REGIONE DEL VENETO

giunta regionale

Direzione ICT e Agenda Digitale
Unità Organizzativa Strategia ICT e Agenda Digitale
P.O. Piani e programmi società dell'informazione

Nuovo Regolamento Europeo in materia di protezione dei dati personali

GDPR

(General Data Protection Regulation, Reg. 2016/679)

Le principali novità introdotte dal nuovo Regolamento Europeo in materia di Privacy sono le seguenti:

- Diritto alla cancellazione («diritto all'oblio») – Art. 17

- Diritto alla portabilità dei dati – Art. 20

- «Privacy by design» e «Privacy by default» – Art. 25

- Valutazione dei rischi del trattamento dei dati personali – Art. 35

- *Data breaches* – Artt.33 e 34

- «*Data Protection Officer*» – Art.37 e ss.

- Certificazione – Art. 42

- Sanzioni – Artt. 83 e 84

Considerazioni sulla nuova norma:

"Tecnologia" ---> Aspetto primario per la Privacy.

Competenze tecniche e giuridiche devono unirsi per assicurare riservatezza e protezione dei dati personali.

E' la prima volta che il "principio tecnologico" prevale sul "principio giuridico" nella stesura di una norma.

REGIONE DEL VENETO

giunta regionale

<u>IL 25 MAGGIO 2018</u> --> Sarà pienamente operativo il nuovo Regolamento UE in materia di Privacy

----> ***MENO di 2 ANNI DI TEMPO PER IMPLEMENTARE UN PIANO DI ADEGUAMENTO*** <-----

Fino alla mezzanotte del 24 maggio 2018, la normativa di riferimento rimarrà (in Italia) il "***Codice in materia di protezione dei dati personali"*** (comunemente noto come "***Codice della Privacy"***) emanato con il Decreto Legislativo 196/2003

---> IL NUOVO REGOLAMENTO UE SOSTITUIRA' LA DIRETTIVA 95/46/CE <---

---> A DIFFERENZA DELLA DIRETTIVA, **<u>IL NUOVO REGOLAMENTO SARA' LEGGE DIRETTAMENTE APPLICABILE IN OGNI STATO MEMBRO</u>** **E QUINDI <u>NON E' NECESSARIA UNA NORMA DI RECEPIMENTO</u>** <----

---> **LA PRIVACY** avrà finalmente **<u>REGOLE COMUNI IN TUTTI GLI STATI MEMBRI</u>** <---

PERCEZIONE ---> - IL 72% DEI CITTADINI EUROPEI RITIENE DI NON AVERE IL PIENO CONTROLLO DEI PROPRI DATI PERSONALI

OBIETTIVI ---> - PIU' GARANZIE E PIU' TUTELE PER LE PERSONE FISICHE; MAGGIORE TRASPARENZA SUI TRATTAMENTI E PIU' SICUREZZA DEI DATI PERSONALI;

IMPATTO ---> - ALCUNE NORME CONTENUTE NEL NUOVO REGOLAMENTO UE RENDERANNO PESANTI E ONEROSI GLI ADEMPIMENTI PER LE IMPRESE E GLI ENTI

Cambio di prospettiva rispetto al passato
ACCOUNTABILITY - Responsabilità e Rendicontazione

Il principio di **accountability** (che potrebbe essere tradotto in **"responsabilizzazione e obbligo di rendicontazione")** introdotto dal nuovo Regolamento UE, sancisce il passaggio da una concezione prettamente formale di mero adempimento ad un **approccio sostanziale di tutela dei dati e delle**

persone stesse ed è pertanto strettamente connesso con le misure di sicurezza e con l'analisi del rischio.
L'attuale Codice della Privacy prevede una serie di adempimenti formali (informativa, consenso, notificazione al Garante, misure minime e idonee) ma non un approccio di responsabilizzazione.

Un Registro obbligatorio delle attività di trattamento dati

Registro delle attività di trattamento di dati personali (art. 30), tenuto a cura del Titolare del trattamento, dovrà essere messo a disposizione dell'Autorità Garante qualora lo richieda, e dovrà contenere:

- 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;
- ove applicabile, i trasferimenti di dati personali verso paesi terzi e la loro identificazione; in taluni casi deve essere allegata la documentazione delle garanzie adeguate;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative.

Eccezioni:

Tali Registri **non sono obbligatori per i Titolari con meno di 250 dipendenti**, salvo che il trattamento non comprenda **dati sensibili**, o non sia presente **un rischio per i diritti e le libertà dell'interessato**.

Soggetti che effettuano il trattamento dei dati col nuovo Regolamento UE

<< Controller >>
E' il titolare del trattamento dei dati. **Ha potere decisionale sulle tecniche appropriate e sulle misure organizzative che assicurano che il trattamento dei dati sia compiuto in conformità con il regolamento**

<< Processor >>
E' il responsabile del trattamento dei dati nominato dal **<<Controller>>** (Titolare del trattamento). Le operazioni di trattamento del **<<Processor>> sono compiute soltanto su istruzioni documentate del Titolare**, definite da un contratto o altro atto giuridico

<< Data Protection Officer >> (DPO)
E' nominato dal Titolare del trattamento e **svolgerà la funzione di maggiore esperto nell'ambito del trattamento dei dati personali. Opera in piena indipendenza, assicura un allineamento dei processi di trattamento dei dati al Regolamento UE** e coopera con l'Autorita di controllo (Garante Privacy).

Garanzie per trasferimento dati personali al di fuori dell 'UE

Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati.

In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni (ad esempio per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).

Breve descrizione di alcune delle principali novità del Regolamento UE in materia di Privacy

Diritto alla cancellazione («diritto all'oblio») – Art. 17

L'interessato avrà il diritto di ottenere dal Titolare del trattamento (e quindi anche dai motori di ricerca, visto che la Corte UE li ha qualificati come autonomi titolari) **la cancellazione (anche on line) di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati** e di ottenere da terzi (che possono essere altri siti o utilizzatori dei dati o gli stessi motori) la cancellazione di qualsiasi link, copia o riproduzione di tali dati, se sussiste uno dei motivi seguenti:
a) se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti;
b) se l'interessato revoca il consenso su cui si fonda il trattamento o se il periodo di conservazione dei dati è scaduto e non sussistono altre motivazioni legittime per trattare i dati;
c) se l'interessato si oppone al trattamento di dati personali;
d) un tribunale o autorità di regolamentazione dell'Unione ha deliberato in maniera definitiva e assoluta che i dati devono essere cancellati;
e) se i dati sono trattati illecitamente;

Eccezioni (comma 3):
Il titolare del trattamento non dovrà dare seguito alla richiesta di cancellazione qualora tale uso sia stato lecitamente fatto:
a) per l'esercizio del diritto alla libertà di espressione e di informazione o del diritto alla difesa in sede giudiziaria;
b) a fini di archiviazione nel pubblico interesse (per es. salute pubblica);
c) quando i dati (resi anonimi) sono necessari per la ricerca storica o per finalità statistiche o scientifiche;

Diritto alla portabilità dei dati – Art. 20

Il Regolamento introduce il diritto alla **"portabilità"** dei propri dati personali per trasferirli da un titolare ad un altro.

Esempio:
Si potrà cambiare il provider di posta elettronica (gmail, libero ecc.) senza perdere i messaggi e i contatti salvati.

Eccezioni al diritto alla portabilità dei dati:
Non sarà consentito l'esercizio del diritto alla portabilità quando si tratta di dati contenuti in archivi di interesse pubblico (ad esempio le anagrafi dei comuni)

«Privacy by design» e «Privacy by default» – Art. 25

Il concetto di "***privacy by default"*** intende sottolineare la tutela della vita privata dei cittadini **"di default"** cioè come **impostazione predefinita.**

Per "***privacy by design"*** si intende la necessità di tutelare (riservatezza e protezione) il dato sin dalla progettazione dei sistemi informatici che ne prevedano l'utilizzo.

Esempio significativo: Social Network (Facebook, Twetter ecc.)

OGGI	DOMANI (REGOLAMENTO UE)
Un nuovo profilo in un social network, quando viene creato, è pubblico e come impostazione di default la maggior parte dei contenuti è visibile a tutti. Per proteggere i propri dati, limitando l'accesso agli stessi, l'interessato dovrà intervenire successivamente sulle impostazioni del proprio profilo per tutelare la propria privacy.	Un nuovo profilo in un social network, al momento della creazione, dovrà per default **(privacy by default)** contenere le limitazioni a tutela della vita privata dell'utente. L'interessato, qualora lo desideri, deciderà (intervenendo sulle impostazioni del proprio profilo) quali contenuti rendere visibili.

Valutazione dei rischi del trattamento dei dati personali – Art. 35

Se un trattamento di dati personali può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento (consultandosi con il Data Protection Officer) **dovrà effettuare, prima di procedere, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali** (DPIA, Data Protection Impact Assessment).

Data breaches – Artt.33 e 34

Il Titolare del trattamento **AVRA' L'OBBLIGO di comunicare eventuali violazioni dei dati personali** (***Data Breach conseguente per esempio ad attacco informatico***) all'autorità nazionale di protezione dei dati (per l'Italia il Garante per la protezione dei dati personali, noto come **Garante Privacy**).

Se l'indagine avviata dal Garante Privacy (per mezzo di ispezione condotta dalla Guardia di Finanza) evidenzia una minaccia per i diritti e le libertà delle persone, **verrà imposto al titolare del trattamento dei dati di informare in modo chiaro, semplice e immediato tutti gli interessati, indicando chiaramente come intende limitare le possibili conseguenze negative.**

Eccezioni all'obbligo di comunicazione del data breach agli interessati dal trattamento dati:
Se il titolare dimostra al Garante Privacy che:
a) la violazione non comporta un rischio per i diritti degli interessati (se non si tratta di frode, furto di identità ecc.)
b) ha adottato misure di sicurezza (cifratura dei dati) a tutela dei dati;
potrà essere esonerato dall'informazione agli interessati della violazione dei dati personali (data breach).
In ogni caso: Il Garante Privacy potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

«*Data Protection Officer*» – Art.37 e ss.

Il Regolamento UE introduce la nuova figura del **DPO "Data Protection Officer"** che dovrà essere nominata dal Titolare del trattamento e che svolgerà la funzione di maggiore esperto nell'ambito del trattamento dei dati personali.

- La nomina del **DPO** deve basarsi su **competenze professionali e su una approfondita conoscenza della materia del trattamento dei dati personali.**
- Il **DPO opera in piena indipendenza**;
- Fornisce informazioni e consigli al Titolare e al Responsabile del trattamento dei dati, **assicura un**

allineamento dei processi di trattamento dei dati al Regolamento UE e coopera con l'Autorita di controllo.

Sanzioni – Artt. 83 e 84

Le sanzioni **raggiungono degli ordini di grandezza mai immaginati prima**. Si può infatti arrivare a sanzioni amministrative pecuniarie **fino a 10.000.000 di Euro, o fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, in casi di violazione per esempio degli obblighi del titolare e del responsabile con riferimento alle condizioni applicabili al consenso dei minori; della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (privacy by design e privacy by default); delle misure di sicurezza; della valutazione d'impatto sulla protezione dei dati. O **addirittura si configurano sanzioni amministrative pecuniarie fino a 20.000.000 di Euro, o fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, in casi di violazioni per esempio dei principi di base del trattamento, comprese le condizioni relative al consenso; dei diritti degli interessati; dei presupposti del trasferimenti di dati personali a un destinatario in un paese extra europeo. **Sanzioni di questa entità potrebbero mettere in ginocchio un'azienda.**