Consiglio Nazionale delle Ricerche

I PRINCIPI ALLA BASE DEL NUOVO RGDP

Dott.ssa Sabina Ponzio
(CNR Ufficio Affari Istituzionali e Giuridici)

I principi alla base del nuovo RGDP

Regolamento generale per la protezione dei dati personali (2016/679)

Art. 1 del RGDP: "*Il presente regolamento protegge i diritti e le libertà fondamentali* ***delle persone fisiche****, in particolare il diritto alla protezione dei dati personali"*

Il principio cardine del nuovo regolamento è costituito dall'**autodeterminazione informativa**.

I principi alla base del nuovo RGDP

L'art. 5 del RGDP definisce i principi applicabili al trattamento dei dati personali:

- LICEITA', CORRETTEZZA E TRASPARENZA
- LIMITAZIONE DELLA FINALITA'
- LIMITAZIONE DELLA CONSERVAZIONE
- MINIMIZZAZIONE DEI DATI
- ESATTEZZA
- INTEGRITA' E RISERVATEZZA
- RESPONSABILIZZAZIONE

I principi alla base del nuovo RGDP

LICEITA', CORRETTEZZA E TRASPARENZA

ART.6 Il trattamento è LECITO solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità
- il trattamento è necessario **all'esecuzione di un contratto** di cui l'interessato è parte o **all'esecuzione di misure precontrattuali** adottate su richiesta dello stesso
- il trattamento è necessario **per adempiere un obbligo legale al quale è soggetto il titolare del trattamento**

I principi alla base del nuovo RGDP

- il trattamento è necessario **per la salvaguardia degli interessi vitali dell'interessato** o di un'altra persona fisica
- il trattamento è necessario **per l'esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
- il trattamento è necessario **per il perseguimento del legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un **minore.**

Tale condizione non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

LICEITA', CORRETTEZZA E TRASPARENZA

Il trattamento è CORRETTO solo se:

- rispetta norme etiche e deontologiche
- **lo scopo** del trattamento è determinato, esplicito e legittimo
- sono corrette **le modalità di raccolta** dei dati **e l'utilizzo dei dati**
- gli interessati sono **informati** delle finalità del trattamento che non deve essere occulto o segreto ma trasparente nei confronti degli interessati.

I principi alla base del nuovo RGDP

LICEITA', CORRETTEZZA E TRASPARENZA

Il trattamento è TRASPARENTE se:

- sono trasparenti le **modalità** con cui sono raccolti i dati personali
- è trasparente **l'utilizzo e la possibile consultazione** dei dati personali
- I dati personali sono **agevolmente accessibili** agli interessati
- sono facilmente **comprensibili le informazioni e comunicazioni** relative al trattamento
- **è aggiornata la documentazione attestante:** i trattamenti svolti, il rispetto dei diritti degli interessati, la ripartizione di ruoli e responsabilità e quella attestante le misure di sicurezza implementate.
- gli interessati vengono **informati sull'identità del Titolare** del trattamento e sulle **finalità del trattamento**.
- gli interessati vengono **sensibilizzati circa i rischi, le norme, le garanzie e i diritti relativi al trattamento dei dati personali.**

I principi alla base del nuovo RGDP

LIMITAZIONE DELLA FINALITA' DEI DATI

I dati devono essere **raccolti** per:

- *finalità determinate*
- *finalità esplicite*
- *finalità legittime*

Successivamente i dati devono essere **trattati** in una modalità che sia compatibile con tali finalità.

Il trattamento dei dati per finalità diverse da quelle per le quali sono stati inizialmente raccolti dovrebbe essere **consentito solo se compatibile con tali iniziali finalità.**

È poi possibile l'ulteriore trattamento ai fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici **art.89 paragrafo 1 del regolamento.**

LIMITAZIONE DELLA CONSERVAZIONE DEI DATI

I dati devono essere **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**; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente **all'art. 89 paragrafo 1 del regolamento**, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.

I principi alla base del nuovo RGDP

MINIMIZZAZIONE DEI DATI

I dati personali raccolti devono essere sempre:

- **adeguati**
- **pertinenti**
- **limitati** a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati.

Il principio è:

raccogliere meno dati possibili ma tutti quelli necessari.

I principi alla base del nuovo RGDP

ESATTEZZA DEI DATI

I dati devono essere sempre **esatti e aggiornati**.

Devono essere adottate tutte le misure ragionevoli per **cancellare o rettificare tempestivamente** eventuali inesattezze.

Il concetto di esattezza implica quindi il concetto di **aggiornamento nel tempo.**

I principi alla base del nuovo RGDP

INTEGRITA' E RISERVATEZZA DEI DATI

I dati devono essere sempre trattati in maniera da garantire una **sicurezza adeguata**, il che prevede l'adozione di **misure di sicurezza tecniche ed organizzative idonee (art. 32 del regolamento)** a proteggere i dati stessi da:

- *trattamenti non autorizzati o illeciti*
- *dalla loro perdita o distruzione*
- *dal danno accidentale*
- *dalla divulgazione non autorizzata.*

I principi alla base del nuovo RGDP

MISURE TECNICHE E ORGANIZZATIVE per garantire un livello di sicurezza adeguato al rischio:

- Pseudonimizzazione (art.4) e cifratura dei dati personali
- Resilienza dei sistemi e dei servizi informatici
- Capacità di ripristinare la disponibilità e l'accesso dei dati personali in caso di incidente (*Disaster Recovery*)
- Procedura per testare e valutare l'efficacia delle misure tecniche e organizzative
- etc….

RESPONSABILITA' DEL TITOLARE DEL TRATTAMENTO (ARTT. 5 e 25 RGDP)

- **ACCOUNTABILITY** (dover render conto del proprio operato) **art.5:**

considerando la **natura**, il **contesto** e le **finalità del trattamento** nonché dei **rischi** che, a seconda del trattamento in questione, possono gravare su diritti e libertà delle persone fisiche, il Titolare del trattamento deve **garantire ed essere in grado di dimostrare che il trattamento è stato effettuato conformemente al Regolamento stesso.**

Un **approccio *RISK BASED*** ha il vantaggio di pretendere degli obblighi che possono andare oltre la pura conformità alla legge, è **più flessibile** e **adattabile** al mutare delle esigenze e degli strumenti tecnologici, ma ha lo svantaggio di **delegare alla P.A. la valutazione del rischio**, rendendo più difficili le contestazioni in caso di violazioni.

I principi alla base del nuovo RGDP

Il **Titolare ha il compito di DECIDERE AUTONOMAMENTE le modalità, le garanzie e i limiti del trattamento dei dati personali.**

Il Titolare deve fare una **VALUTAZIONE di CONFORMITA'** "tenendo conto *dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei* ***rischi*** *aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento*" (**art. 25, par. 1**).

Il principio di responsabilizzazione richiede **un diverso approccio applicativo delle disposizioni del Regolamento**, "ribaltando" sui Titolari del trattamento un **obbligo di AUTOVALUTAZIONE** rispetto a:

- *trattamento effettuato*
- *tipologia dei dati personali trattati*
- *rischi derivanti dal trattamento*
- *adeguatezza delle misure tecniche e organizzative* ossia "***misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento***" (**art.25 par. 2**)

I principi alla base del nuovo RGDP

OBBLIGO DI DIMOSTRAZIONE DEL TITOLARE

Il principio di responsabilizzazione implica anche l'**obbligo di dimostrazione, gravante sul Titolare del trattamento, di aver rispettato i principi generali previsti al paragrafo 1 dell'articolo 5 e di aver adottato misure tecniche e organizzative adeguate.**

Pertanto, il Titolare deve acquisire **evidenze probatorie** finalizzate a comprovare che ha rispettato le disposizioni del Regolamento.

PRINCIPIO DI RESPONSABILIZZAZIONE

Il Regolamento fornisce **spunti operativi** ai fini dell'attuazione del principio di responsabilizzazione e della dimostrazione del rispetto del medesimo, come:

- **Adozione di Codici di condotta** (art. 40 consid. 77,81)
- **Istituzione di Sistemi di certificazione** (art. 42 consid. 81,100)
- **Registri delle attività di trattamento** (art. 30 consid. 82) obbligatori per le P.A.
- **Data Breach:** obbligo di comunicazione dell'avvenuta violazione dei dati personali (art. 34)
- **Data Protection Officer** (art. 37)

I principi alla base del nuovo RGDP

Fermo restando il **regime sanzionatorio**, la portata generale del principio di responsabilizzazione investe l'intera disciplina del Regolamento.

Altri 2 principi sono previsti dal Regolamento all'**art. 25:**

- **PRIVACY BY DESIGN** in base al quale **i prodotti e i servizi dovranno essere progettati fin dall'inizio in modo da tutelare la privacy degli utenti**, ossia il trattamento deve essere previsto e configurato fin dall'inizio prevedendo le garanzie per tutelare i diritti degli interessati.
- **PRIVACY BY DEFAULT** stabilisce che **per impostazione predefinita** le P.A. dovrebbero trattare **solo i dati personali necessari e sufficienti** per ogni specifica finalità del trattamento e **per il periodo strettamente necessario per tale finalità.**

I principi alla base del nuovo RGDP

Il **principio di privacy by default** statuisce che il Titolare debba attuare specifiche misure che garantiscano un idoneo trattamento dei dati, che deve esser **personalizzato, a seconda delle finalità e del tipo di operazioni da porre in essere.**

Tale obbligo varia a seconda della:

- quantità dei dati personali raccolti
- della portata del trattamento
- del periodo di conservazione
- dell'accessibilità.

La **minimizzazione** costituisce quindi una misura di riduzione del trattamento by default finalizzata a impostare a priori la massima protezione dei dati con il loro minimo trattamento, sia in fase di raccolta sia in fase di trattamento successivo all'acquisizione dei dati personali, secondo **i principi di necessità, pertinenza, adeguatezza e non eccedenza rispetto alle finalità.**

I principi alla base del nuovo RGDP

Per garantire il rispetto dei suddetti principi, il Titolare del trattamento è tenuto ad adottare:

- **politiche interne**
- **misure tecniche e organizzative adeguate**

con la finalità di assegnare agli addetti al trattamento dati un'idea di privacy c.d. "tecnologica".

In conclusione l'idea del Legislatore comunitario è di far adottare agli Stati strumenti per **progettare sistemi di raccolta dati e software** che, grazie all'uso della tecnologia, garantiscano il rispetto dei principi sanciti nel Regolamento.

GRAZIE PER L'ATTENZIONE!

Dott.ssa Sabina Ponzio
(CNR Ufficio Affari Istituzionali e Giuridici)