GDPR: ISTRUZIONI PER L'USO

CHE COS'E' ?

Il Regolamento Generale sulla Protezione dei Dati che entrerà in vigore tra tre mesi, il 25 Maggio 2018 riguarda tutti i paesi membri dell'Unione Europea e si occupa dei dati identificativi, sensibili e giudiziari relativi alle sole persone fisiche. In generale sono esclusi soltanto quei dati che riguardano società, enti e associazioni.

La differenza più significativa che introduce riguarda la reinterpretazione del concetto di privacy:

E' necessario implementare, **fin dalla fase progettuale**, procedure e tecniche che assicurino la sicurezza dei dati. Lo scopo è la tutela e la gestione del dato **fin dalla sua introduzione** nei sistemi aziendali.

Ogni azienda, in base alla tipologia di attività e di dati trattati, deve **calcolare il rischio** connesso alla loro gestione e implementare un sistema di tutela adeguato.

Il trattamento deve essere <u>monitorato nel tempo</u> e ritarato qualora le condizioni iniziali variassero. Questo nuovo tipo di approccio è basato sui principi di:

- **minimizzazione del dato** limitata ai soli dati necessari, esplicitando la finalità del trattamento;
- **limitazione della conservazione** al solo periodo di conservazione nei database aziendali indicato in maniera esplicita.

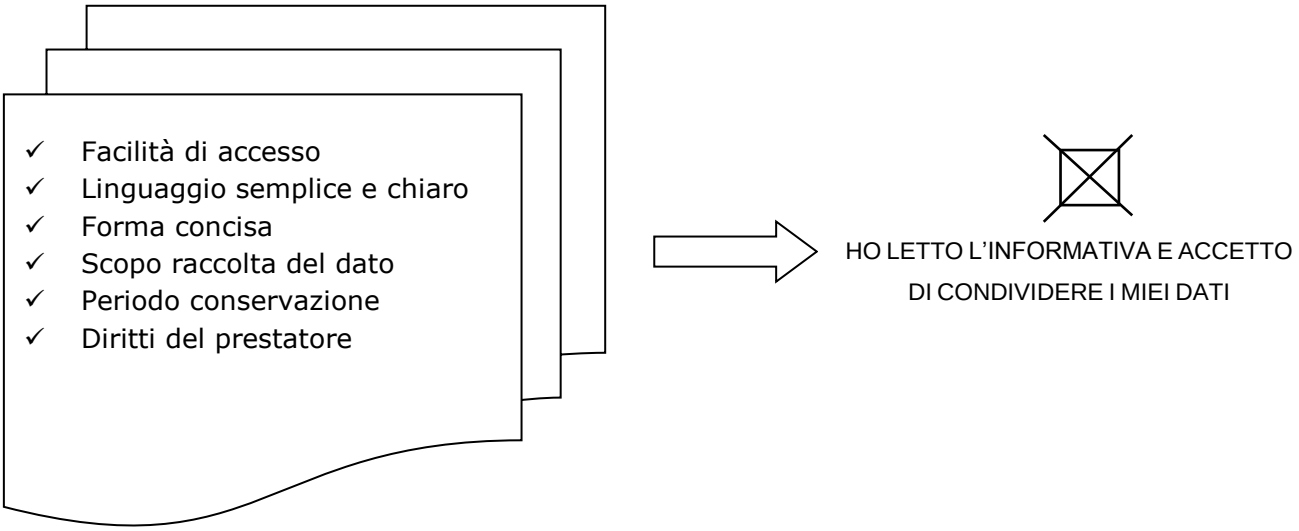
Al prestatore dovrà essere in futuro notificata la scadenza del periodo e l'eventuale richiesta di prolungamento.

COSA CAMBIA?

RACCOLTA E IMMAGAZZINAMENTO DEL DATO

La nuova normativa implica che il prestatore debba esprimere la volontà di condividere il dato attraverso **consenso consapevole** (non più consenso esplicito, nè silenzio assenso).

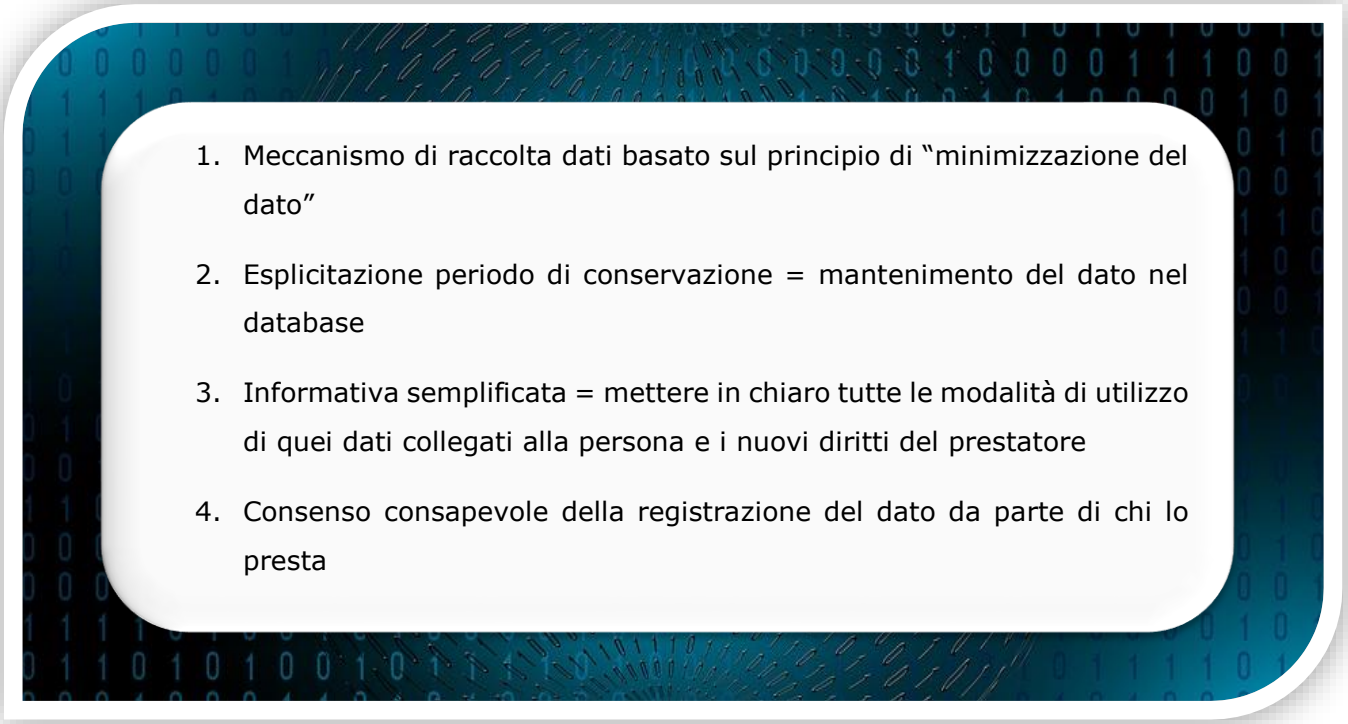
Sarà dunque necessario chiarire in modo semplice ed evidente le finalità di utilizzo e i passaggi relativi a come il dato viene trattato (**INFORMATIVA SEMPLIFICATA**), solo in questo modo il consenso potrà essere espresso in maniera consapevole (**AZIONE POSITIVA**).



ESEMPIO DI INFORMATIVA SEMPLIFICATA *ESEMPIO DI AZIONE POSITIVA*

Nel regolamento il consenso consapevole viene definito come "… *comportamento valido se frutto di un'azione compiuta e in maniera non equivoca"*

COSA FARE?



I DATI RACCOLTI FINO AD ORA

ANALISI

- Verifica di **consistenza** e **provenienza** del dato

PROGRAMMA DI PULIZIA

- Notificare al prestatore come verranno utilizzati da ora in poi i dati
- Richiesta di rinnovo del consenso

I dati raccolti prima dell'entrata in vigore del Regolamento non si potranno mantenere nei database senza questi aggiornamenti, pena l'imputabilità delle stesse sanzioni previste in caso di data breach.

ORGANIZZAZIONE INTERNA

- **Il management** va sensibilizzato sull' importanza strategica del dato come "fattore abilitante per il business" e come base del processo produttivo contemporaneo, poichè da esso dipende la BUSINESS CONTINUITY in quanto un Data Breach implica:

SANZIONI
generando rischi finanziari e reputazionali

BLOCCO ALL'ACCESSO DEI DATI
ossia interruzione dell'attività produttiva

- **Personale strettamente interessato e non:** studio dei flussi e delle "best practice" da implementare in base all'assessment iniziale e al ruolo specifico dell'interessato nel trattamento dei dati mappati

IL PRINCIPIO DI ACCOUNTABILITY

In caso di DATA BREACH il Garante della Privacy verificherà il principio di accountability adoperato dall'azienda, quindi **quanto è stato fatto per mettere i dati in sicurezza** e scongiurare la loro diffusione.

COME FARE?

AUTOVERIFICA PRELIMINARE

Gap analysis che evidenzia gli scostamenti dalla corretta applicazione della norma.

+

DATA PRIVACY IMPACT ASSESSMENT

Documento di valutazione d'impatto in caso di violazione del Regolamento.

Riguarderanno gli ASSET AZIENDALI di tipo **logico** (dati e software), **fisico** (dotazioni di strumenti, ambienti) e **organizzativo** (persone, procedure, norme)

PENA

Sanzioni previste in caso di Data Breach

MASSIME	MINIME
• Fino a 20.000 € per organizzazione singola • Fino al 4% del fatturato globale per organizzazioni facenti parte di un gruppo	• Scelta del garante della privacy dopo aver verificato l'entità del danno