GDPR Regolamento Europeo n. 679/2016

Il diritto della Privacy

La direttiva è intesa a proteggere i diritti e le libertà delle persone fisiche in ordine al trattamento dei dati personali

SI APPLICA A:

- Dati trattati con l'ausilio di strumenti elettronici;
- Dati contenuti o destinati a figurare in archivi non automatizzati

NON SI APPLICA:

- Trattamento per finalità personale o domestica;
- Trattamento per finalità escluse dall'applicazione del diritto comunitario come la pubblica sicurezza, la difesa, la sicurezza dello Stato

FINALITÀ

- *assicurare un livello coerente di protezione delle persone in tutta l'Unione*

AMBITO DI APPLICAZIONE

- A ***titolari*** e ***responsabili*** di trattamento ***stabiliti*** nell'Unione ***indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione***
- A ***titolari*** e ***responsabili*** di trattamento ***non stabiliti*** nell'UE che trattino dati personali di **PERSONE FISICHE** che si trovano nell'UE quando il trattamento è in relazione a offerte di beni servizi

PRINCIPI GENERALI:

- Liceità, correttezza e trasparenza nel trattamento
- Principio di finalità
- Adeguatezza e pertinenza
- Principio di esattezza
- Principio di limitazione della conservazione
- Integrità e riservatezza
- **RESPONSABILIZZAZIONE – Accountability**

MODIFICHE

- Consenso (art. 7)
- Informativa (artt. 12 ss.)
- Diritto di accesso dell'interessato (artt. 15 ss)
- Diritto all'oblio (art.17)
- Compiti del responsabile (art. 28)
- Sicurezza del trattamento (art. 32)
- Sanzioni (artt. 82 e ss)

NOVITÀ

- Diritto alla **portabilità** dei dati (art. 20)
- **Responsabilità del Titolare**
- **Trasparenza** (art. 24)
- **Privacy by design and by default** (art. 25)
- **Registro dei trattamenti** (art.30)
- **Notifica** della violazione dei dati personali (art. 33)
- **Valutazione** di Impatto (art. 35)
- **Data protection officer** – responsabile della protezione dei dati (art. 37)
- **Certificazione / Marchi** (art. 42)

DEFINIZIONI: *DATO PERSONALE*

Ampliamento della applicazione materiale del Regolamento Europeo rispetto a quanto sancito dalla direttiva 95/46

DATO PERSONALE = *INFORMAZIONE*

Concezione da uniformarsi al progresso ***tecnologico e scientifico***

- «Qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale***»

  identificativi online:

  - Indirizzi IP
  - Marcatori temporanei –cc.dd. Cookies
  - Tag

DATI PARTICOLARI

(ART. 9 CO.1) *è vietato trattare dati personali che rivelino:*

- L'origine razziale od etnica
- Le convinzioni religiose, filosofiche
- Le opinioni politiche
- L'appartenenza sindacale
- **Trattare dati genetici, dati biometrici intesi ad indentificare in modo univoco una persona fisica**
- Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona

ALTRE TIPOLOGIE DI DATI

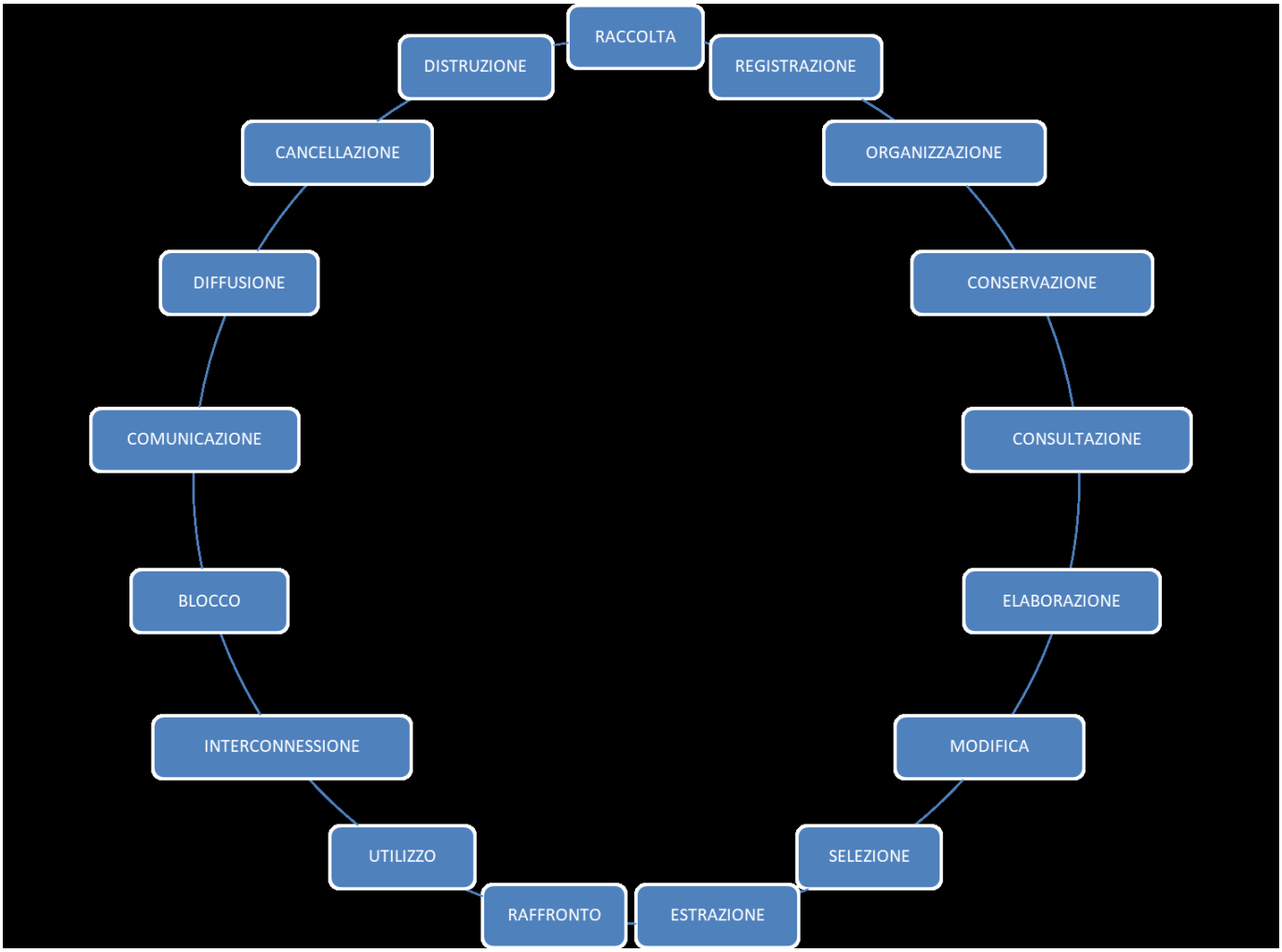
- **DATI GIUDIZIARI:** sono quelli idonei a rivelare provvedimenti in materia di:
  - casellario giudiziale
  - anagrafe delle sanzioni amministrative, dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o di indagato
- **ESCLUSI:** sono quelli relativi a provvedimenti civili ed amministrativi
- **DATI SEMI SENSIBILI:** sono quelli che non sono né sensibili e né giudiziari ma per i quali possono presentarsi dei rischi specifici e vi rientrano:
  - I dati inseriti nelle centrali rischi bancarie
  - I dati relativi alla situazione finanziaria
  - Videosorveglianza

DATI PARTICOLARI (ART. 9)

- **È VIETATO TRATTARE DATI PARTICOLARI salvo eccezioni come ad esempio:**
  - Consenso esplicito
  - Assolvimento obblighi del titolare del trattamento o dell'interessato in materia di **diritto del lavoro e della sicurezza sociale e protezione sociale**
  - Necessità di tutelare un interesse vitale dell'interessato
  - Il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, **da una fondazione, associazione** o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali
  - dati resi manifestamente pubblici dall'interessato
  - **accertare o difendere un diritto in sede giudiziaria**
  - motivi di interesse pubblico dominante

DEFINIZIONE: *TRATTAMENTO DEI DATI*

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti



PROFILAZIONE (ART. 4 C. 1 SUB 4)

- ***Trattamento automatizzato*** di dati personali consistente nell'utilizzo di essi per valutare determinati aspetti relativi ad una persona fisica, in particolare:
  - Analisi produttive relative al rendimento professionale
  - Situazione economica
  - La salute
  - Preferenze personali
  - Interessi
  - Comportamento
  - L'affidabilità
  - Ubicazione o spostamento della persona interessata

REGISTRO DEI TRATTAMENTI (ART. 30)

- **Non obbligatorio per imprese < 250 dipendenti a meno che:**
  - Il trattamento possa presentare un ***rischio per i diritti e le libertà*** dell'interessato
  - Il trattamento non sia occasionale
  - **Includa dati particolari** (art. 9 paragrafo 1);
  - ***Includa dati personali relativi a condanne penali e reati*** (art. 10);

- ***A DISPOSIZIONE DEL GARANTE DEVE CONTENERE:***
  - Il nome e i dati del titolare del trattamento e del responsabile della protezione dei dati
  - Le finalità del trattamento e le misure di sicurezza
  - Una descrizione delle categorie degli interessati
  - Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati
  - Ove applicabile, i trasferimenti di dati personali verso paesi terzi e la loro identificazione
  - *I termini ultimi per la cancellazione delle diverse categorie di dati*

DATA BREACH NOTIFICATION (ART. 33)

VIOLAZIONE DEI DATI PERSONALI (perdita, distruzione, diffusione indebita dei dati)

- ***Obbligo di notifica al garante*** (entro 72 ore) (tipologia della violazione realizzata, modalità in cui si è realizzata, possibili danni ai dati personali):
  - Obbligatoria per tutti i titolari del trattamento nel nuovo regolamento UE
  - Indicare le misure di contrasto adottate
- ***Obbligo di comunicazione all'interessato*** (senza ritardo)
  - In caso di rischio elevato
  - Per disposizione del Garante

NOTIFICA AL GARANTE: COSA CAMBIA

CODICE PRIVACY		REGOLAMENTO UE
Obbligatoria per particolari trattamenti	**Notifica Generale**	Abolita
Obbligatoria per taluni settori	**Notifica Data Breach**	Obbligatoria per tutti i titolari

SOGGETTI COINVOLTI

- **TITOLARE DEL TRATTAMENTO** -Data Controller
  - Determina finalità e mezzi di trattamento dei dati personali
  - Impartisce istruzioni e direttive
  - Svolge funzioni di controllo
- ***RESPONSABILE DEL TRATTAMENTO –Data Processor***
  - Preposto dal titolare al trattamento dei dati personali
- ***INCARICATO AL TRATTAMENTO***
  - Persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (art. 4 lett. H-Codice della Privacy)

TITOLARE

PERSONA FISICA O GIURIDICA, L'AUTORITA' PUBBLICA, IL SERVIZIO O ALTRO ORGANISMO ***CHE DETERMINA LE FINALITA' E I MEZZI DEL TRATTAMENTO DEI DATI PERSONALI.***

- In caso di azienda persona giuridica o di studio associato il Titolare sarà l'azienda o lo studio stesso
- In caso di azienda individuale o professionista non associato il Titolare sarà la persona fisica
- In ogni caso non è necessario alcun atto di nomina né requisiti minimi in capo al Titolare.

RESPONSABILE DEL TRATTAMENTO

- ***Soggetto scelto dal titolare in grado di prestare*** *«garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del regolamento, anche in materia di sicurezza del trattamento»* (Considerando 81 Reg. UE 679/2016)
- **Può** essere sia una **persona fisica** che una **persona giuridica**.
- La sua designazione è fondamentale e risponde ad esigenze di natura organizzativa
  - È designato dal titolare facoltativamente
  - Deve attenersi alle istruzioni del titolare
  - I compiti devono essere indicati dettagliatamente
  - A sua volta può designare sub-responsabili con il previo consenso del Titolare

NOMINA DEL RESPONSABILE DEL TRATTAMENTO

- Deve essere dallo stesso sottoscritta per accettazione
- Può essere a tempo indeterminato
- La cessazione dell'ufficio avviene per revoca/cessazione
- Deve essere informato delle responsabilità giuridiche che gli sono affidate nell'ambito del trattamento dei dati
- Deve attenersi alle istruzioni date dal titolare
- Il titolare può verificare periodicamente sulla puntuale osservanza delle proprie disposizioni
- I suoi compiti sono analiticamente specificati per iscritto dal titolare.

INCARICATO DEL TRATTAMENTO - OBBLIGO DI ISTRUZIONE

Il Regolamento pur non definendo l'Incaricato come veniva fatto nel Codice Privacy ne chiarisce i limiti all'art 29 stabilendo che chiunque agisca sotto l'autorità del Titolare o del Responsabile del trattamento non può trattare i dati se non è ***istruito*** in tal senso dal Titolare del trattamento.

AMMINISTRATORE DI SISTEMA - *Altri soggetti*

- Figura professionale finalizzata alla ***gestione*** e alla ***manutenzione*** di un impianto di elaborazione o di sue componenti.
- A tale figura sono equiparate altre professionalità sulle quali incombono rischi affini relativi alla protezione dei dati:
  - Amministratori di basi di dati
  - Amministratori di reti e apparati di sicurezza
  - Amministratori di sistemi di software complessi
  - Valutazione delle qualità tecniche, professionali e di condotta
  - Designazione individuale con elencazione analitica delle funzioni singolarmente attribuite
  - Predisposizione di procedure e meccanismi di controllo
  - Adozione di idonee soluzioni per effettuare la registrazione degli accessi
  - ***Adozione di un modello organizzativo da coordinare con quello previsto dal d.lgs. 231/01***

DATA PROTECTION OFFICER DPO

Responsabile della protezione dei dati art 37 Regolamento

- Soggetto incaricato di affiancare il titolare e il responsabile del trattamento, fornito di ***conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati*** nel rispetto delle disposizioni contenute nel regolamento europeo.
- Nello svolgimento delle sue funzioni deve godere di ***indipendenza*** può essere:
  - Dipendente del titolare o del Responsabile
  - Esterno con contratto di servizi

Figura di garanzia aggiuntiva interna all'azienda **NOMINA OBBLIGATORIA:**

- 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**.

COMPITI DEL DPO:

- ***Informazione e di consulenza*** in merito agli obblighi derivanti dal Regolamento UE 2016/679, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- ***Sorveglianza*** tramite attività di audit;
- ***Verifica e controllo*** circa l'attuazione e l'applicazione del Regolamento, della disciplina nazionale e delle policy interne del titolare del trattamento;
- Controllare la corretta notifica e comunicazione in caso di ***data breach notification***;

- ***Verificare*** che i processi interni siano sviluppati secondo i principi della privacy by design e privacy by default
- ***Interloquire*** con l'Autorità Garante e le altre autorità competenti
- ***Partecipazione*** alle valutazioni di data protection impact assessment e sorvegliarne lo svolgimento;

ANALISI E GESTIONE DEL RISCHIO

- **L'analisi del rischio** ha l'obiettivo di identificare i rischi per la sicurezza, individuando le possibili cause di un evento sfavorevole
- **La valutazione del rischio** permette di stimare l'entità dei fattori di rischio in termini di probabilità
- **La gestione del rischio** è il processo di identificazione, controllo, eliminazione e riduzione degli eventi che possono avere un impatto

SCELTA DEL METODO DI GESTIONE DEL RISCHIO

Esistono diversi metodi di gestione del rischio, a titolo esemplificativo si distinguono in:

- ***METODI QUANTITATIVI:***
  - Come quelli economico finanziari che indicano il rischio in termini monetari
- ***METODI QUALITATIVI:***
  - Hanno lo scopo di identificare il rischio secondo una scala di valori alto, medio e basso

CODICE DELLA PRIVACY: ART. 31, COMMA 1 DEL D.LGS. N. 196/2003

- *Stabilisce che i dati personali oggetto di trattamento devono essere custoditi e controllati in modo da ridurre al minimo i rischi di:*
  - ***DISTRUZIONE O PERDITA, ANCHE ACCIDENTALE DEI DATI***
- Il rischio va letto in correlazione all'art. 11, comma 1 lett. d), in base al quale i dati devono essere completi e disponibili, proteggendo fisicamente gli apparecchi che li contengono
  - ***ACCESSO NON AUTORIZZATO***
- Il rischio fa riferimento sia all'accesso fisico ad ambienti dove sono custoditi dati personali sia a banche dati elettroniche
  - ***TRATTAMENTO NON CONFORME ALLE FINALITA' DELLA RACCOLTA***
- Il rischio fa riferimento a un trattamento inizialmente lecito e corretto, ma che con il tempo si è discostato dal principio di finalità.
  - ***TRATTAMENTO NON CONSENTITO***
- Il rischio va letto in correlazione con l'art. 11, comma 1 lett. a) e fa riferimento a qualunque operazione che renda il trattamento illecito o non corretto

REG. UE 679/2016 («ACCOUNTABILITY»)

Art. 24 del regolamento -responsabilità del titolare del trattamento

- Il titolare deve poter mostrare all'esterno di aver predisposto un modello di gestione privacy affidabile e coerente tenuto conto dei "**rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche**"
- Il titolare deve anche garantire il rispetto di politiche adeguate internamente alla propria struttura
- Il titolare deve adottare **MISURE TECNICHE E ORGANIZZATIVE ADEGUATE** a garantire un livello di sicurezza adeguato al rischio (art. 32 Reg. UE 679/2016)

CHE VUOL DIRE CHE IL TITOLARE DEVE ADOTTARE **MISURE TECNICHE E ORGANIZZATIVE ADEGUATE** A GARANTIRE UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO?

PRIVACY BY DESIGN /BY DEFAULT IN GENERALE (ART.25)

- ***Prevenire*** non correggere problemi vanno valutati nella fase di progettazione;
- Privacy come impostazione di ***default*** nel disegno del prodotto/servizio;

- Privacy *incorporata* nel progetto;
- Massima *funzionalità*, in maniera da rispettare tutte le esigenze;
- *Sicurezza* durante tutto il ciclo del prodotto o servizio;
- *Trasparenza*
- *Centralità* dell'utente
  - Trattati solo dati necessari per ciascuna finalità (minimizzazione, pseudominimizzazione)
  - Dati non accessibili ad un numero indeterminato di persone
  - Conservati non oltre il tempo necessario

BY DESIGN:

- La **protezione dei dati fin dalla progettazione** dovrà essere attuata in via preventiva:
  - Tenuto conto dello stato dell'arte
  - Dei costi di attuazione
  - Della natura, dell'ambito di applicazione
  - Del contesto
  - Delle finalità del trattamento
  - Dei rischi aventi probabilità e gravità diverse

BY DEFAULT:

- Con la **protezione per impostazione predefinita:** Il Titolare mette in atto misure tecniche ed organizzative per garantire che siano trattati i **soli dati necessari** per ogni singola finalità del trattamento ciò vale anche per:
  - La quantità dei dati personali raccolti
  - La portata del trattamento
  - Il periodo di conservazione
  - L'accessibilità

IN DETERMINATI CASI IL REGOLAMENTO IMPONE L'OBBLIGO IN CAPO AL TITOLARE (O AL RESPONSABILE) DI EFFETTUARE UNA **VALUTAZIONE DI IMPATTO**

VALUTAZIONE D'IMPATTO ART. 35 Reg.UE(Data protection impact assessment)

- È lo strumento, posto in capo al ***titolare del trattamento***, che consente di conoscere a fondo i processi di trattamento dei dati, c.d. Valutazione di impatto sul trattamento dei dati
- Assicura ***trasparenza e protezione*** nelle ***operazioni di trattamento dei dati personali***

Art.35 par.1 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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi

È ESPRESSAMENTE RICHIESTA NEI CASI DI:

- ***Valutazione sistematica e globale di aspetti personali*** basata su trattamenti automatizzati come la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono analogamente sulle persone fisiche
- ***Trattamento su larga scala di dati particolari*** di cui all'art. 9 paragrafo 1 o di dati di cui all'art. 10
- ***Video sorveglianza*** sistematica e su larga scala di una zona accessibile al pubblico

- Altre tipologie di trattamento indicate dall'autorità di controllo

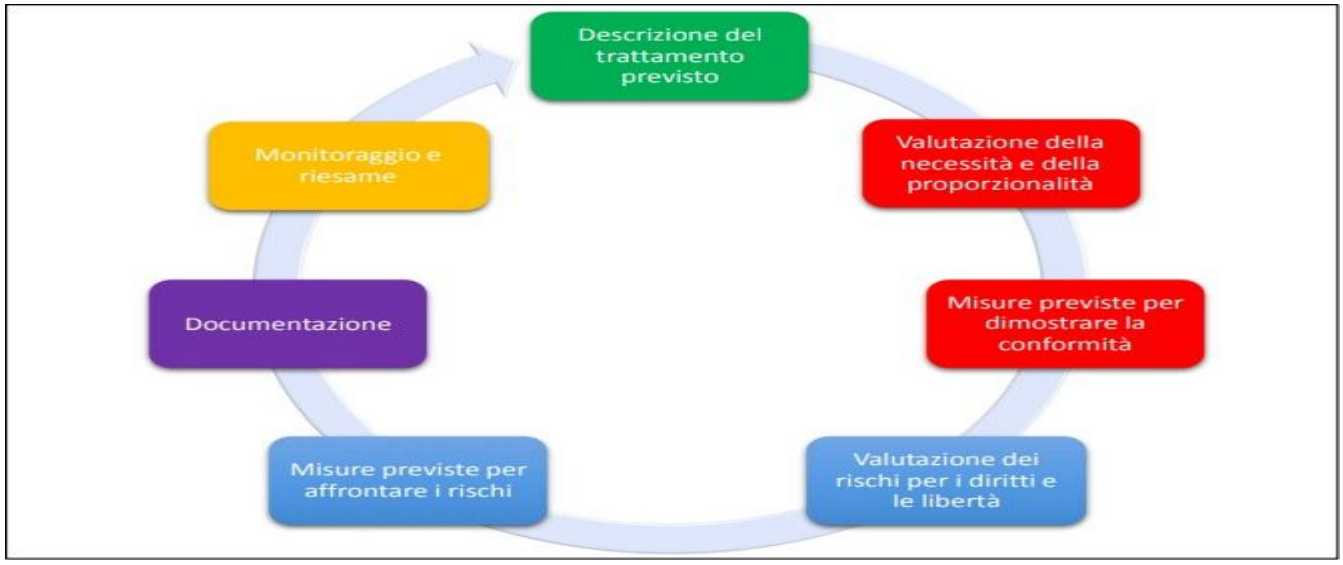
*IL GRUPPO DI LAVORO ART.29 HA ADOTTATO DELLE **LINEE GUIDA (04/04/2017)** IN CUI SI RIPORTANO I CRITERI IN BASE AI QUALI É RAGIONEVOLE RITENERE CHE IL TRATTAMENTO PRESENTI UN **RISCHIO ELEVATO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE CHE RENDONO NECESSARIA LA VALUTAZIONE D'IMPATTO***

Quest'ultima è necessaria nel caso in cui il trattamento presenti almeno 3 di questi requisiti:

- Valutazione o assegnazione di un punteggio
- Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sui diritti dell'interessato
- Monitoraggio sistematico
- Dati sensibili o aventi carattere altamente personale
- Trattamento dati su larga scala
- Combinazione o raffronti di dati
- Dati relativi a interessati vulnerabili
- Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative
- Quando un trattamento in sé "impedisce agli interessati di esercitare in diritto o di avvalersi di un servizio o di un contratto"

Nel caso in cui il Titolare nonostante la presenza di almeno tre dei criteri innanzi indicati decida di non fare la valutazione di impatto deve annotarne le motivazioni nel Registro dei Trattamenti

VALUTAZIONE DI IMPATTO



Cosa è necessario fare se dopo la valutazione d'impatto permangono rischi residui elevati?

CONSULTAZIONE PREVENTIVA

- Il Trattamento deve essere assoggettato alla approvazione del **Garante**
  - Per i casi di rischio adeguato in assenza di misure adeguate per attenuarlo
  - Anche per trattamenti di interesse pubblico (qualora previsto dal singolo Stato membro)

CONSERVAZIONE DEI DATI

- **PRINCIPIO DI STRETTA NECESSITÀ**
- **ANCHE TRAMITE CONTROLLI PERIODICI DEVE ESSERE VERIFICATO IL RISPETTO DEL PRINCIPIO DELLA**

RISPETTO AGLI INCARICHI IN CORSO, DA INSTAURARE O CESSATI
In caso contrario NON POSSONO ESSERE UTILIZZATI

DIRITTO DI ACCESSO

Informazioni alle quali l'interessato ha diritto di accedere:

- *Le finalità* del trattamento;
- *Le categorie* di dati personali in questione;
- *I destinatari* o le *categorie di destinatari* a cui i dati personali sono stati o saranno comunicati;
- Il *periodo* e/o *criteri di conservazione*;
- Il *diritto di* proporre *reclamo* a un'autorità di controllo;
- *Qualora i dati non siano raccolti* presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- *L'esistenza di un processo decisionale* automatizzato, compresa la profilazione

MODALITÀ DI ACCESSO

- Il titolare del trattamento fornisce all'interessato le informazioni senza giustificato ritardo, al più tardi entro ***un mese*** dal ricevimento della richiesta stessa
- Tale termine può essere prorogato a ***due mesi***, considerata la complessità e il numero delle richieste
- Le informazioni sono a titolo gratuito
- Tuttavia, se siano manifestamente infondate o eccessive il titolare può:
  - ***Addebitare*** un contributo spese ragionevole
  - ***Rifiutare*** di soddisfare la richiesta

IL DIRITTO DI ACCESSO IMPLICA:

- **DIRITTO A CHIEDERE LA RETTIFICA DEI DATI O LA LIMITAZIONE DEL TRATTAMENTO (art. 16-18)**
  - In caso di dati inesatti, fino alla rettifica
  - In caso di contestazione, fino a chiarimento
  - Su richiesta, in alternativa alla cancellazione
- **DIRITTO ALL'OBLIO (art. 17) e chiederne la cancellazione:**
  - Se è esaurita la finalità del trattamento
  - Se è stato revocato il consenso
  - Se è stata fatta opposizione al trattamento
  - Se trattati in violazione di legge

- Se i dati sono stati resi pubblici il Titolare è obbligato a cancellarli informando i titolari che stanno trattando i dati della richiesta di cancellarne ogni link, copia o riproduzione, tenuto conto della tecnologia disponibile e dei costi di attuazione.

La richiesta dell'interessato di ACCESSO ai dati personali che lo riguardano può avvenire in **QUALSIASI FORMA**
Il titolare del trattamento fornisce le informazioni richieste **senza giustificato ritardo**, al più tardi entro **un mese** dal ricevimento della richiesta stessa.
Tenuto conto della complessità e del numero delle richieste tale termine può essere prorogato a **due mesi.**
Le informazioni devono essere fornite **gratuitamente**.
Nel caso in cui siano manifestamente infondate o eccessive il titolare può:

- Addebitare un contributo spese ragionevole
- Rifiutare di soddisfare la richiesta

CANCELLAZIONE/DISTRUZIONE DEI DATI

- ***DATI MEMORIZZATI SU SUPPORTI ELETTRONICI***

No sufficiente:

- Cancellazione dei dati
- Formattazione dei dati

Opportuno ricorrere a sistemi di:

- Memorizzazione sicura
- Cancellazione sicura
- Demagnetizzazione o distruzione fisica del dispositivo di memorizzazione

- **DATI MEMORIZZATI SU SUPPORTI CARTACEI**
  1. Utilizzazione di apposito *distruggi documenti*:
     larghezza massima della striscia non deve superare i ***due millimetri*** e la superficie massima del frammento non deve superare i ***594 millimetri quadrati***

CONSENSO (ART. 4 CO.11 REG. UE 679/2016)

- MANIFESTAZIONE DI VOLONTA' LIBERA E SPECIFICA
- INFORMATA E INEQUIVOCABILE
- ESPRESSA MEDIANTE DICHIARAZIONE O AZIONE POSITIVA
- DIMOSTRABILE

TRA GLI ADEMPIMENTI RICHIESTI RIENTRANO ANCHE QUELLI DI:

- Aggiornare l'informativa
- Verificare che siano state adottate misure tecniche organizzative adeguate a garantire un livello di sicurezza pari al rischio
- Verificare l'idoneità dei sistemi informatici ad assicurare la protezione dei dati sin dalla progettazione
- Definire contrattualmente i rapporti con i Responsabili esterni del trattamento
- Valutare se procedere, per uno o più trattamenti, ad una valutazione di impatto

SANZIONI PECUNIARIE

Violazione obblighi sanciti dal Regolamento Europeo

Commisurate a percentuali del fatturato lordo mondiale dell'impresa diverse ***fasce di gravità***

- ***10.000.000 euro e 2% di fatturato per la violazione degli obblighi:***
  - del titolare e del responsabile del trattamento
  - dell'organismo di certificazione
  - dell'Organismo di controllo

- ***20.000.000 euro e 4% di fatturato per la violazione:***
  - delle condizioni relative al consenso
  - dei diritti degli interessati
  - di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi dei dati dell'Autorità di Controllo
  - di un ordine da parte dell'Autorità di Controllo di trasferimenti di dati a un destinatario in un paese terzo o organizzazione internazionale

SANZIONI AMM.VE PECUNIARIE PREVISTE DAL REGOLAMENTO EUROPEO

Irrogate tenendo conto di:

- ***Natura, gravità e durata*** della violazione
- ***Misure*** adottate dal titolare del trattamento o dal responsabile del trattamento ***per attenuare il danno subito***
- ***Eventuali*** precedenti ***violazioni*** pertinenti commesse dal titolare del trattamento
- ***Grado di responsabilità*** del titolare del trattamento o del responsabile del trattamento
- Maniera con cui l'autorità di controllo ha avuto ***conoscenza della violazione***
- ***Rispetto di provvedimenti*** disposti nei confronti del titolare e del responsabile del trattamento;
- ***Adesione*** a codici di condotta
- Eventuali ***altri fattori aggravanti o attenuanti*** applicabili alle circostanze del caso
- ***Carattere doloso o colposo*** della violazione
- Grado di ***cooperazione*** con l'autorità di controllo
- ***Categorie di dati personali interessate*** dalla violazione