LE RESPONSABILITÀ: LA GARANZIA DELLA SICUREZZA DEI DATI

Gabriele Faggioli
CEO Partners4innovation
Presidente Clusit
Adjunct Professor MIP-Politecnico di Milano

EVOLUZIONE NORMATIVA

Direttiva 95/46
l'Unione europea ha introdotto un sistema di regole volte a governare i trattamenti di dati personali.

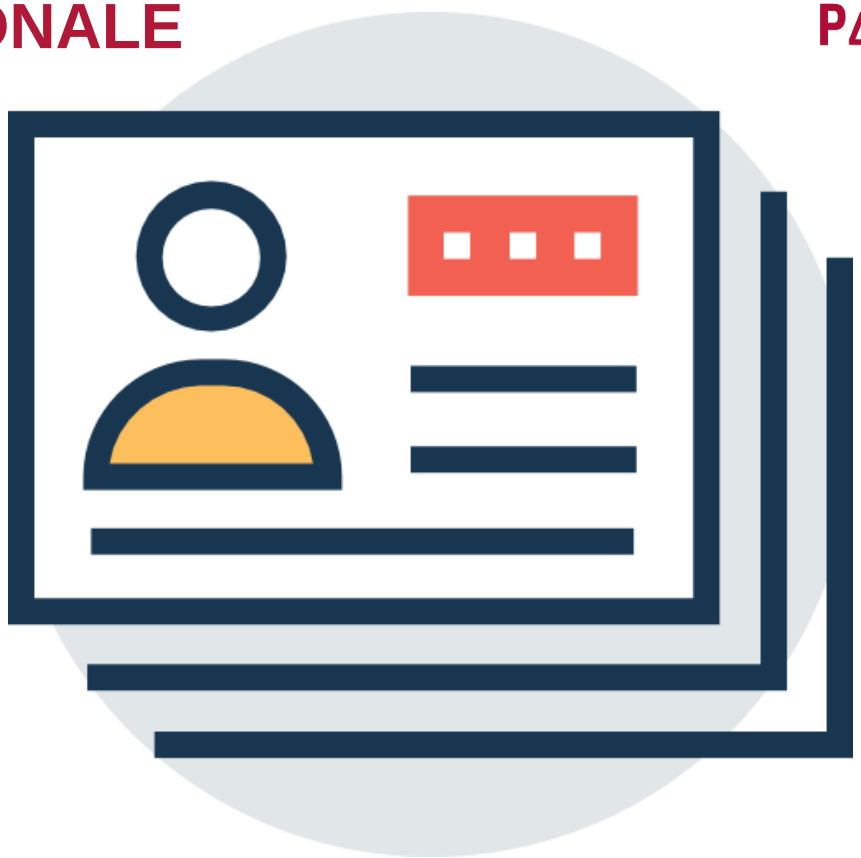
L. 675/1996
La Direttiva è stata recepita in Italia dalla Legge n. 675 del 1996, la prima legge sulla protezione dei dati personali a livello nazionale.

D.lgs. 196/2003
Il c.d. Codice Privacy ha abrogato la precedente legge in materia di protezione dei dati personali.

Il Regolamento europeo (c.d. GDPR)
è entrato in vigore il 24 maggio 2016 e diverrà direttamente applicabile in tutti gli stati dell'Unione europea a partire dal 25 maggio 2018.

DEFINIZIONI – DATO PERSONALE

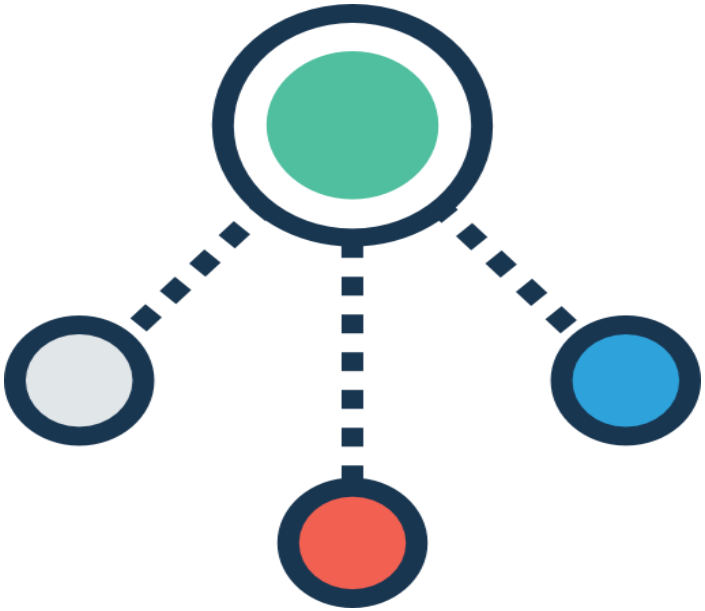
P4I



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».

CATEGORIE DI DATI PERSONALI



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
- (..)

PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

P4I

liceità, correttezza e trasparenza

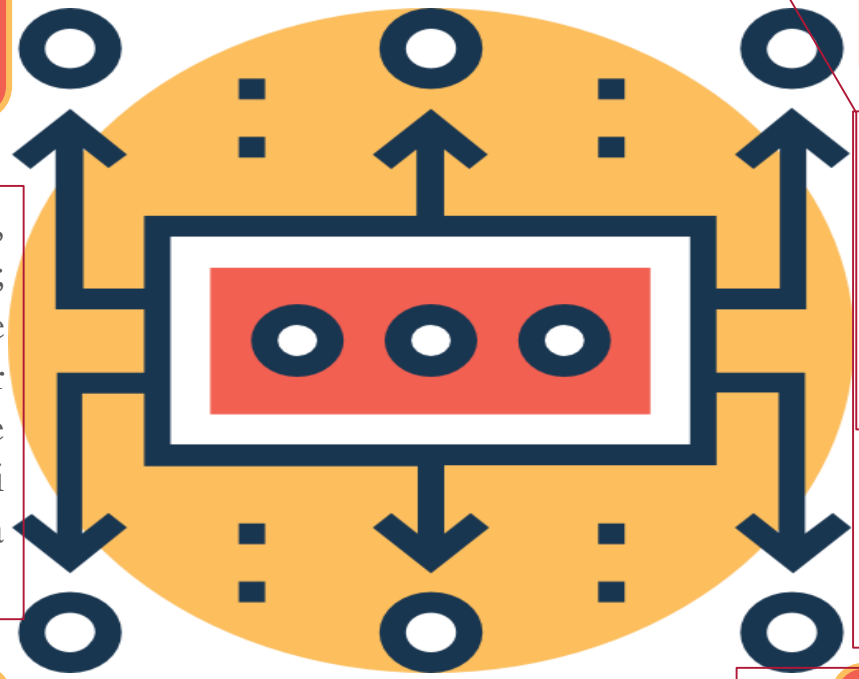
I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

limitazione della finalità

I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non limitati a quanto necessario, rispetto alle finalità per le quali sono trattati

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

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

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

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)

P4I

Il TITOLARE è responsabile per la *compliance* ai principi privacy e deve essere in grado di DIMOSTRARLA (art. 4, co.2)

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

Mette in atto

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.

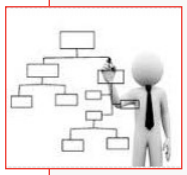
Ciò implica l'adozione di un SISTEMA DI GESTIONE DELLA DATA PROTECTION che consenta di gestire nel tempo la compliance (vedi slide successiva).

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; 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

OBBLIGHI IN CAPO AL TITOLARE

P4I

PRIVACY BY DESIGN

Realizzare qualsiasi progetto, servizio o sistema (sito web, software, soluzione IT, ambiente di lavoro, etc.) considerando la riservatezza e protezione dei dati personali sin dalla progettazione, utilizzando tecniche quali la minimizzazione e pseudonimizzazione

PRIVACY BY DEFAULT

Trattare di default solo i dati necessari («**minimizzazione**» dei dati già in fase di raccolta)

DATA PROTECTION IMPACT ASSESSMENT «DPIA»

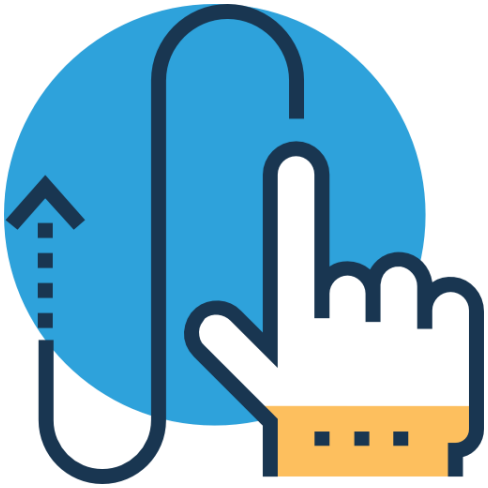
Effettuare una **valutazione (preliminare) d'impatto** sulla protezione dei dati nei casi in cui il trattamento, soprattutto se effettuato mediante nuove tecnologie, presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Sostituisce l'attuale notifica al Garante.

DATA BREACH

Notificare alle Autorità Garanti, senza ingiustificato ritardo (e, ove possibile, entro 72 ore) eventuali violazioni dei dati e comunicarle agli interessati laddove vi sia un rischio elevato per i diritti e le libertà delle persone fisiche.

RESPONSABILITÀ PER IL PROCESSOR (1/2)

Di regola la responsabilità per i danni derivanti dal trattamento è allocata in capo al Titolare (che decide finalità e mezzi del trattamento), in quanto il Responsabile svolge solo attività strumentali nei limiti dell'incarico che ha ricevuto e deve agire secondo le istruzioni del Titolare (e di impartirle ai propri collaboratori).



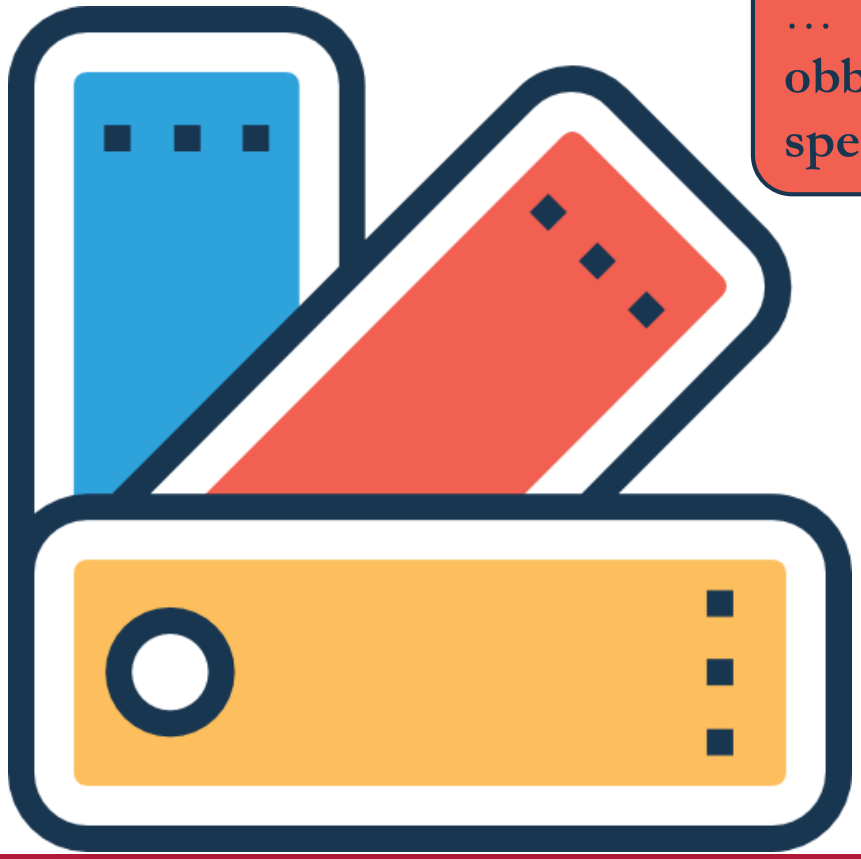
TUTTAVIA

Il GDPR prevede dei casi specifici, individuati dall'art. 82 co. 2, in cui il Responsabile è tenuto al risarcimento.

RESPONSABILITÀ PER IL PROCESSOR (2/2)

Il **responsabile** risponde non solo se **ha agito in modo difforme o contrario rispetto alle** legittime **istruzioni del titolare…**

… ma anche se **non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili**



RESPONSABILITÀ SOLIDALE

Qualora più titolari o responsabili oppure entrambi siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni **titolare** o **responsabile** è responsabile **in solido** per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato

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**

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

P4I

…che comprendono,
tra le altre, se del caso:

- **Pseudonimizzazione** → il trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti 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 tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **Cifratura** → la cifratura è una modalità di conversione del testo originale in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta chiave di decifratura potrà riconvertire nel file di testo originale
- **Capacità di**

1) **assicurare** la continua **riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi** che trattano i dati personali;
2) **ripristinare *tempestivamente*** la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

- **Procedura**

per **provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzativ**e al fine di garantire la sicurezza del trattamento

FOCUS SU MISURE DI SICUREZZA ADEGUATE (ART. 32)

P4I

- Dovrà essere predisposta una **metodologia di analisi dei rischi**

Dovranno essere individuate **adeguate contromisure** da adottare in funzione di tutti i parametri indicati nell'art. 32 (es. pseudonimizzazione)

IN PRATICA

- I **sistemi** dovranno essere predisposti **alla cancellazione dei dati** dopo il termine stabilito

- Dovranno essere predisposte procedure di **verifica periodica** delle **misure** adottate per assicurarne l'efficacia.

GRAZIE PER L'ATTENZIONE!

gabriele.faggioli@p4i.it

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