LE NUOVE NORME SULLA PRIVACY:

OBBLIGHI E ADEMPIMENTI DELLE IMPRESE

Padova, 11 aprile 2018

IL NUOVO APPROCCIO AL TRATTAMENTO DEI DATI PERSONALI NEL REGOLAMENTO UE 2016/679

AVV. ANNA SOATTO

Il caso di Cambridge Analytica

I dati raccolti per mezzo di una app per scopi di ricerca scientifica sono stati utilizzati per attività commerciali come la vendita di servizi al fine di prevedere e influenzare scelte elettorali attraverso annunci politici personalizzati

Il GDPR introduce regole più severe che garantiscono agli utenti un maggiore controllo sulle proprie informazioni personali

Bilanciamento di interessi

1. Il regolamento stabilisce norme relative alla **protezione delle persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla **libera circolazione di tali dati**.
2. Il presente regolamento protegge i **diritti e le libertà fondamentali delle persone fisiche**, in particolare il diritto alla protezione dei dati personali.
3. La libera **circolazione dei dati** personali nell'Unione **non** può essere **limitata** né **vietata** per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

L’ambito di applicazione territoriale del regolamento: art. 3

Il Regolamento si applica:

1. ai trattamenti effettuati da **titolari stabiliti nell’UE**, indipendentemente dal fatto che il trattamento sia effettuato o meno nella UE;
2. ai trattamenti effettuati da titolari non stabiliti nell’UE se il trattamento ha ad oggetto dati personali di **interessati che si trovino nell’Unione** e riguarda
   a) l’offerta di beni e servizi (anche non a pagamento) ai suddetti interessati,
   b) il monitoraggio di comportamenti che abbiano luogo nel territorio dell’UE.

Novità

- ✓ Nuove definizioni
- ✓ Informativa
- ✓ Consenso
- ✓ Diritti
  - ✓ diritto all'oblio,
  - ✓ portabilità dei dati
- ✓ Nuovo approccio e nuovi adempimenti:
  - ✓ privacy by design, privacy by default,
  - ✓ registro dei trattamenti,
  - ✓ valutazione preventiva d'impatto,
  - ✓ notifica dei data breach,
- ✓ Precisazione di ruolo e compiti di titolare, contitolari e responsabili
- ✓ Nuova figura del responsabile della protezione dei dati
- ✓ Responsabilità e sanzioni

Definizione di dato personale

Dato personale: art. 4

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Categorie particolari di dati personali: art. 9

Non esiste una specifica definizione di dati personali ‘sensibili’ o di dati personali ‘giudiziari’.

«categorie particolari di dati personali»: si tratta delle informazioni ‘‘che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona fisica’’.

«dati relativi alla salute»: art. 4: ‘‘dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute’’.

Definizione di trattamento

Trattamento: art. 4

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 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

Criteri su cui impostare gli atti

Fondamenti di liceità del trattamento

Principi generali applicabili al trattamento di dati personali: art. 5

- ✓Liceità
- ✓Correttezza
- ✓Trasparenza
- ✓Limitazione delle finalità (esplicite e legittime)
- ✓Minimizzazione dei dati (adeguati, pertinenti, limitati)
- ✓Esattezza (e aggiornamento)
- ✓Limitazione della conservazione (non superiore al conseguimento delle finalità per le quali sono trattati)
- ✓Integrità e riservatezza (protezione da trattamenti non autorizzati o illeciti e dalla perdita mediante misure tecniche e organizzative adeguate)

Consenso dell'interessato

Consenso dell'interessato

- Libero
- Specifico
- Informato
- Inequivocabile
- La formula utilizzata per chiedere il consenso deve essere comprensibile, semplice, chiara
- Esplicito: per categorie particolari di dati

Consenso dell'interessato

- Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali

- Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Il consenso: segue

L’esecuzione di un contratto o la prestazione di un servizio non possono essere condizionati alla prestazione del consenso al trattamento di dati personali non necessario all’esecuzione del contratto o servizio

Qualora il trattamento di basi sul consenso non occorre che l’interessato presti di nuovo il suo consenso, se è stato espresso secondo le modalità conformi alle condizioni del regolamento, affinché il titolare del trattamento possa proseguire il trattamento dopo la data di applicazione del regolamento

Revoca del consenso e diritto all'oblio

L'interessato ha il **diritto di revocare il proprio consenso** (deve essere informato di questo diritto) in qualsiasi momento, con modalità di esecuzione della revoca del consenso facili come la sua prestazione originaria

La revoca non pregiudica la liceità del trattamento fino a quel momento effettuato

diritto all'oblio: cancellazione se l'interessato revoca il consenso e non sussiste altro fondamento giuridico per il trattamento

Check list consenso

- ✓ Le modalità formali soddisfano il requisito della inequivocabilità?
- ✓ Il titolare qualifica come consenso il silenzio o l'inattività dell'interessato o la preselezione di caselle?
- ✓ La formula del consenso è chiaramente distinguibile o è contenuta in una clausola specifica separata dalle altre clausole del contratto o da altri contenuti?
- ✓ Sono indicate l'identità del titolare, le finalità del trattamento e il periodo di conservazione dei dati?
- ✓ È precisato che il consenso può essere revocato ed è indicata la modalità di revoca?

Informativa

Contenuto dell'informativa secondo il codice privacy

Essa deve contenere indicazione di:

1. Gli estremi identificativi del titolare
2. Le finalità e le modalità del trattamento
3. I soggetti o le categorie di soggetti cui i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili od incaricati e l'eventuale ambito di diffusione dei dati medesimi
4. I diritti dell'interessato
5. La natura obbligatoria o facoltativa del conferimento dei dati
6. Le conseguenze del rifiuto di rispondere

Informativa: integrazione del regolamento UE: artt. 13 e 14

Rispetto agli elementi prescritti dal Codice Privacy il titolare dovrà inserire obbligatoriamente **anche**:

- i **dati di contatto** del nuovo DPO ove previsto
- la **base giuridica** del trattamento a corredo dell'illustrazione delle finalità del trattamento
- qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare o di terzi, la **specificazione di quali siano i legittimi interessi** perseguiti dal titolare o da terzi
- l'**ambito del trasferimento all'estero** o ad un'organizzazione internazionale dei dati personali
- il **periodo di conservazione** dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo
- l'esistenza del **diritto alla portabilità** dei dati

Informativa: integrazione del regolamento (segue)

- l'esistenza del **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca
- il diritto di proporre **reclamo al Garante** Privacy
- l'esistenza di un **processo decisionale automatizzato**, compresa la profilazione e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato
- le **categorie** di dati personali oggetto di trattamento (se i dati non siano raccolti presso l'interessato)
- la **fonte** da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico (se i dati non siano raccolti presso l'interessato)

Informativa: tempi e modalità

Nel caso di dati personali non raccolti direttamente presso l'interessato l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato)

Concisa, trasparente, intelligibile per l'interessato e facilmente accessibile, con linguaggio semplice e chiaro

Le informazioni sono fornite per iscritto o con altri mezzi, anche se del caso con mezzi elettronici

Le informazioni da rendere agli interessati possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone devono essere leggibili da dispositivo automatico.

Diritti degli interessati

Modalità per l'esercizio dei diritti: art. 12

- Termine per la risposta all'interessato entro un mese dalla richiesta

- Spetta a titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato (se si tratta di richieste manifestamente infondate o eccessive, altrimenti è gratuito)

- È opportuno che i titolari adottino misure tecniche e organizzative necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati

Diritto di accesso (art. 13)

Diritto all'oblio (art. 17)

Diritto di limitazione del trattamento (art. 18)

Diritto alla portabilità dei dati (art. 20)

Diritto alla cancellazione, diritto all'oblio: art. 17

Specificazione del diritto alla cancellazione dei dati personali.

L'interessato esercita il diritto all'oblio chiedendo al titolare che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano 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 che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento

Rimane lecita l'ulteriore conservazione dei dati in caso di diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale o un compito di interesse pubblico, per motivi di interesse pubblico nel settore della sanità pubblica, ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, per accertare, esercitare o difendere un diritto in sede giudiziaria.

Diritto alla portabilità dei dati: art. 20

Si tratta del diritto dell'interessato di ricevere i dati dal titolare e trasferirli ad altro titolare del trattamento senza impedimenti da parte del titolare cui i dati sono stati in precedenza forniti.

Il diritto è **esercitabile quando** il trattamento:

A) sia effettuato con mezzi automatizzati; e

B) si basi sul consenso precedentemente prestato dall'interessato; o si basi su un contratto o su trattative precontrattuali.

In questi specifici casi l'interessato, fermo restando il suo diritto alla cancellazione dei dati, ha il diritto di ottenere la trasmissione diretta dei dati da un titolare del trattamento all'altro «*se tecnicamente fattibile*»

Diritti dell'interessato: artt. 15-21

CONFERMA e COMUNICAZIONE

INFORMAZIONI (origine, finalità, modalità del trattamento esistenza processo decisionale automatizzato, destinatari comunicazione o diffusione, periodo conservazione),

A C C E S S O

RETTIFICA
INTEGRAZIONE
CANCELLAZIONE OBLIO
LIMITAZIONE
PORTABILITA'
OPPOSIZIONE

Responsabilizzazione «accountability»

Responsabilizzazione («accountability»)

Il Regolamento tende a **non** definire **adempimenti specifici**, **ma** a definire **principi di conformità**.

Il titolare deve implementare i propri processi per raggiungere tali obiettivi.

In assenza di specifici adempimenti viene valutata l'impostazione complessiva dei trattamenti riguardo ai rischi che ne derivano.

Accountability

Adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento

I titolari hanno il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali.

Il titolare dunque sarà valutato a posteriori, in un'eventuale verifica, sull'adeguatezza dei propri comportamenti, dei processi dagli stessi implementati per raggiungere gli obiettivi.

Questo principio è applicato innanzitutto nella gestione della sicurezza e protezione dei dati personali.

Approccio responsabilizzante: art. 24

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Compliance

- ✓ La conformità normativa (compliance) è un aspetto procedurale (organizzativo) e non (solo) documentale.
- ✓ La conformità normativa è il risultato del controllo dei processi di trattamento dei dati personali.
- ✓ Controllare un trattamento significa **conoscere** le modalità organizzative con cui viene svolto.
- ✓ Il controllo è la conseguenza dell'analisi dei trattamenti.
- ✓ Un **approccio complessivo**, logico e conforme allo spirito del GDPR prevede che la conformità normativa parta dalla conoscenza dei trattamenti per giungere alla gestione degli adempimenti e non dalla predisposizione della documentazione.

Data protection by design

Protezione dei dati fin dalla progettazione

Configurare il trattamento prevedendo fin dall'inizio (al momento di determinare i mezzi di trattamento e al momento del trattamento stesso) le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto di:

a) stato dell'arte e costi di attuazione;
b) natura, ambito di applicazione, contesto e finalità del trattamento;
c) rischi aventi probabilità e gravità diverse per i diritti e le libertà degli interessati.

Applicare **misure tecniche e organizzative adeguate** (es. pseudonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie per tutelare i diritti degli interessati.

Protezione per impostazione predefinita

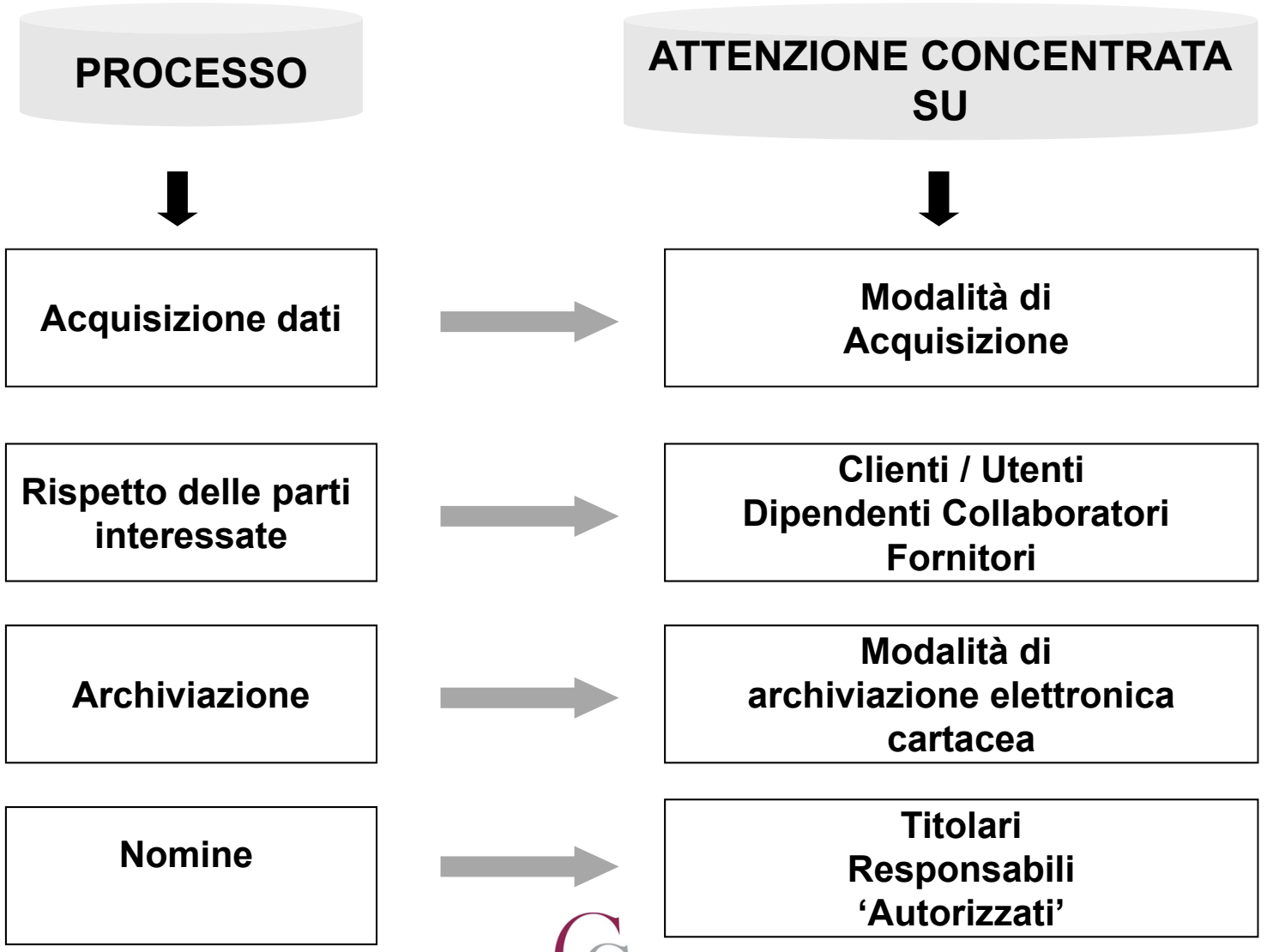
il titolare mette in atto misure tecniche e organizzative adeguate **per garantire che siano trattati, per impostazione predefinita** (by default) **solo i dati personali necessari per ogni specifica finalità del** trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Il titolare potrà utilizzare un meccanismo di certificazione, approvato da organismi designati dagli Stati membri, per dimostrare la conformità ai principi di privacy by design e by default (artt. 42-43)

Approccio alle misure di sicurezza e protezione dei dati

- ✓ L'approccio alle misure di sicurezza e protezione dei dati personali è responsabilizzante nei confronti del titolare del trattamento.
- ✓ Non esiste un corrispondente delle misure minime di sicurezza come erano definite nel disciplinare tecnico del codice privacy.
- ✓ L'obbligo non è solo quello di adottare misure di sicurezza ma quello di definire politiche di sicurezza.
- ✓ Tra gli obblighi di sicurezza vi è anche quello di essere in grado di dimostrare le politiche di sicurezza adottate

Approccio all'acquisizione dei dati



Adempimenti

Registro delle attività di trattamento: deve essere redatto (anche in formato elettronico) nelle Imprese o organizzazioni con più di 250 dipendenti sia dal titolare che dal responsabile del trattamento e va esibito su richiesta del Garante

L'obbligo si applica **anche alle imprese con meno di 250 dipendenti**, **se** il trattamento

a) presenta un rischio per i diritti e le libertà dell'interessato;
b) non è occasionale e include dati personali sensibili, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, relativi a condanne penali e a reati

Registro dei trattamenti: contenuto obbligatorio

- ✓ Nome e dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare e del responsabile della protezione dei dati.
- ✓ Finalità del trattamento.
- ✓ 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.
- ✓ Trasferimenti di dati personali verso un paese terzo.
- ✓ Termini ultimi previsti per la cancellazione delle diverse categorie di dati, ove possibile.
- ✓ Descrizione generale delle misure di sicurezza tecniche e organizzative, ove possibile.

Registro dei trattamenti: contenuto suggerito

- ✓Caratteristiche di liceità e correttezza del trattamento
- ✓Modalità di informativa
- ✓Modalità di raccolta del consenso
- ✓Archivi trattati, modalità di aggiornamento e relativa protezione
- ✓Individuazione degli incaricati
- ✓Misure di sicurezza specifica
- ✓Sistemi informatici utilizzati per i trattamenti

Valutazione di impatto: contenuto minimo art. 35

Quando un tipo di intervento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare effettua, prima di procedere al trattamento una valutazione (d'impatto) che contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento
b) valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità
c) una valutazione dei rischi per i diritti e le libertà degli interessati

Analisi preventiva

Devono sostanziarsi in attività specifiche e dimostrabili

- Mappatura dei trattamenti di dati personali
- Analisi del rischio di impatti negativi sulle libertà e diritti degli interessati
- Processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative anche di sicurezza che il titolare ritiene di adottare per mitigare tali rischi

Contenuto della valutazione d'impatto e consultazione preventiva

La valutazione, soggetta a riesame periodico, contiene almeno: una **descrizione sistematica dei trattamenti previsti e delle finalità** del trattamento, la valutazione della **necessità** e **proporzionalità** dei trattamenti in relazione alle finalità, la valutazione dei **rischi** per i diritti e le libertà degli interessati e le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati.

Se la valutazione preventiva indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio, il titolare, prima di procedere al trattamento, è tenuto a consultare il Garante.

Valutazione di impatto

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

Larga scala

Fattori:

- ✓ Numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento
- ✓ Il volume dei dati e/o delle diverse tipologie di dati oggetto di trattamento
- ✓ Durata, ovvero la persistenza, dell'attività di trattamento
- ✓ Portata geografica dell'attività di trattamento

Orientamenti Commissione UE per l'applicazione diretta del regolamento

Il Regolamento non ha modificato in modo sostanziale i concetti e i principi fondamentali della legislazione in materia di protezione dei dati personali introdotta nel 1995. La grande maggioranza dei titolari del trattamento e dei responsabili del trattamento che rispettano già le disposizioni UE non dovrà quindi introdurre importanti modifiche nelle proprie operazioni di trattamento dei dati per conformarsi al regolamento. 24.01.2018

CORTELLAZZO & SOATTO
Economia Diritto e Finanza di Impresa

Via Porciglia, 14 – Padova
Via Tuveri, 25 – Cagliari
www.cortellazzo-soatto.it

CORTELLAZZO & SOATTO
Economia Diritto e Finanza di Impresa