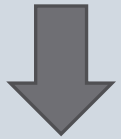
Il trattamento dei dati personali e il regolamento UE 679/16
Obdelava osebnih podatkov in Uredba (EU) 2016/679

AVV.MICHELE GRISAFI

GORIZIA- GORICA, 25 MAGGIO 2018

QUADRO NORMATIVO

DIRETTIVA EUROPEA 95/46/EC



“Legge sulla Privacy”(Legge 675/96)

“Codice in materia di Protezione dei Dati Personali”

(D.Lgs. n.196/2003)

QUADRO NORMATIVO

- Il **24 maggio 2016**, è entrato in vigore il cd. «General Data Protection Regulation» (GDPR), **Regolamento UE 2016/679**, che fornisce una disciplina unitaria in materia di privacy e protezione dei dati a livello UE
- Il GDPR si applicherà a decorrere dal **25 maggio del 2018**
- **Obbligatorio** e **direttamente applicabile** agli Stati membri

LE PRINCIPALI NOVITA’

- **Extraterritorialità**: la disciplina è obbligatoria per qualunque titolare svolga un trattamento di dati di residenti UE
- Ampliamento dei diritti dell’interessato:

-Diritto alla **portabilità dei dati**

-Diritto all’**oblio**

LE PRINCIPALI NOVITA’

- Accountability
- Privacy by design e Privacy by default
- Registro dei trattamenti
- Data Breach

LE PRINCIPALI NOVITA’

- Valutazione d’impatto Privacy (**Privacy Impact Assessment**)
- Data Protection Officer (**DPO**)
- Misure di sicurezza «**adeguate**»
- Sanzioni più severe

AMBITO DI APPLICAZIONE

- TRATTAMENTO DATI RELATIVI A **PERSONE FISICHE** CHE SI TROVANO NELL'UE; NO A PERSONE GIURIDICHE
- TRATTAMENTO **AUTOMATIZZATO DI DATI O NON AUTOMATIZZATO DI DATI** CONTENUTI IN UN ARCHIVIO O DESTINATI A FIGURARVI (INSIEME STRUTTURATO DI DATI)
- NO TRATTAMENTO DATI PER ATTIVITA' **PERSONALE/DOMESTICA**

I DATI «PARTICOLARI»

Codice Privacy:

DATI SENSIBILI

DATI GIUDIZIARI

DATI COMUNI

Regolamento UE:

DATI PARTICOLARI

- EX SENSIBILI

- GENETICI

- BIOMETRICI

DATI PENALI (CONDANNE, REATI, MISURE DI SICUREZZA)

I DATI «PARTICOLARI»

Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

IL «TRATTAMENTO»

«Trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

I SOGGETTI DEL TRATTAMENTO

- **TITOLARE**
- **RESPONSABILE**:PERSONA FISICA O GIURIDICA CHE TRATTA I DATI PER CONTO DEL TITOLARE DEL TRATTAMENTO
- **ART. 29**: CHIUNQUE ABBIA ACCESSO A DATI PERSONALI SOTTO L'AUTORITA' DIRETTA DEL TITOLARE O DEL RESPONSABILE (**EX INCARICATI** DEL TRATTAMENTO)

INFORMATIVA

- PERIODO DI CONSERVAZIONE DEI DATI PERSONALI
- DIRITTO DI REVOCA DEL CONSENSO
- DIRITTO DI PROPORRE RECLAMO AD AUTORITA' DI CONTROLLO
- PER TRATTAMENTI BASATI SUL LEGITTIMO INTERESSE, I LEGITTIMI INTERESSI PERSEGUITI
- DATI DI CONTATTO DEL DPO

IL CONSENSO

LIBERO, SPECIFICO, INFORMATO;

«INEQUIVOCABILE» QUALE DICHIARAZIONE O AZIONE POSITIVA

Es. selezionando un’apposita casella in un sito internet o con altra dichiarazione o comportamento che indichi chiaramente in questo contesto che si accetta il trattamento proposto.

NO FORMA SCRITTA PER SUA VALIDITA’- **ONERE DELLA PROVA A CARICO TITOLARE**

REGISTRO DEI TRATTAMENTI

Esentati enti, imprese e altri organismi con meno di 250 dipendenti.

L'esenzione non opera per qualunque **titolare con un numero di dipendenti inferiore a 250** che effettui un **trattamento che può presentare un rischio per i diritti e le libertà** degli interessati ed al contempo, alternativamente:

- il trattamento non sia occasionale;

- per quanto occasionale, **il trattamento includa** i dati «particolari» cioè **dati 'sensibili', biometrici, genetici e/o 'giudiziari'**.

REGISTRO DEI TRATTAMENTI

NOME E DATI DI CONTATTO TITOLARE E RESPONSABILE

FINALITA' DEL TRATTAMENTO

LE CATEGORIE DEI DATI E DEGLI **INTERESSATI**

LE CATEGORIE DEI DESTINATARI A CUI SARANNO COMUNICATI DATI

I **TERMINI ULTIMI PER LA CANCELLAZIONE** DELLE DIVERSE CATEGORIE DEI DATI

DESCRIZIONE GENERALE DELLE **MISURE TECNICHE ED ORGANIZZATIVE**

VALUTAZIONE D'IMPATTO «DPIA»

Art. 35: «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, **può presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una **valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali»**.

VALUTAZIONE D'IMPATTO «DPIA»

E' richiesta in particolare nei casi seguenti:

a) una **valutazione sistematica** e globale di aspetti personali relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la **profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il **trattamento, su larga scala, di categorie particolari di dati** personali;

c) la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico.**

DATA BREACH

VIOLAZIONE DEI DATI: PERDITA, DISTRUZIONE, DIFFUSIONE INDEBITA DI DATI PERSONALI

- **OBBLIGO DI NOTIFICAZIONE ALL'AUTORITA' GARANTE** ENTRO 72 ORE

- IN CASO DI RISCHIO ELEVATO PER I DIRITTI E LE LIBERTA' DELLE PERSONE (FRODE, FURTO DI IDENTITA', DANNI D'IMMAGINE, ETC.), **OBBLIGO DI COMUNICAZIONE ALL'INTERESSATO**

DESCRIZIONE DELLE PROBABILI CONSEGUENZE E DELLE MISURE ADOTTATE PER PORRE RIMEDIO

MISURE DI SICUREZZA «ADEGUATE»

ELIMINATA DISTINZIONE TRA MISURE MINIME OBBLIGATORIE E MISURE IDONEE

MISURE TECNICHE E ORGANIZZATIVE «ADEGUATE» PER GARANTIRE UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO

PARAMETRI:

-stato dell'arte

-natura, oggetto, finalità e contesto del trattamento

-probabilità e gravità rischi

-bilanciamento costi/rischi

RESPONSABILITA’

CIVILE

PENALE (?)

AMMINISTRATIVA

Le sanzioni pecuniarie possono arrivare fino a 20 milioni di Euro oppure fino al 4% del fatturato mondiale totale annuo

CRITERI DI VALUTAZIONE

la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b) il carattere doloso o colposo della violazione;
c) le misure adottate per attenuare il danno subito dagli interessati;
d) il grado di responsabilità tenendo conto delle misure tecniche e organizzative da essi messe in atto;
e) eventuali precedenti violazioni;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione

ADEMPIMENTI

- Censimento dei dati e Mappatura dei trattamenti
- Registro dei Trattamenti
- Modificare informative e moduli del consenso
- Redigere contratti con i Responsabili del Trattamento

ADEMPIMENTI

- Analizzare i rischi e adottare misure adeguate di sicurezza, tecniche ed organizzative
- Adottare un piano formativo del personale
- Adottare procedure per garantire l’esercizio dei diritti degli interessati
- Adottare procedure per il Data Breach

ADEMPIMENTI

- Privacy by Design
- Privacy by Default
- DPIA
- Aggiornamento continuo
- Sistema di gestione Privacy

...e grazie per l'attenzione!