

LE NOVITÀ DEL GDPR E GLI IMPATTI PER LE AZIENDE



Francesca Lonardo

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

23 novembre 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**, **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.



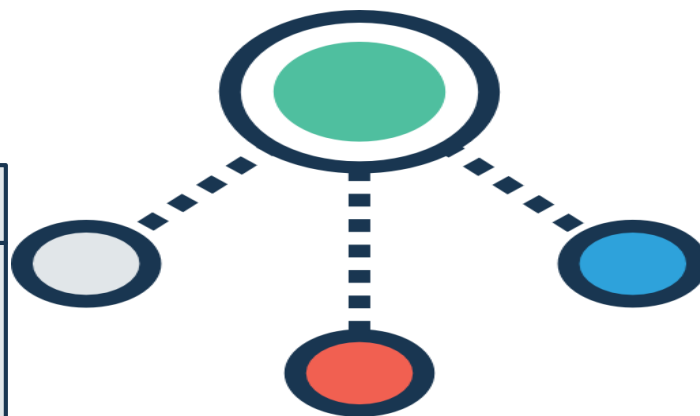
La nuova normativa europea in materia di tutela dei dati personali è un **REGOLAMENTO** e non più una Direttiva



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

COSA 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**



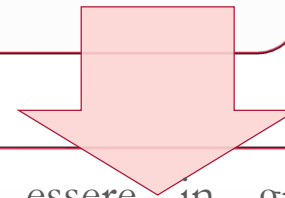
Viene introdotto un nuovo approccio metodologico, **risk-based**, basato sulla protezione dei dati dell'utente e sull'effettivo rischio per ogni azienda

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»

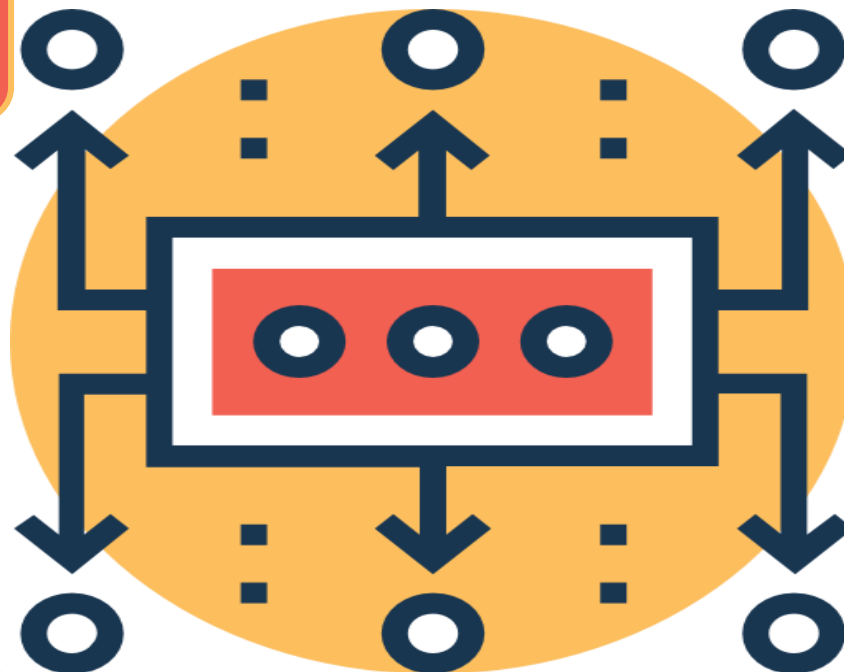
PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

P4I

liceità, correttezza
e trasparenza

limitazione della finalità

minimizzazione
dei dati



esattezza

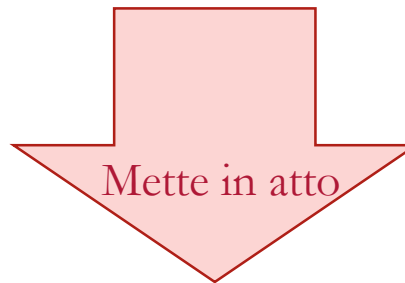
limitazione della
conservazione

integrità e
riservatezza

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

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).

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 adottate e adeguate politiche di informazione aziendale



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



6. Monitorare le misure ed aggiornare se necessario (audit interni o esterni)

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...

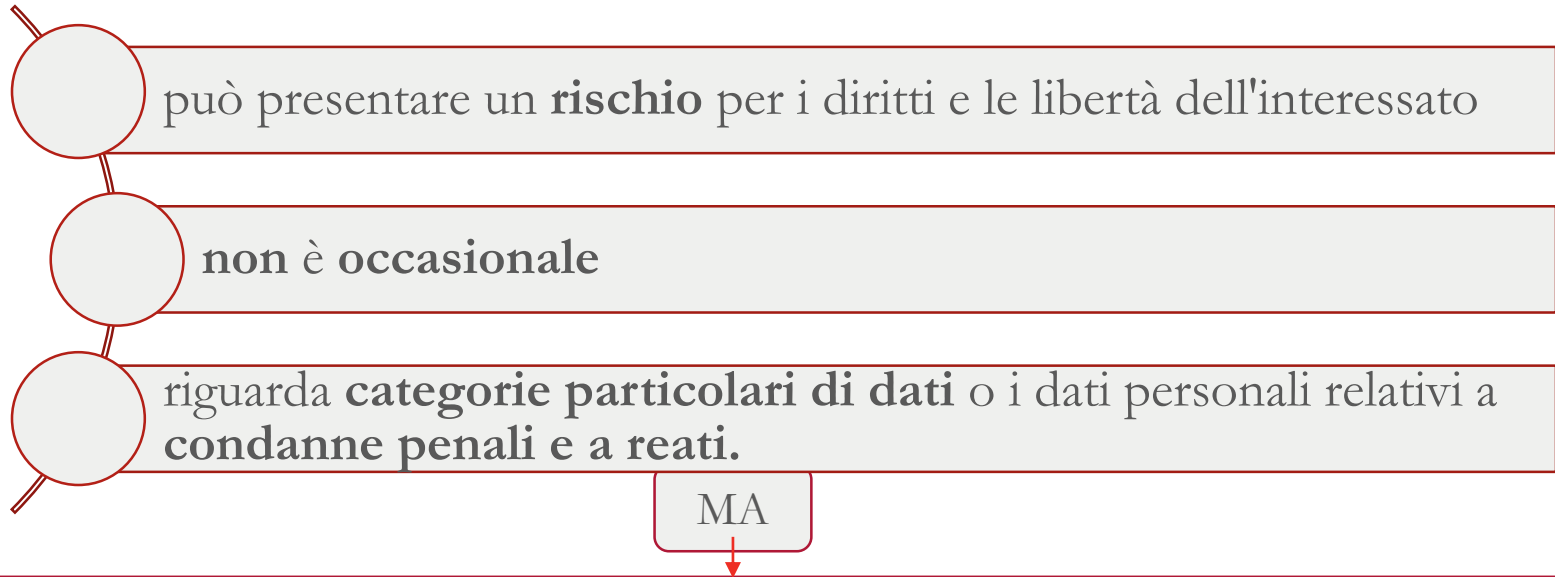
... tenuto conto di:

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 :



Nella “Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali” del 28 aprile 2017 il Garante ha invitato **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

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

Dati personali																					
Categorie di dati											Termini di conservazione										
Comuni	Categorie particolari	Categorie Particolari Dati che rivelano l'origine razziale o etnica	Categorie Particolari Dati che rivelano opinioni politiche	Categorie Particolari Dati che rivelano convinzioni religiose o filosofiche	Categorie Particolari Dati che rivelano appartenenza sindacale	Categorie Particolari Dati generali	Categorie Particolari Dati biometrici	Categorie Particolari Dati relativi alla salute	Categorie Particolari Dati relativi alla vita sessuale/orientamento sessuale	Relativi a condanne penali e reati	Candidati	Dipendenti	Organi sociali	Fornitore / Dipendenti del Fornitori / Consulenti	Clienci e Prospect / Dipendenti dei Clienti	Visitatori / Utenti di servizi internet	MINORI	Altro	per Dati Comuni	per Categorie particolari	per Dati i 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				

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



Fino a oggi le sanzioni sono state tendenzialmente contenute



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