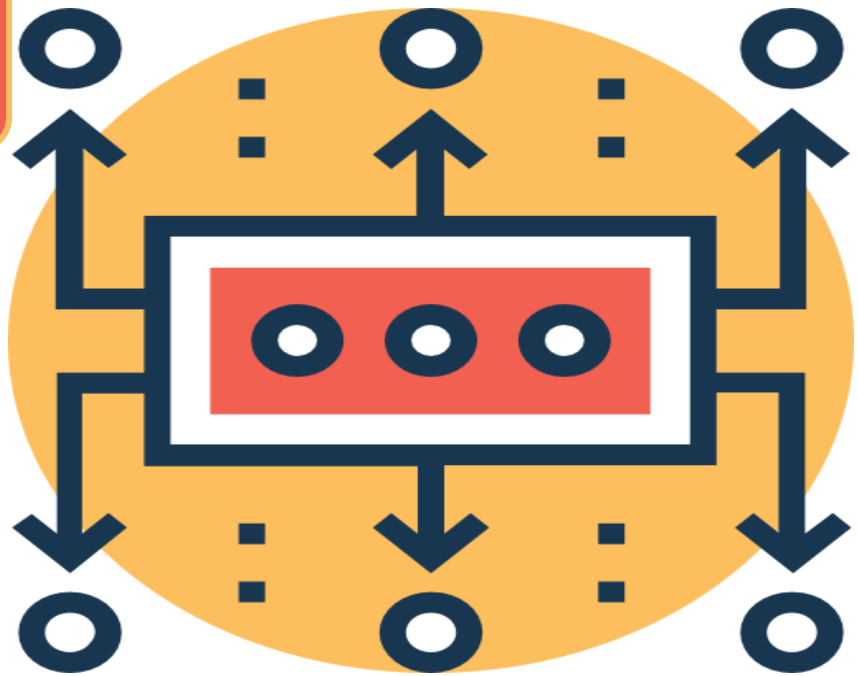
La **maggiore discrezionalità** per i TITOLARI di **DECIDERE** le **MODALITÀ** attraverso le quali conformarsi alle sue disposizioni è gravata dall'ONERE di essere IN GRADO DI DIMOSTRARE le **RAGIONI** che hanno portato a tali decisioni e le **MOTIVAZIONI** alla base delle scelte

Sarà per esempio necessario essere in grado di documentare il processo che ha portato alla valutazione di un determinato rischio in materia di sicurezza, alla decisione di notificare o meno agli interessati un «data breach», di aver attuato in relazione ad un nuovo trattamento le necessarie valutazioni legate alla privacy «by design»

# PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

**liceità, correttezza e trasparenza**

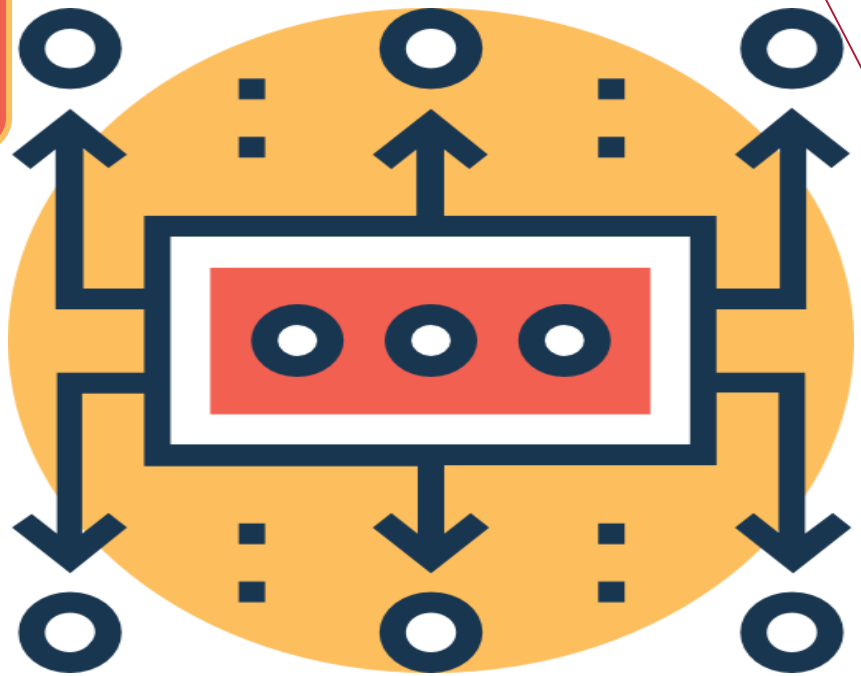
I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.



# PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

liceità, correttezza e trasparenza

limitazione della finalità

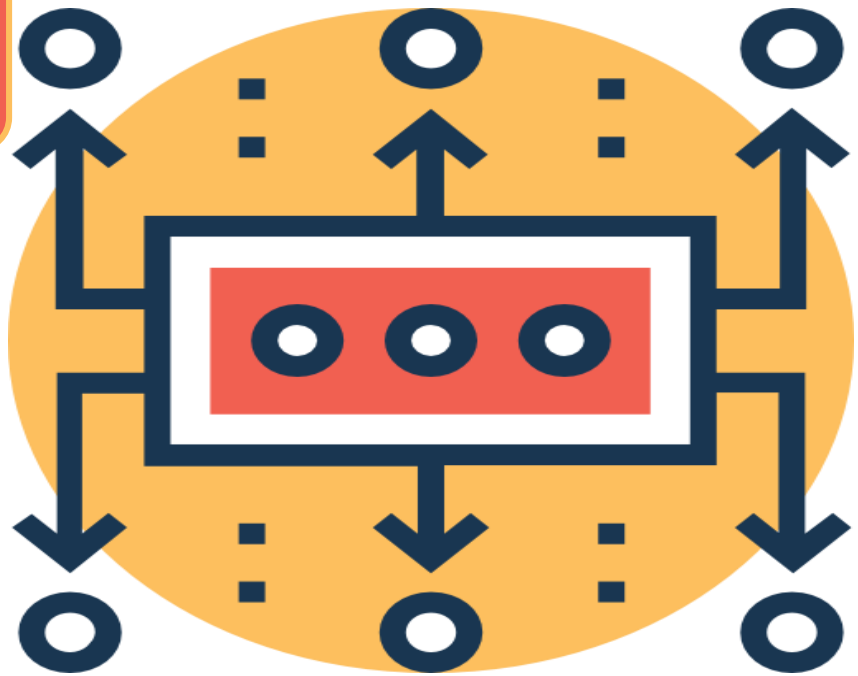


I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità

# PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

liceità, correttezza e trasparenza

limitazione della finalità



minimizzazione dei dati

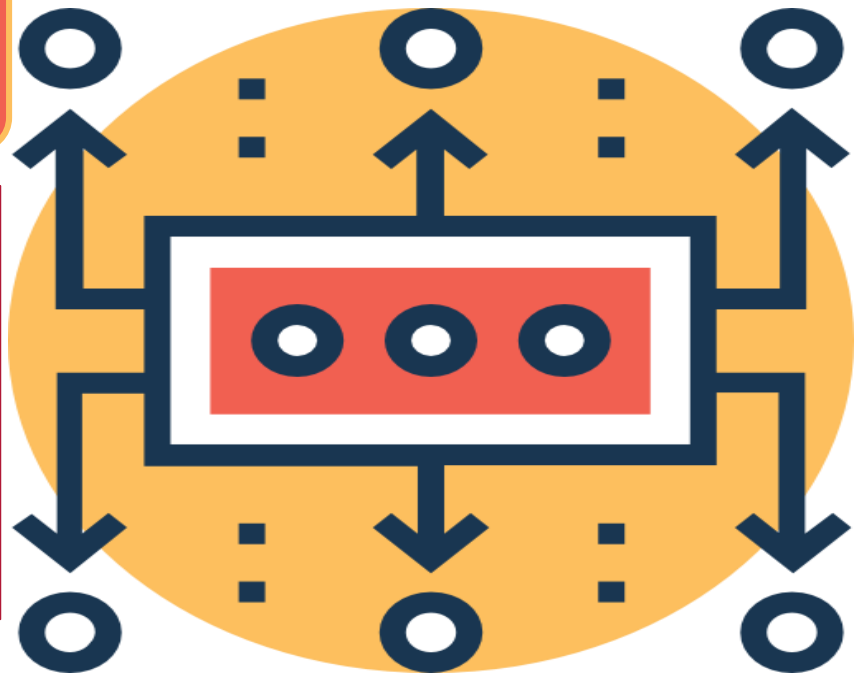
I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

# PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

liceità, correttezza e trasparenza

limitazione della finalità

minimizzazione dei dati



I dati personali sono esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati

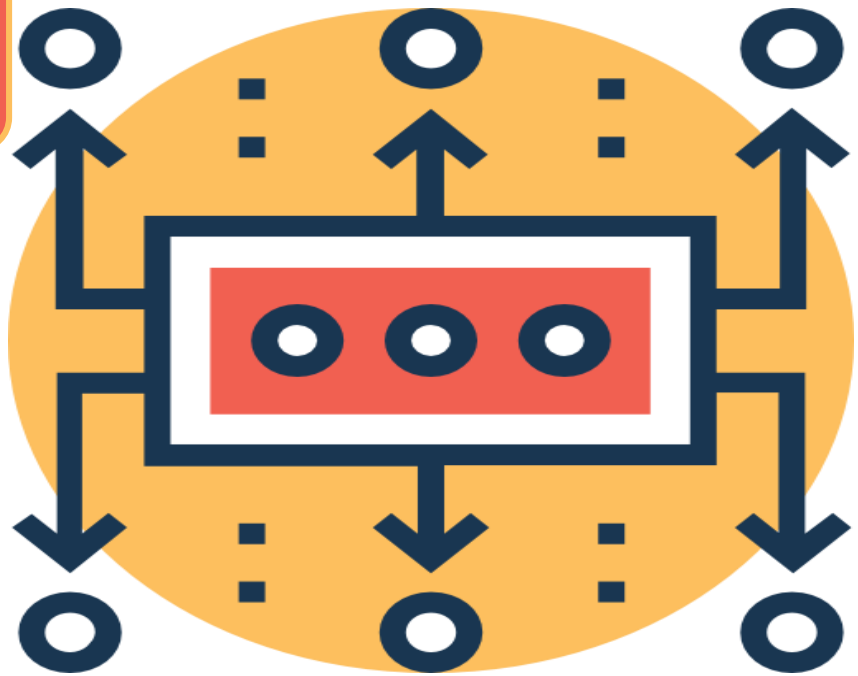
esattezza

# PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

liceità, correttezza e trasparenza

limitazione della finalità

minimizzazione dei dati



esattezza

limitazione della conservazione

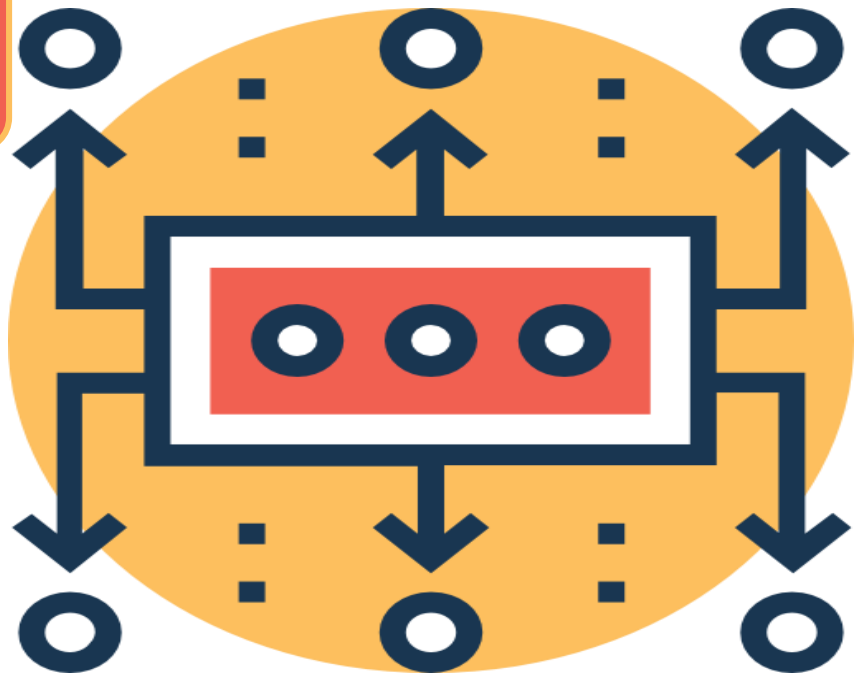
I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati

# PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

liceità, correttezza e trasparenza

limitazione della finalità

minimizzazione dei dati



I dati personali sono trattati in maniera 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

esattezza

limitazione della conservazione

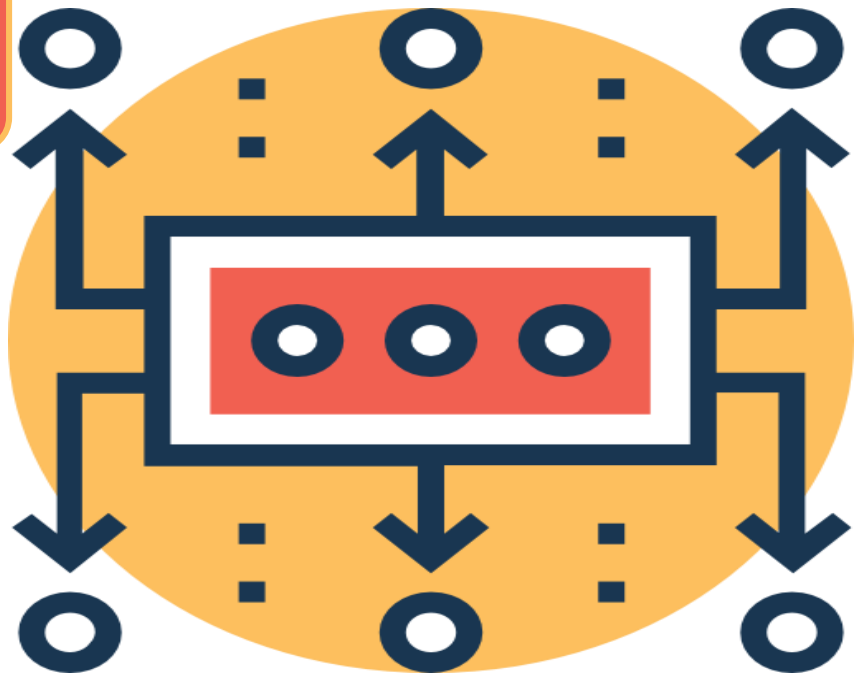
integrità e riservatezza

# PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

liceità, correttezza e trasparenza

limitazione della finalità

minimizzazione dei dati



esattezza

limitazione della conservazione

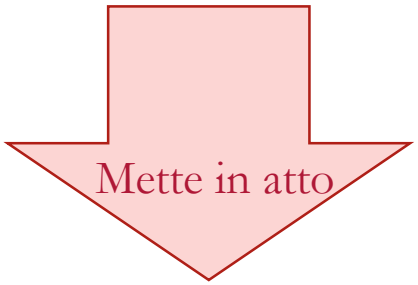
integrità e riservatezza

Il titolare del trattamento è responsabile del rispetto del principi sopra indicati e deve essere in grado di dimostrarlo («***accountability***») - art. 5 co 2.

# FOCUS SU ACCOUNTABILITY (ARTT. 4, CO.2 E 24)

**Il TITOLARE** è responsabile per la *compliance* ai principi privacy e deve essere in grado di DIMOSTRARLA (art. 5, co.2)

Tenuto conto di
**NATURA, AMBITO, CONTESTO, FINALITA', RISCHI**




Misure **TECNICHE** ed **ORGANIZZATIVE ADEGUATE** per garantire, ed essere in grado di **dimostrare**, che il trattamento è effettuato conformemente al GDPR. Dette misure sono riesaminate ed aggiornate qualora necessario.

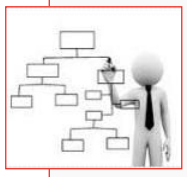
Ciò implica l'adozione di un SISTEMA DI GESTIONE DELLA DATA PROTECTION che consenta di gestire nel tempo la compliance in ottica gestionale (vedi slide successiva).

# IMPLICAZIONI PER LE AZIENDE

Predisporre un **SISTEMA DI GESTIONE DELLA DATA PROTECTION**

1. Considerare la privacy sin dalla fase di progettazione

4. Formalizzare la documentazione di adeguamento ai singoli obblighi normativi



2. Attribuire RUOLI e RESPONSABILITÀ in materia di data protection all'interno dell'organizzazione; formalizzare un preciso **organigramma privacy interno** che definisca "chi fa cosa", coerentemente alle mansioni azienda

5. Implementare **meccanismi di controllo interno** per verificare l'effettiva applicazione delle misure adottare e adeguate politiche di informazione aziendale


3. Prevedere regolamenti e procedure per la gestione della data protection

6. Monitorare le misure ed aggiornale se necessario (audit interni o estreni)

# MISURE DI SICUREZZA ADEGUATE (ART. 32, CO. 1)

**NON** sono più previste **MISURE MINIME** come quelle indicate tassativamente e «tipizzate» nell'Allegato B D.Lgs. 196/03

**TITOLARE «CONTROLLER»**

**RESPONSABILE «PROCESSOR»**

Mettono in atto

Misure **TECNICHE** ed **ORGANIZZATIVE** **adeguate per garantire un livello di sicurezza** adeguato al rischio…

… tenuto conto di:

**STATO DELL'ARTE** e dei **COSTI DI ATTUAZIONE**, nonché **NATURA, AMBITO, CONTESTO, FINALITA', RISCHI**

# REGISTRO DEI TRATTAMENTI

Con il GDPR è stato introdotto l'**obbligo** di tenere un **registro delle attività di trattamento** contenente le informazioni di cui all'art. 30 del GDPR

- **per le imprese con più di 250 dipendenti** (sempre)
- per le imprese con meno di 250 dipendenti, quando il trattamento :

- può presentare un **rischio** per i diritti e le libertà dell'interessato
- **non** è **occasionale**
- riguarda **categorie particolari di dati** o i dati personali relativi a **condanne penali e a reati.**

MA

Nella "*Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*" del 28 aprile 2017 il Garante ha <u>invitato</u> **tutti** i titolari e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi del registro.

# CONTENUTO DEL REGISTRO DEI TRATTAMENTI DEL TITOLARE (ART. 30, CO. 1)

Il registro del Titolare **contiene** le seguenti informazioni:

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

# CONTENUTO DEL REGISTRO DEI TRATTAMENTI DEL RESPONSABILE (ART. 3°, CO. 2)

Il registro del Responsabile **contiene** le seguenti informazioni:

- il **nome** e i **dati di contatto** del **Responsabile** o dei **Responsabili del trattamento**, di ogni **Titolare** del trattamento **per conto del quale agisce il responsabile del trattamento**, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

- le **categorie dei trattamenti** effettuati per conto di ogni titolare del trattamento;

- ove applicabile, i **trasferimenti** di dati personali verso un **paese terzo** o un'**organizzazione internazionale,** compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

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

# REGISTRO DEI TRATTAMENTI

| | | | | | Finalità del trattamento | |
|---|---|---|---|---|---|---|
| ID | Titolari del trattamento | Processo | Attività | Descrizione | Finalità generale | Finalità specifica |

| Dati personali | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Categorie di dati | | | | | | | | | | | | | | | | | | | | | | | | Termini di conservazione | | |
| Comuni | Categorie particolari | Categorie Particolari Dati che rivelino l'origine razziale o | Categorie Particolari Dati che rivelino | Categorie Particolari Dati che rivelino convinzioni | Categorie Particolari Dati che rivelino | Categorie Particolari Dati che rivelino | Categorie Particolari Dati genetici | Categorie Particolari Dati biometrici | Categorie Particolari Dati relativi alla | Categorie Particolari Dati relativi alla vita sessuale/orientam | Relativi a condanne penali e reati | Candidati | Dipendenti | Organi sociali | Fornitore / Dipendenti dei Fornitori / | Clienti e Prospect / Dipendenti dei Clienti | Visitatori / Utenti di servizi internet | MINORI | Altro | per Dati Comuni | per Categorie particolari | per Dati relativi a condanne penali e reati |

| Referente interno del trattamento | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Società | Funzione / Divisione | Ufficio | Nome e Cognome | Categorie di Soggetti Autorizzati al trattamento | Responsabili esterni del trattamento | Base giuridica | Raccolta del consenso | Modalità di raccolta del consenso (ove necessario) | |

| DESTINATARI | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Comunicazione | | | | | Trasferimento extra UE | | Modalità di trattamento | | |
| Persona fisica | Persona giuridica | Studi professionali | Autorità Pubblica | Altri organismi | Paese | Garanzia | Cartacea | Digitale | Applicativi |

# SANZIONI AMMINISTRATIVE GARANTE 2013-2015




**Fino a oggi le sanzioni sono state tendenzialmente contenute**

# SANZIONI (ART. 83)

Il Regolamento prevede la possibilità per le Autorità nazionali di irrogare **sanzioni fino a € 20.000.000** o, in caso di «*undertaking*», **al 4% del fatturato globale annuo**, a seconda di quale risulti la sanzione più elevata.

Le sanzioni più alte si applicano, inter alia, a:

- violazioni dei principi del trattamento, incluse le condizioni per il consenso;
- violazione dei diritti degli interessati;
- inosservanza delle norme in tema di trasferimento internazionale dei dati

Le sanzioni più basse (fino a €**. 10.000.000** o al **2%** del fatturato globale annuo) si applicano, fra l'altro, a

- violazione delle obbligazioni di controllers e processors, incluso gli obblighi di sicurezza e data breach notification.

Il concetto of ***'undertaking'*** potrebbe mettere a rischio le *revenues* di un gruppo societario, anche se non tutte le società del gruppo sono responsabili della violazione.
La sanzioni non sono infatti imposte in riferimento alle revenues della specifica società sanzionata, ma alle revenue di un "undertaking". Ciò, in estrema sintesi, potrebbe comportare che, se la società sanzionata è parte di un "undertaking", il 4% o 2% saranno calcolati sul fatturato totale annuo dell'intera undertaking e non il fatturato totale annuo della sola specifica società sanzionata.

# GRAZIE PER L'ATTENZIONE!

Avv. Francesca Lonardo
francesca.lonardo@p4i.it

Icons designed by {Prosymbols} {DinosoftLabs} {Freepik} from Flaticon