Privacy

Il nuovo Regolamento Europeo 679/2016

Seminario informativo
Estratto materiale

Welcome

Privacy

Il nuovo Regolamento Europeo 679/2016

Avv. Valeria Tocchio
Avvocato – Patrocinante in Cassazione
Consulente di imprese pubbliche e private -Mediatore civile
Curatore fallimentare – Commissario e liquidatore giudiziale
- Docente a contratto diritto civile S.S.P.L.E L. Migliorini Università degli Studi di Perugia
Master in Prvacy officer e consulenza della privacy

L

IL NUOVO REGOLAMENTO EUROPEO 679/2016

Welcome

- DOPO OLTRE UN VENTENNIO VIENE ABROGATA LA DIRETTIVA MADRE N. 95/46/CE E IL **25 MAGGIO 2018** INIZIA UFFICIALMENTE L'ERA DEL GDPR **GENERAL DATA PROTECTOR REGULATION**

- 99 ARTICOLI E 173 CONSIDERANDO
- **QUADRO COMUNE** IN MATERIA DI TUTELA DEI DATI PERSONALI PER TUTTI GLI STATI MEMBRI

- **LA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI DI CARATTERE PERSONALE È UN DIRITTO FONDAMENTALE.**

- **A PRESCINDERE DALLA LORO NAZIONALITÀ O DALLA LORO RESIDENZA**

IL NUOVO REGOLAMENTO EUROPEO 679/2016

Welcome

- **OBIETTIVO COMUNE** UNIFORMARE E ARMONIZZARE LE BARRIERE CREATE DALLE DIFFERENTI NORMATIVE NAZIONALI
- (N..B. RESTANO TUTTAVIA LE PLURALITÀ DI FONTI)

- **A BENEFICIO** - DEL **MERCATO UNICO DIGITALE** CHE SECONDO LA COMMISSIONE UE HA UN POTENZIALE DI 415 MILIARDI DI EURO ANNUI - DELLE IMPRESE EUROPEE ALLE QUALI VIENE RESTITUITA **COMPETITIVITÀ**

I PRINCIPI DEL REGOLAMENTO

CORRETTEZZA
LICEITA'
LEGITTIMITA'
FINALITA'
MINIMIZZAIZONE
CONSERVAZIONE LIMITATA
PERTINENZA
INTEGRITA'
RISERVATEZZA
RESPONSABILIZZAZIONE DEL TITOLARE DEL TRATTAMENTO

PRINCIPI DEL REGOLAMENTO

LICEITA'
OGNI TRATTAMENTO DEVE TROVARECONFERMA IN UNA SUA BASE GIURIDICA

PRESUPPOSTI DI LICEITA':
CONSENSO
CONTRATTO
OBBLIGO LEGALE
SALVAGUARDIA INTERESSI VITALI
COMPITI DI INTERESSE PUBBLICO
LEGITTIMO INTERESSE DEL TITOLARE

PRINCIPI DEL REGOLAMENTO

LICEITA'

CONSENSO ESPLICITO:
PER I DATI SENSIBILI
PER I TRATTAMENTI AUTOMATIZZATI

LA FORMA SCRITTA NON RICHIESTA
MA PROVA LA INEQUIVOCABILITA'

CONSENSO

INTENZIONE LIBERA, SPECIFICA, INFORMATA E INEQUIVOCABILE DI ACCETTARE IL TRATTAMENTO DEI DATI PERSONALI

Es. DICHIARAZIONE SCRITTA,

ATTRAVERSO MEZZI ELETTRONICI,

O ORALE.

SELEZIONE DI UN'APPOSITA CASELLA IN UN SITO

INDICHI CHIARAMENTE IN TALE CONTESTO CHE L'INTERESSATO ACCETTA IL TRATTAMENTO PROPOSTO.

.

NOVITA' : IL CONSENSO DEL MINORE

Per offerta diretta di servizi della società dell'informazione

N..B. Al di sotto dei 16 anni o in età inferiore, ma non sotto i 13

è lecito

se vi è consenso della potestà genitoriale

I DIRITTI DEGLI INTERESSATI

TRASPARENZA

I DIRITTI DEGLI INTERESSATI

INFORMATIVA

FORMA CONCISA

INTELLEGIBILE

TRASPARENTE

FACILMENTE ACCESSSIBILE
UTILIZZO DI ICONE IN COMBINAZIONE

I DIRITTI DEGLI INTERESSATI

DIRITTO DI ACCESSO GARANTITO,

I DIRITTI DEGLI INTERESSATI

DIRITTO DI OTTENERE LA RETTIFICA L'INTEGRAZIONE DEI DATI INCOMPLETI AGGIORNAMENTO

I DIRITTI DEGLI INTERESSATI

OBLIO

IL DIRITTO DI CHIEDERE CHE SIANO CANCELLATI E NON PIÙ SOTTOPOSTI A TRATTAMENTO I PROPRI DATI PERSONALI

NON PIÙ NECESSARI PER LE FINALITÀ PER LE QUALI SONO STATI RACCOLTI

O ALTRIMENTI TRATTATI,

QUANDO ABBIA RITIRATO IL PROPRIO CONSENSO

O SI SIA OPPOSTO AL TRATTAMENTO DEI DATI PERSONALI

O QUANDO IL TRATTAMENTO DEI DATI PERSONALI NON SIA CONFORME AL REGOLAMENTO.

I DIRITTI DEGLI INTERESSATI

LA LIMITAZIONE DEL TRATTAMENTO

SE

-SI CONTESTI L'ESATTEZZA DEL DATO

-TRATTAMENTO ILLECITO

-VENIRE MENO DEL BISOGNI

-OPPOSIZIONE AL TRATTAMENTO

I DIRITTI DEGLI INTERESSATI

PORTABILITA' DEI DATI

L'INTERESSATO FACOLTÀ DI RICHIEDERE I DATI PERSONALI TRATTATI DA UN TITOLARE SU UN FORMATO STRUTTURATO, DI USO COMUNE E LEGGIBILE DA DISPOSITIVO AUTOMATICO DI SUA SCELTA, DI TRASMETTERLI A UN ALTRO TITOLARE DEL TRATTAMENTO DI SUA SCELTA SENZA IMPEDIMENTI.

I DIRITTI DEGLI INTERESSATI

OPPOSIZIONE AL TRATTAMENTO

L'INTERESSATO

HA IL DIRITTO DI OPPORSI

iN QUALSIASI MOMENTO,

. IL TITOLARE DEL TRATTAMENTO SI ASTIENE DAL TRATTARE ULTERIORMENTE I DATI PERSONALI

SALVO CHE EGLI DIMOSTRI L'ESISTENZA DI MOTIVI LEGITTIMI CHE PREVALGONO

Il GDPR rafforza i criteri di:

- Trasparenza
- Evidenza
- Responsabilità

Principio di Accountability…..

)

Welcome

"METTERE IN ATTO MISURE TECNICHE E ORGANIZZATIVE ADEGUATE PER GARANTIRE ED ESSERE IN GRADO DI DIMOSTRARE, CHE IL TRATTAMENTO È EFFETTUATO CONFORMEMENTE AL GDPR".

Valutazione di Impatto

- a DPIA (Data Protection Impact Analysis) è un processo di valutazione del rischio.

- La DPIA è regolata dalle linee guida WP 248 del Garante

- OBBLIGATORIO solamente quando sono presenti elevati rischi:

  → per i diritti e
  → le libertà delle persone fisiche

Valutazione di Impatto

La DPIA è NECESSARIA

- Valutazione sistematica e globale di aspetti personali tramite trattamenti automatizzati e che generano informazioni per decisioni con effetti giuridici e che incidono sulle persone

- Trattamento su larga scala di particolari dati sensibili

- Sorveglianza sistematica su larga scala in zone accessibile al pubblico

Valutazione di Impatto

La Casi in cui la DPIA NON è NECESSARIA:

- Trattamenti non suscettibili di provocare rischi elevati peri diritti e le libertà delle persone fisiche
- Trattamenti con DPIA analoghe
- Trattamenti con base giuridica nel diritto dell'unione e dello stato membro
- Trattamenti definiti dall'autorità di vigilanza

Privacy by Design & by Default

- Principi introdotti all'art. 25 finalizzati all'impostazione della tutela dei dati personali fino dalla progettualità dei trattamenti

Obbligatorietà del Registro dei trattamenti

Obbligatorietà del Registro dei Trattamenti	
> 250 dipendenti	< 250 dipendenti
Sempre	Trattamenti con rischi Privacy
	Trattamenti non occasionali
	Trattamenti con Dati sensibili
	Trattamenti con dati giudiziari

Definizione del DPO

DPO (Data Protection Office) o RPD (Responsabile Protezione Dati.

- Chi è il DPO ?
- Il DPO è una figura obbligatoria?
- Cosa fa il DPO?
- Qual è il profilo del DPO?

Definizione del DPO

- Ruolo di Sorveglianza sul rispetto del GDPR (osservanza)
- Ruolo da Intermediario tra gli stakeholder (autorità, interessata, titolare, responsabili)
- Ruolo consultivo (applicazione della normativa, definizione policy aziendali, rapporti con Autorità)

Obbligatorietà del DPO

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

- le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Profilo del DPO

Deve essere nominato in base a criteri di adeguatezza e accountability:

- Competenza
- Indipendenza
- Raggiungibilità

- Conflitto di interesse

- Valutazione per ruoli esterno

Reclami ed assistenze degli interessati

- Reclami e assistenze degli interessati
  - Accesso ai dati personali
  - Richiesta di conoscere alcune notizie sul trattamento
  - Richiesta di intervento sui dati
  - Opposizione al trattamento per fini pubblicitari
  - Opposizione al trattamento per motivi legittimi

Reclami ed assistenze degli interessati

- Reclami e assistenze degli interessati

    - Modello per esercizio dei diritti: possibile ricorso all'autorità giudiziaria o al Garante se non c'è risposta entro 15 giorni

    - Si passa a 72 ore

- Potrebbero essere riesaminati in ambito di certificazioni

Scenari di Certificazioni

"Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, **potrebbero** essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati."

Data Breach

Per "Violazione di dati" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito:

- la distruzione,
- la perdita,
- la modifica,
- la divulgazione non autorizzata
- o l'accesso

ai dati personali trasmessi, conservati o comunque trattati
Si tratta di incidenti di sicurezza in cui dati personali vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

Data Breach

Il titolare deve notificare all'autorità di controllo la violazione di dati personali (data breach) entro settantadue ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

???

REGIME SANZIONATORIO

- **RESPONSABILITÀ PENALE:** DIRITTO INTERNO, MA PREVIA COMUNICAZIONE ALLA COMMISSIONE EUROPEA

- **RESPONSABILITÀ CIVILE** PER RISARCIMENTO DEL DANNO DEMANDATA AL DIRITTO NAZIONALE SECONDO LE REGOLE DI GIURISDIZIONE DEL GDPR

- **RESPONSABILITÀ AMMINISTRATIVA** E SANZIONI AMMINISTRATIVE: PREVISTE DA GDPR MA COMMINATE DALL'AUTORITÀ NAZIONALE

IL NUOVO REGOLAMENTO EUROPEO 679/2016

???

SANZIONI

SINO A 10.000.000 EURO 2% FATTURATO SE IMPRESE (ART.83 CO.4)

- VIOLAZIONE DEI TRATTAMENTI DI DATI DEL MINORE ANNI 16/13 (ART.8
- VIOLAZIONE DEL PRINCIPIO DEL PRIVACY BY DESIGN (ART.25)
- INADEGUATEZZA DELL'ACCORDO DI CONTITOLARITÀ (ART.26)
- VIOLAZIONE DELL'OBBLIGO DI DESIGNAZIONE PER ISCRITTO DEL RAPPRESENTANTE NELL'UNIONE (ART.27)
- VIOLAZIONI IN MATERIA DEI CONTENUTI DELLE NOMINE E DELLE DELEGHE
- VIOLAZIONE DELLE NORME SUL REGISTRO DEI TRATTAMENTI
- MANCATA COOPERAZIONE CON AUTORITÀ (ART.31)
- INADEGUATEZZA DELLE MISURE DI SICUREZZA (ART.32)
- OMESSA NOTIFICA PER DATA BREACH (ART.33)
- OMESSA COMUNICAZIONE ALL'INTERESSATO (ART.34)
- VIOLAZIONE DELL'OBBLIGO DI PROCEDERE ALLA VALUTAZIONE D'IMPATTO (ART.35)
- OMESSA CONSULTAZIONE PREVENTIVA O DI INFORMAZIONI DA DARSI ALL'AUTORITÀ (ART.36)
- OMESSA O INADEGUATA IDENTIFICAZIONE DEL DPO O SUA INADEGUATA INDIPENDENZA (ART.37-38)
- VIOLAZIONI DEL DPO
- OMESSE INFORMAZIONI ALL'ENTE DI CERTIFICAZIONE
- VIOLAZIONI DEGLI ORGANISMI DI CERTIFICAZIONE

???

SANZIONI

FINO A 20 000 000 EUR, O PER LE IMPRESE, FINO AL 4 % DEL FATTURATO MONDIALE TOTALE ANNUO (ART.83 CO.5)

- PER VIOLAZIONE AI PRINCIPI BASE DEL TRATTAMENTO
- PER VIOLAZIONE DEI DIRITTI DELL'INTERESSATO (CANCELLAZIONE, PORTABILITÀ ETC…)
- PER VIOLAZIONI SU TRASFERIMENTI A PAESI EXTRA EU
- VIOLAZIONI AD OBBLIGHI INTRODOTTI DA STATI MEMBRO
- INOSSERVANZA DELLE PRESCRIZIONI/INIBIZIONI DELL'AUTORITÀ AI SENSI DELL'ART. 58