TORTORETO
ASSOCIAZIONE ALBERGATORI

NUOVO REGOLAMENTO sul Trattamento dei Dati Personali

PRIVACY COSA CAMBIA CON IL NUOVO REGOLAMENTO EUROPEO

- E' stato pubblicato il 4 maggio 2016 nella Gazzetta Ufficiale dell'Unione Europea il **Regolamento UE 2016/679** relativo alla protezione dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- Come prevede l'art. 99 il Regolamento entrerà in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale (25 maggio 2016), ma si applicherà a decorrere dal 25 maggio 2018.

PRIVACY COSA CAMBIA CON IL NUOVO REGOLAMENTO EUROPEO

- Ma perché un Regolamento Europeo?
- La tecnologia attuale consente alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività e, sempre più spesso, gli stessi privati rendono pubbliche sulla rete mondiale informazioni personali che li riguardano.
- Le nuove tecnologie non hanno trasformato solo l'economia, ma anche le relazioni sociali.

Privacy?

- A chi si applica?
- Tutte le aziende che sono in regola oggi lo saranno anche domani?
- Se inizio il trattamento oggi a quale normativa devo far riferimento?

Privacy?

A chi si applica?

A tutte le aziende che trattano dei dati personali.

TORTORETO
ASSOCIAZIONE ALBERGATORI

Privacy?

Tutte le aziende che sono in regola oggi lo saranno anche domani?

- Non è detto perché nuove modalità, nuove cogenze sono entrate con il nuovo Regolamento UE.

TORTORETO
ASSOCIAZIONE ALBERGATORI

Privacy?

Se inizio il trattamento oggi a quale normativa devo far riferimento?

- Ad oggi si deve fare riferimento alla 196/03, dal 25 maggio 2018 al Regolamento UE.

Gli adempimenti obbligatori del GDPR saranno attivi dal 25 maggio 2018

(Art 95 abroga la direttiva 95/46/CE entra il vigore il 24 maggio 2016 e si applica a decorrere dal 25 maggio 2018)

COSA CAMBIA

Oggetto e finalità
STESSA RATIO

Codice Privacy

Chiunque ha il diritto alla protezione dei dati che lo riguardano a fronte di una finalità che deve essere garantita minimale e delle libertà fondamentali durante il trattamento dei dati personali.

Regolamento UE

Il regolamento protegge i diritti e le libertà fondamentali **delle persone fisiche**, in particolare il diritto alla protezione dei dati.

La libera circolazione dei dati in UE non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

PROTAGONISTI DELLA PRIVACY

- **L'INTERESSATO**

è il PROPRIETARIO dei dati (diritti sanciti dal GDPR)

- **STRUTTURA AZIENDALE**

TITOLARE, RESPOSANBILE E INCARICATO-ADDETTI AL TRATTAMENTO (ART 28 C. 3 lett b-29-32) ci saranno dei responsabili che per conto del titolare in maniera autonomia nelle modalità e nei mezzi trattano i dati degli interessati.

PROTAGONISTI DELLA PRIVACY

- **DPO**

Il Regolamento ha introdotto la figura del **Responsabile della Protezione dei Dati Personali** (detto **DPO**).

Si tratta di un soggetto in possesso di specifici requisiti come competenza, esperienza, indipendenza, autonomia di risorse, con il compito di garantire la **tutela della privacy** attraverso la verifica della corretta applicazione del Regolamento, la formazione del personale, la sensibilizzazione, la consulenza ecc

DATI PERSONALI (Art. 4, comma 1 n1)

CAMBIANO SOLO I TERMINI

Codice Privacy (196/03)

I dati personali si distinguevano in 3 tipi:

- **Dati identificativi**
- **Dati sensibili** (art. 4 comma 1 lettera d) - **giudiziari** (art. 4 comma 1 lettera e),
- **Dati anonimi** (cioè il dato che in origine o a seguito del trattamento, non può essere associato ad un interessato identificato o identificabile).

Regolamento UE (679/2016)

Per il regolamento UE la distinzione è cambiata:

- **Dati PERSONALI** (art. 4 comma 1 nr1)
- **Dati GENETICI** (art. 4 comma 1 nr13) non più dati sensibili generali ma
- **Dati BIOMETRICI** (art. 4 comma 1 nr 14)
- **Dati relativi allo STATO DI SALUTE** (art. 4 comma 1 nr15)
- rimangono i **Dati GIUDIZIARI** come nella 196

PRINCIPI GENERALI

- Liceità - correttezza - trasparenza
- Limitazioni delle finalità
- Minimizzazione dei dati (principio di necessità)
- Esattezza
- Limitazione della conservazione (limiti temporali)
- Integrità e riservatezza

I Principi del Regolamento sono gli stessi della 196

Principio di liceità e correttezza

ovvero posso trattare il dato solo se lo tratto in modo corretto e solo se è lecito poterlo trattare

I Principi del Regolamento sono gli stessi della 196

Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano facilmente accessibili e di facile comprensione e che sia utilizzato un linguaggio semplice e chiaro.

Ciò riguarda in particolare l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento

I Principi del Regolamento sono gli stessi della 196

Principio delle limitazione delle finalità

ovvero posso trattare le informazioni a fronte di finalità obbligatorie per legge o a fronte di finalità per cui l'interessato ha dato il consenso

I Principi del Regolamento sono gli stessi della 196

Principio della minimizzazione dei dati

ovvero posso trattare i dati nella loro situazione o condizione minima (solo dati necessari).

Principio di esattezza

ovvero i dati che tratto devono essere il più possibile esatti

I Principi del Regolamento sono gli stessi della 196

Principio di integrità e riservatezza

ovvero il dato può essere trattato solo dalle persone autorizzate a trattarlo al fine di preservarne e garantirne l'integrità

Principio della limitazione della conservazione (Nuovo)

ovvero non possiamo trattare i dati per sempre ma le aziende dovranno indicare per quanto tempo vogliono trattare le informazioni delle persone ed informare l'interessato sulla limitazione temporale.

NUOVO Principio
Il principio di Accountability

Il Regolamento promuove la responsabilizzazione (*accountability*) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

DOMANDA

Quando io azienda posso trattare i dati personali?

Posso trattare i dati personali solo quando l'interessato mi ha dato il **consenso** al trattamento in base alle finalità dichiarate o quando il **trattamento è necessario** (es. stipula il contratto) o quando il **trattamento è obbligatorio** per adempiere ad un obbligo di legge o la salvaguardia di interessi vitali.

GLI ADEMPIMENTI

- Cosa dobbiamo fare ???

La prima cosa da fare è fornire una informativa e se necessario recuperarne un consenso.

- **INFORMATIVA** all'interessato (Artt. 13-14)
- **CONSENSO** dell'interessato (Artt. 6-7)

CONSENSO

Quando si parla di consenso, qualora il trattamento sia basato sul consenso ai sensi dell'art. 7 il Titolare del trattamento **deve essere** in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Diritto di REVOCA

- Diritto di revoca del consenso: in qualunque momento l'interessato ha il diritto di revocare un consenso qualora il consenso non sia obbligatorio per legge o per la gestione di un contratto.

TORTORETO
ASSOCIAZIONE ALBERGATORI

Per le INFORMAZIONI raccolte presso l'interessato dobbiamo fornire **L'INFORMATIVA**

INFORMATIVA (Art. 13 e succ.)

- Le **INFORMAZIONI DA FORNIRE**, qualora i dati siano raccolti presso l'interessato (ART13)
- Identità Titolare
- Finalità e base giuridica
- Soggetti a cui vengono comunicati i dati (categorie destinatari) ed il riferimento delle garanzie
- Periodo di conservazione (quanto tempo noi andremo a mantenere le informazioni relative al consenso)
- L'esistenza del diritto di revoca se basato sul consenso, il diritto di proporre reclamo ad una Autorità di Controllo
- Se la comunicazione dei dati è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto
- Esistenza processo automatizzato di profilazione, logiche e conseguenze
- Verifica necessità adeguamento informative

INFORMATIVA (Art. 14.)

INFORMAZIONI DA FORNIRE qualora i dati non siano stati ottenuti presso l'interessato (ART. 14)

- Tutto quanto previsto dall'art. 13
- La fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che provengano da fonti accessibili al pubblico o banche dati
- Se le informazioni sono recuperate non direttamente dall'interessato, dobbiamo fornire le informazioni entro un termine ragionevole e comunque entro 1 mese dall'ottenimento dei dati personali. Se i dati sono destinati alla comunicazione, al più tardi entro la prima comunicazione (con l'interessato o con l'altro destinatario). Nell'informativa va indicato: dove sono stati presi i dati, come verranno utilizzate queste informazioni di cui in possesso, con quali finalità, come sono conservate, per quanto tempo verranno conservate, se sono gestite sul territorio italiano piuttosto che europeo

INFORMATIVA (Art. 14)

L’informativa è il primo obbligo ed è il biglietto da visita su come trattiamo i dati dell’interessato.

NOVITA' GDRP

- Informative più chiare (art. 13-14)
- Consenso NON equivoco (espresso per ogni finalità differenti)
- Diritto alla cancellazione (diritto all'oblio)
- Diritto alla portabilità dei dati

PORTABILITA' DEI DATI (ART 20)

L'interessato ha il diritto di ricevere in un formato elettronico strutturato, di uso comune e leggibile (non criptato) tutti i dati personali che lo riguardano forniti ad un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento a cui li ha forniti.

NOVITA' GDRP

- Registro dei trattamenti
- Valutazione dei rischi
- Concetti di privacy by design, by defaul e security by design
- Figura del responsabile della protezione dei dati (DPO)
- Data Breach (deve essere comunicata all'interessato)

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (ART. 30)

Non obbligo per tutti

NON SI APPLICA SE SI TRATTA DI IMPRESE CON MENO DI 250 DIPENDENTI

però il regolamento dice:

- A meno che non vi siano rischi per i diritti e le libertà delle persone, il trattamento non sia occasionale o includa **dati sensibili e giudiziari**.
- Quindi si evince che, tutte le aziende che hanno dipendenti devono avere il registro del trattamento (dati sensibili).

La tenuta del registro è un obbligo del Titolare del trattamento e deve contenere quanto riportato nell'art. 30

Valutazione dei Rischi

Identificare	IDENTIFICARE I RISCHI
Valutare	In corrispondenza di ogni rischio dobbiamo attribuire una valutazione di probabilità e gravità.
Pianificare	Le relative risposte nei tempi prestabiliti
Implementare	Step finale: l'organizzazione realizza tutte le risposte individuate

1° STEP da implementare (art. 25)

Il titolare prima di fare qualsiasi trattamento deve verificare che il trattamento abbia un rischio basso, quindi la prima cosa che dovrà fare è

la MAPPATURA di tutti i trattamenti

Dopo aver mappato tutti i trattamenti deve predisporre

una ANALISI DEI RISCHI

per verificare che il rischio sia basso e quindi si possa effettuare il determinato trattamento.

Privacy by design è la prima attività che tutte le aziende devono fare.

2° STEP da implementare (art. 30)

L'analisi viene confrontata con il registro dei trattamenti

- Dobbiamo avere un elenco di tutti i trattamenti
- Il registro è obbligatorio per aziende con più 250 dipendenti oppure per aziende che hanno meno di 250 dipendenti che però fanno trattamenti a rischi. Quali sono i trattamenti a rischio? I trattamenti a rischio sono quelli ad esempio che gestiscono i dati particolari. Quali sono i dati particolari? I dati particolari sono ad esempio i dati sulla salute. Le aziende che gestiscono i dati dei dipendenti (buste paghe) devono avere il registro dei trattamenti.

3° STEP da implementare

Su tutti i trattamenti dobbiamo fare **una VALUTAZIONE dei rischi**.
Ci sono **5 rischi fondamentali** da gestire:

-Rischio di cancellazione di un dato quando un dato non deve essere cancellato

-Rischio di modifica di un dato quando un dato non deve essere modificato

-Rischio di visualizzazione di un dato da parte di chi non aveva l'autorizzazione a poteva visualizzare

-Rischi di perdita di un dato che non poteva essere perso

-Rischio comunicazione e diffusione per un dato che non poteva essere comunicato o diffuso

Esempio Rischio di incendio non è un rischio sui dati personali è un rischio che ricade sul dato.

4° STEP da implementare

Identificazione dei soggetti che intervengono nel trattamento

Titolare, co-titolare, Responsabili (esterni, interni se del caso), Nomine/atti giuridicamente vincolanti, Incaricati, Data Protection Officer (DPO)

5° STEP da implementare

FORMAZIONE CONTINUA

AUDIT INTERNI

Art. 32 Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento

6° STEP da implementare

Importante è anche **rivedere la modulistica**, che, se non in linea con le modifiche previste dalla nuova normativa, potrebbe causare sanzioni.

INFORMATIVE - CONSENSI

7° STEP da implementare

In sintesi, bisogna dotarsi di una struttura adeguata (Manuale e procedure), anche per gestire correttamente i **diritti degli utenti**, che potranno:

- ottenere la cancellazione dei dati, ovvero ritirare il consenso (**diritto all'oblio**)
- richiedere, e ricevere, i dati concessi a un titolare, per trasferirli a un altro (**diritto alla portabilità dei dati**)

7° STEP da implementare

- Inoltre, per il **diritto di accesso**, occorre essere completamente trasparente riguardo la raccolta e l'utilizzo dei dati ed essere in grado di notificare agli utenti eventuali **violazioni dei dati**.

DATA BREACH: le violazioni dei dati, per esempio in caso di attacchi informatici o furti.

La norma introduce infatti il diritto per tutti i cittadini, siano essi aziende o persone fisiche, di conoscere la violazione dei dati che le aziende saranno obbligate a comunicare al Garante.

TORTORETO
ASSOCIAZIONE ALBERGATORI

Grazie per l'attenzione